The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study

THEA RIEBE, Technical University of Darmstadt, Darmstadt, Germany
MARC-ANDRÉ KAUFHOLD, Technical University of Darmstadt, Germany
CHRISTIAN REUTER, Technical University of Darmstadt, Darmstadt, Germany

Besides the merits of increasing digitization and interconnectedness in private and professional spaces, critical infrastructures and societies are more and more exposed to cyberattacks. In order to enhance the preventative and reactive capabilities against cyberattacks, Computer Emergency Response Teams (CERTs) are deployed in many countries and organizations. In Germany, CERTs in the public sector operate on federal and state level to provide information security services for authorities, citizens, and enterprises. Their tasks of monitoring, analyzing, and communicating threats and incidents is getting more complex due to the increasing amount of information disseminated into public channels. By adopting the perspectives of Computer-Supported Cooperative Work (CSCW) and Crisis Informatics, we contribute to the study of organizational structures, technology use, and the impact on collaborative practices in and between state CERTs with empirical research based on expert interviews with representatives of German state CERTs (N=15) and supplementary document analyses (N=25). We derive design and policy implications from our findings, including the need for interoperable and modular architecture, a shift towards service level agreements, cross-platform monitoring and analysis of incident data, use of deduplication techniques and standardized threat exchange formats, a reduction of resource costs through process automation, and transparent reporting and tool structures for information exchange.

CCS Concepts: • **Human-centered computing → Computer supported cooperative work**; *Empirical studies in collaborative and social computing*

KEYWORDS: Cyber Incident Response; Computer Emergency Response Team; Public Security Sector; Interorganizational Collaboration; Crisis Informatics

ACM Reference format:
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. In *PACM on Human Computer Interaction*, Vol. 5, CSCW2, Article 478, October 2021. ACM, New York, NY, USA. 30 pages, https://doi.org/10.1145/3479865.

Author's addresses: Thea Riebe, Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), Technical University of Darmstadt, Pankratiusstraße 2, 64289 Darmstadt, Germany, riebe@peasec.tu-darmstadt.de; Marc-André Kaufhold, Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), Technical University of Darmstadt, Pankratiusstraße 2, 64289 Darmstadt, Germany, kaufhold@peasec.tu-darmstadt.de; Christian Reuter, Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), Technical University of Darmstadt, Pankratiusstraße 2, 64289 Darmstadt, Germany, reuter@peasec.tu-darmstadt.de.

2573-0142/2021/10 - Art478 $15.00
https://doi.org/10.1145/3479865

1 INTRODUCTION

Research into computer-supported cooperative work (CSCW) has driven the field of crisis informatics [67], which is a multidisciplinary field "concerned with the ways in which information systems are entangled with socio-behavioral phenomena connected to disasters" [84]. Despite acknowledging the impact of human-induced emergencies, most research so far has focused on collective and individual behavior in natural disasters [64, 76] and the use of social media in the context of crisis response [92, 100]. However, driven by the increasing digitalization and interconnectedness of society, cyberattacks pose an increasing threat to both the virtual and physical realm. Looking at the 2015 Ukraine power grid cyberattack, the 2017 WannaCry ransomware attack, or the 2020 University Hospital of Düsseldorf hack, the vulnerability of critical infrastructures and society to cyberattacks becomes apparent [2, 18, 22]. As a consequence, securing information technology and cyber incident response for citizens, public services, and critical infrastructures have become part of national security agendas [6, 53, 101]. Related strategies do not only focus on the security of governmental organization and communication but also emphasize the importance of public-private partnerships (PPP) and multi-organizational collaboration for incident communication and response [68–70, 101].

The need for incident response and management led to the deployment of Computer Emergency Response Teams (CERTs), sometimes also called Computer Security Incident Response Teams (CSIRTs), in the public and private sector across the world. CERTs are monitoring, analyzing, and communicating threats and incidents [24], offering reactive services and preventive measures for authorities, citizens, and enterprises [54]. However, managing these tasks while processing the increasing amount of available data across different channels, such as blogs, feeds, social media, and websites has become a complex challenge [28, 77, 86]. Besides information overload, the quality and speed of incident response is threatened by false or inaccurate information [48]. In order to provide effective incident management and response, CERTs are not only required to conduct ad hoc analysis to enhance their cyber situational awareness [28], but also to collaborate with other teams or third parties, sometimes with less advanced skill levels [51]. As security incidents become more widespread in interconnected infrastructures both in the public and the private sector, their services and collaboration by sharing threat information and specialized skills is becoming increasingly important [27, 41, 81]. The collaboration of CERTs, to the best of our knowledge, has not been studied from the CSCW perspective yet. The study of CERTs in Germany offers an interesting case to address this gap. As a federal country with 16 states, Germany has installed 13 CERTs (from which the CERT Nord is responsible for four states) as well as a CERT for the federal administration (CERT-Bund). Since 2001 they have become "a focal point for preventive and reactive measures in security-related incidents in computer systems"[26] in Germany. The states have implemented individual plans, resulting in a network of differently structured and resourced CERTs. In the light of resulting deviations in expertise, organizational structures, and used technologies, effective collaboration is of utmost importance to increase cyber situational awareness, the analysis and response to cyber incidents, and thus the cyber security of the public sector, society, and industrial production. However, there is a lack of empirical studies examining the collaborative practices of CERTs [51]. We investigate German CERTs that work in and for the public administration to answer the following research question:

- How do organizational structure, technology use, and cross-organizational collaboration contribute to cyber incident response of German state-level CERTs?

To answer our research question, we conducted semi-structured expert interviews with 15 participants and analyzed 25 secondary documents. Through a qualitative content analysis of the captured data, we:

- Offer insights into the organizational structure and work processes of German state-level CERTs.
- Describe the technologies and practices used for cyber incident awareness, collaboration, and incident response.
- Analyze the collaboration and its constraints among German state-level CERTs and external stakeholders.
- Provide key insights, challenges, and design and policy implications for successful organizational structure, technology use and cross-organizational collaboration in German state-level CERTs.

Our study contributes to the CSCW discourse by describing "a work environment/setting where collaboration is important" [95p. 4], connecting cyber security, crisis informatics and CSCW, and building foundations for design and evaluation studies to support the collaboration of CERTs. The paper is structured as follows: First, we present related work on the organization, technology use, and collaboration for cyber incident response to highlight our research gap (Section 2). Second, we outline the methodology in terms of case selection, mode of content analysis, conducted interviews, and analyzed documents (Section 3). Based on this, we present the results of our qualitative content analysis (Section 4). The paper concludes with a discussion of findings, implications for design and policy, limitations, and future work (Section 5).

2 RELATED WORK

The collaboration of spatially and temporally distributed emergency response teams in general and specifically in the public sector is a central research field within CSCW [15, 60, 61, 78]. There has been extensive research on how the design and use of technology influences and supports response teams, their workflows, and collaborative work [15, 58, 78, 80]. In this sense, collaboration can be described as the development of a set of common practices to monitor individual behavior and enable task coordination as well as flexible division of labor. In this context, technology provides a set of tools through which certain activities within the present setting become visible or publicly accessible. To allow the effective management of crises, the practices are designed to be independent of personnel, so that they can also be adopted by newcomers without previous collaboration and without much explanation [33].

2.1 Organization of Governmental CERTs

Incident response in situations of uncertainty and high pressure has been studied in CSCW with regard to natural and man-made disasters, focusing on the collaboration among different emergency services, as well as with citizens [64, 76, 78, 80, 84]. In terms of cyber incident response, state-level CERTs have become important organizations to protect citizens, public administration, and critical infrastructures against cyberattacks and their potential real-world impact [54]. CERTs exist in public and private organizations and offer a variety of proactive and reactive services [98] to achieve their goal "to be a focal point for preventing, receiving and responding to computer security incidents" [50]. Existing studies have been emphasizing the necessity of collaboration between the different CERTs [71, 83] as well as other security experts

and volunteers [25, 97]. In a comparison of national security strategies, Boeke [9] has highlighted that due to the state size, Estonian cyber security is largely dependent on the help of state-directed civilian volunteers and international cooperation. In the United Kingdom, studies have found that cyber security is the task of private companies with less importance of state interference as a consequence of privatizing communication infrastructure [16].

With specific regard to Germany, research has focused on the federal structure and its consequences for cyber security [87]. Legal experts have suggested to update federal security architectures in line with the increasing challenges of cyber security, including the effective integration of local and state level response into the national security strategy [21]. In accordance, studies have shown that a decentralized approach to security can also provide benefits in crisis response [79]. Distributed management as well as the sharing of information and experiences has shown to positively impact effectiveness of cyber security [21, 96]. Van der Kleij [22, p. 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 [1], who suggests double-loops for learning, which means that the learning should not only include individual incidents but also systematic response structures, as well as taking part in cyber security defense competitions for simulation training [27]. To create educational simulations for the training of municipal security experts for effective defense, Gedris et al. derived design implications for cyber security scenarios which highlight the complex socio-technical context of public infrastructure [29].

2.2 Technology and Collaboration of CERTs

To fulfil their tasks, CERTs use a variety of different technologies, especially Cyber Threat Intelligence (CTI) platforms, to enhance cyber incident response. Furthermore, they maintain cross-organizational collaboration with other CERTs and external stakeholders to facilitate collective crisis management [57]. Incident monitoring has shown to be complex due to increasing digitalization and services that CERTs have to provide. Often, incident reporting and procedures in connection with incidents are not standardized, and sometimes there are legal and psychological restraints in reporting due to data protection and company policies [8]. Therefore, receiving and analyzing threat incident information made additional security infrastructure and access for CERTs necessary, such as information on network traffic [91], deep packet inspection [72], and the use of machine learning to support incident detection [56]. Padayachee and Worku [66] have pointed out the advantage of collaboration among CERTs as they are more easily alerted to large-scale cyber security incidents and better capable to manage them adequately than alone. While many private and governmental organizations manage cyber security incidents individually, the protection of interconnected networks against internationally operating criminal groups can be better addressed with a shift towards cross-organizational information exchange [82]. Khurana et al. [49] propose the prototype "Palantir" to enable effective multi-site cyber incident response including a collaborative workspace for discussions and data sharing. The authors highlight the crucial role of trust between organizations for sharing incident data.

Despite the identified need for cross-organizational collaboration and information sharing between cyber security organizations such as CERTs [51, 81, 97], mainly the cooperation between law enforcement agencies has been examined [17, 41]. With view to the collaboration of German CERTs, the communication between the federal- and the state-level, CERTs as well as the private CERTs is considered as crucial to gain the situational awareness on the scope and

severity of an incident and decide on the response [34, 38, 101]. When CERTs were first established in Germany, Kossakowski [54, 55] observed that in addition to a lack of time resources, also insufficient mutual trust also resulted in low levels of cooperation. Thus, the work of security experts consists of "heterogenous bundles of practices" for the shared commitment towards cyber security [52]. Therefore, our study takes the organizational structure and the technology use into account.

2.3 Adapting Crisis Informatics Research to the Cyber Security Domain

Since the 2001 September 11 attacks, a considerable body of knowledge has been established in the research domain of crisis informatics, including empirical investigations of social media use and role patterns in crises [85, 93, 94], collection, processing, and refinement of social media data [3, 13, 46], system design and evaluation [5, 48, 65], as well as cumulative and longitudinal research [39, 64, 75]. Although it is common to distinguish anthropogenic (e.g., building collapse, shootings) and natural disasters (e.g., earthquakes, epidemics, hurricanes, floods, wildfires) in crisis informatics [64], only little domain-specific research considers the anthropogenic risks of cyberattacks [29]. However, like regular emergency services, such as fire or police departments, CERTs provide preventive and reactive capabilities and started to use social media (tools) to enhance their situational awareness but in response to cyber threats [36, 47]. Since CERTs are confronted with similar issues when analyzing open and social data, including information quality and information overload [73], it seems sensible to examine the adoptability of findings from crisis informatics to the domain of cyber security.

Besides researching formal crisis response organizations, crisis informatics has examined the emergence of digital volunteers, which are citizens that assist crisis response using the virtual realm and sometimes organize as Virtual and Technical Communities (V&TCs) [31, 74, 85]. Grasping the potentials of organized digital volunteers, so-called Virtual Operations Support Teams (VOST), comprising of trusted volunteers, were deployed during the 2011 Shadow Lake fire in the USA to monitor social media activities related to the emergency [19]. In the following years, VOSTs were deployed across the globe to assist emergency services by crowdsourcing emergency-related tasks, among them the VOST of the German Federal Agency for Technical Relief (VOST-THW) [25]. This concept is also becoming more interesting for the domain of cyber security: for instance, to overcome the resource limitations of federal and state-level CERTs in Germany, a recent initiative seeks to utilize the capabilities of organized digital volunteers by establishing a formalized Cyber Relief Agency [4].

2.4 Research Gap

Our literature review revealed a body of research on the organization of CERTs, including structure [34, 54, 55, 83, 88], national comparisons [9, 16], governmental frameworks [14, 20, 42, 43, 63], management [37, 62], and their effectiveness [1, 12, 27, 51]. Further studies investigated situational awareness, including the access [8, 72] and analysis [32, 56, 91] of data, and the dissemination of warnings [41, 68]. While plenty of research has been conducted on data collection and data visualization, in their systematic literature review, Franke and Brynielsson [28] noted a lack of empirical research on information exchange between relevant actors. Especially the collaboration between IT security teams, not only from the perspective of IT security, but also focusing on socio-technical systems has been highlighted as a field for further research [51, 52]. At the same time, the lack of exchange has been named as an obstacle in responding to large-scale cyberattacks [82]. To the best of our knowledge, no empirical studies

on the collaboration of state CERTs in the federal system of Germany have been published yet, calling for an analysis through the lens of CSCW. However, the lack of exchange has been named as obstacle in responding to large-scale cyberattacks [82].

An exercise that aimed to test the defense skills of 900 participants from EU member states showed that public-private cooperation is central for guaranteeing cyber security, but also stressed the importance of strengthening cooperation on a national level by establishing more structured operating processes [23]. In a survey with CERT members, Ioannou et al. [41] identified important challenges in communication and coordination that weakened cyber security culture. Van der Kleij et al. [51] conducted semi-structured interviews with Dutch CERT members, highlighting the need across CERTs for collaborative sensemaking, including collaborative problem-solving capacity and shared incident awareness However, as it was a study from the field of psychology and the focus was on team effectiveness, it did not address the aspect of technologies used or required for collaboration and situational awareness. By analyzing empirical data from documents and interviews, our paper contributes findings on the implications for cross-organizational collaboration and technology design for German state-level CERTs.

3 METHODOLOGY: EMPIRICAL STUDY WITH GERMAN CERTS

The German federal administration provides an interesting case as it facilitates the collaboration between independent cyber security organizations 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 German Federal Office for Information Security (BSI). The individual CERTs are part of the Administrative CERT Network (Verwaltungs-CERT-Verbund, VCV) which provides an information exchange platform for public administration, thus offering an institutionalization of CERTs' partnerships [102]. The structure, size, and the skill set of these CERTs depend on financial resources and the requirements of the target groups. They usually have a strategic head, the chief information security officer (CISO), and an operational head of team, who leads a small number of incident managers and cyber security specialists. In some cases, CERTs provide a public safety answering point (PSAP) for citizens and enterprises. The basic skill sets of CERT employees comprise IT security knowledge to detect threats and estimate their severity as well as communication skills to enable a proper response to incidents [89]. In 2019, the BSI reported 770,000 emails containing malware in German governance networks, 114 million new versions of malware, and 252 reported incidents by critical infrastructure operators [10]. While the skills and level of organization of criminals increase, one CERT employee (I14) assumed that the number of incidents at least doubles once per year, making the collaboration between CERTs even more important. The objective of our empirical study, which comprises semi-structured interviews and document analyses, is to examine the organizational structure, technology use and cross-sector collaboration in German state CERTs.

3.1 Data Collection: Interviews and Document Research

The semi-structured interviews were designed to provide insights into the organizational structure, technology use, and collaborative practices within and between CERTs. To acquire the necessary data, we sent requests for semi-structured expert interviews [30, 45] in two rounds. We approached all 14 CERTs on federal and state level, but only six CERTs responded and agreed to participate the interviews. After receiving their acceptance and informed consent,

each interview session lasted around 50 minutes. In the first round of interviews (n=8, I1-I8), we put a strong emphasis on organizational factors and collaborative practices. Our interview guide, covering the categories of the codebook (section 3.1), comprised nine open-ended questions structured in three parts: (1) an introduction of the interviewee and his/her organizational role, (2) the deployment, organization, and work processes of the CERT, and (3) the communication and cooperation between CERTs.

As we wanted to gain further insights into technology use by CERTs, we conducted a second round of interviews with those CERTs that were interested in further research collaboration (n=7, I9-I15). In this second round, we also included the perspective of some non-CERT organizations (I09, I10, I15). For instance, we approached a civil protection VOST (I09) and a voluntary humanitarian organization (I15) to gain insights into cyber security practices and technology use in the domain of crisis management and civil protection. Furthermore, we interviewed an information security officer (I11) of a state company who previously worked in a CERT organization to utilize his prior experience and get insights into how his work has changed as an information security officer. The interview guidelines comprised technology-focused questions on the (1) interviewees' role and organization, (2) reporting of cyber incidents, (3) monitoring of cyber incident data (e.g., indicators of compromise), (4) analysis, prioritization, and verification of gathered evidence, as well as (5) communication of recommendations and warnings.

To include and gain insight into the remaining eight state-level CERTs of Germany which were not available for interviews, we conducted document analyses using public CERT websites, protocols of parliamentary debates, and administrative documents (N=25, see Section 6.1 of the appendix for more details). While these official documents are publicly available and allow the identification of the related CERT, we at least had to ensure the anonymity of the interviewed CERTs.

Table 1 summarizes the analyzed documents and conducted interviews.

Table 1. Overview of the interviewed organizations, theirs types, as well as corresponding documents and interviews, only one interviewee participated in both rounds (I3, I10). Abbreviations: Head of Team (HT), Incident Manager (IM), Information Security Officer (IS), Public safety Answering Point (PSAP)

Organization Type	Documents	Interviews (First Round)	Interviews (Second Round)
Ministry CERT	-	I04 (IM), I05 (IM)	-
Service CERT	D01-D03	-	-
Ministry CERT	-	I08 (HT)	-
Service CERT	D04-D06	-	-
Service CERT	D07-D10	-	-
Ministry CERT	-	I1 (IM), I02 (HT)	I12 (HT), I13 (PSAP), I14 (IM)
Ministry CERT	D11-D13	-	-
Service CERT	D14, D15	-	-
Service CERT	D16-D19	-	-
Service CERT	-	I03 (HT)	I10 (HT)
Ministry CERT	-	I07 (IM)	-
Ministry CERT	D20-D23	-	-
Service CERT	D24, D25	-	-
Civil Protection	-	-	I09 (HT)
State Company	-	-	I12 (IS)
Civil Protection	-	-	I15 (IS)

3.2 Data Analysis: Codebook Development and Structured Content Analysis

We conducted a qualitative content analysis following the step model of deductive category application [59]. This requires defining analytical categories and developing a codebook, which comprises analytical categories, definitions, examples, and coding rules to be applied to our interview transcripts and collected documents. We preferred this deductive approach over an inductive, bottom up, or open coding to allow a structured comparison of the capabilities and services of CERTs. The codebook design was deductively informed by relevant literature and especially by the work of Skopik et al. [101], who assume that CERTs serve as interface organizations which monitor and collect data on threats, assess risks for their customers, communicate and handle incidents, as well as interact, cooperate, and collaborate with other organizations. The latter includes expert networks, such as the VCV, where CERTs exchange knowledge and services. Based on the literature, the first two authors identified ten analytical categories summarized under the domains of organization (CERT association membership, defined protocols for cross-organizational collaboration, distinct target group definition for incident reporting), technology (use of exchange platforms, alerting and reporting service, advisory service), and collaboration (information access, coordination competence, public-private partnerships, information interface to emergency services). For each category they developed definitions and coding rules, which are specified in the detailed codebook in the appendix (Section 6.2).

Table 2. Anonymized CERT scores in terms of organization, technology, and collaboration. Note that the character "–" is used when no information was available based on our interview and document analyses; however, it is treated as 0 when calculating sums.

Domain	Category	Service CERTs							Sum		Ministry CERTs							Sum	
		#1	#2	#3	#4	#5	#6	#7	Σ	%	#8	#9	#10	#11	#12	#13	#14	Σ	%
Organization	CERT association member (VCV)	1	1	1	1	1	1	1	7	100%	1	1	1	1	1	1	1	7	100%
	Defined protocols for cross-organizational communication	1	-	0.5	1	1	1	1	5.5	79%	1	1	1	0.5	1	1	0.5	6	86%
	Distinct target group definition for incident reporting	1	1	1	1	1	1	1	7	100%	1	1	1	0.5	1	1	1	6.5	93%
Technology	Use of exchange platforms	1	1	1	0.5	1	1	1	6.5	93%	1	1	0.5	1	1	1	1	6.5	93%
	Alerting and reporting service	1	1	1	0.5	0.5	1	1	6	86%	1	1	1	1	1	1	1	7	100%
	Advisory service	0.5	0.5	0.5	0.5	0.5	1	0.5	4	57%	1	1	1	0	1	0	1	5	71%
Collaboration	Information access	-	1	-	0.5	-	1	1	3.5	50%	1	1	-	0	1	0	1	4	57%
	Coordination competence	-	-	1	0	-	1	1	3	43%	0	1	0.5	1	1	1	1	5.5	79%
	Public-private partnerships	1	-	1	0	0.5	0.5	0.5	3.5	50%	0.5	0.5	0	0	1	0.5	1	3.5	50%
	Information interface ES	-	-	1	1	1	0.5	-	3.5	50%	1	1	0.5	0	1	0	1	4.5	64%

For the analysis and interpretation of the collected documents (D1-D25) and conducted interviews (I1-I15), we followed the approach of Kaiser [44], which comprises the steps of transcription, coding of text, identification of core statements, extension of the data corpus, as well as theoretical analysis and interpretation. First, we created full transcripts of the interview data. Since we had to delete the audio material after transcription to ensure anonymity, we refrained from paraphrasing to preserve the richness of the data. Then, we analyzed the collected documents and created interview transcripts carefully to apply codes of the developed codebook to fitting passages. Four coders were involved in the process: while three coders conducted the initial round of coding, the main author checked and – if required – amended codes in a second round to ensure consistent coding across all interviews and documents. Also,

core statements were added as examples to the codebook. Although our work was guided by the codebook, we also inductively considered categories that emerged from data in our qualitative analysis.

Besides the qualitative analysis of documents and interviews, one aim of our study was to understand the ways in which differences in the hierarchical establishment influence the capabilities and services provided by CERTs. The information whether a CERT is embedded into a ministry or into a separate state company was extracted from the individual CERT websites. To facilitate a comparison of both ministry and service CERTs, we used the categories of the codebook to quantify their organizational, technological, and collaborative capabilities and services. We used the interview data of the six interviewed CERTs plus the analyzed documents of the eight non-interviewed CERTs to determine the scores. Since each category of the codebook represents a specific capability or service, we used a 3-point scale to evaluate whether a CERT meets the definition of the category to full extent (1 point), only partially (0.5 points), or not at all (0 points). For each category, a different coding rule is used to determine its score (Section 6.2, Appendix). The coding was conducted by two researchers initially and then checked and amended by the leading author. The individual but anonymized CERT scores are presented in Table 2. Besides the descriptive and summative lines and columns, each line represents a category (e.g., capability or service) and each column either a service CERT (n=7) or ministry CERT (n=7). In the following Tables 3-5, we summarize the scores per category for both ministry and service CERTs and display the percentage-based results. For instance, service CERTs achieve a 79% score for the "defined protocols for cross-organizational communication" category, which means that they acquired 5.5 of 7 possible points.

4 RESULTS

In this section, we present our findings categorized by the themes of organization structure, practices and technologies for cyber incident response, as well as collaboration among CERTs and other stakeholders.

4.1 Organizational Structure, Interorganizational Exchange and Target Groups

The organizational establishment of state-level CERTs in Germany was driven by a directive of the IT Planning Council (I3), which is an institution that coordinates the collaboration between the federal government and states in Germany: "States are obliged to follow and implement the resolutions of the IT Planning Council" (I1). Aside from this legally binding dimension, there are various ways to associate CERTs either within a state ministry or an IT service provider. The latter can be so-called state companies which are legally dependent, but organizationally outsourced parts of the state administration (I10). In accordance with the different forms of hierarchical establishment, it became evident that there is a "administrative-focused perspective" in ministry CERTs, which work more closely with other ministerial security organizations, in contrast to a "technology-focused perspective" in service CERTs, which work closer to the operators of IT infrastructures. Due to different hierarchical establishments, internal administrative regulation, external regulations of superordinate authorities, but also a lack of necessary regulations, challenges in daily work and collaboration become apparent:

> "The legal basis for this is not yet available in the level of detail that would actually be necessary, so that colleagues from [another CERT, anonymized] can work with us at

all, and it is not yet clear how a common file storage system can be created. It is probably not even possible" (I1).

When examining the *interorganizational exchange* between CERTs, the interviewees indicated that the VCV network is used for bilateral cooperation and multilateral exchange: "And there is a general interest to work hand in hand because without such a network you are nothing" (I5). Besides state CERTs, the federal CERT-Bund (as part of the BSI) is present in the VCV but operates at federal-level and thus works under different framework conditions (I3). Still, the cooperation with state CERTs is defined by agreements, guidelines, and technology:

> "The cooperation on a state and federal level is organized by a cooperation agreement, a guideline of the IT Security Council and a formal, political decision. This decision provides the contents, complemented by a regulation for reports, and is supported with a wiki page and a shared chat software by the CERT-Bund" (I5).

Facilitated by the role of the BSI (I3), cooperation among CERTs is planned to be shifted towards service level agreements:

> "There need to be respective contact persons, there needs to be appropriate conversation, and the BSI needs to appropriately support the states. This is why the BSI has built a centre for liaison in the past months. Therefore, various cooperation agreements exist that are planned to become service level agreements" (I5).

Table 3. Categories (representing capabilities or services) and anonymized CERT scores (percentage-based, cf. Table 2) in terms of organization and work

Categories	Service CERTs	Ministry CERTs	Observations and identified challenges	Design or policy implications
CERT association member (VCV)	100%	100%	• All CERTs are in regular and institutionalized exchange in the VCV	• Technology design should make use of the existing exchange infrastructure of the VCV
Defined protocols for cross-organizational communication	79%	86%	• Almost uniform standardization regarding the structure of information is observed (TLP)	• Although the TLP is the most common protocol, support for different information classification protocols is required
Distinct target group definition for incident reporting	100%	93%	• Service CERTs seem to have a more precise definition of target groups, while ministry CERTs address a broader range of groups (such as citizens and SMEs)	• Design of incident reporting and communication needs to address the needs of the different target groups

There are different protocols and standards that regulate the work, information management, and communication of CERT teams (Table 3). These include, amongst others, the standard on how to report cyber threats, for instance, via phone call or online form and the information sharing traffic light protocol (TLP), which is used to determine the confidentiality of information in intra- and interorganizational communication by classifying documents or information as red, amber, green, or white (with decreasing confidentiality). Almost all CERTs mentioned those two procedures either in the interviews or in public documents. All CERTs primarily support the public administration as their main target group. Still, some of them also include citizens, small and medium-sized enterprises (SMEs), or critical infrastructure providers as their target group (I12). Due to their variations in employee expertise and quantity, hierarchical integration, and specified target groups, all CERTs offer a different portfolio of services: "Therefore, the teams are relatively difficult to compare because they all have a little bit different focus" (ID3). Within the ministry, CERTs have IT-security appointees as a point of contact. The coded documents and the interviews showed no difference regarding this target group. In summary, the values in Table 3 confirm that interorganizational exchange is well developed both regarding ministry and service CERTs due to the establishment of the VCV. Still, protocols and work processes could be improved in at least four CERTs.

4.2 Technologies and Practices for Cyber Incident Response

When analyzing responses of the second-round interviews (I10-14), we identified differences and similarities in their use of ICT. An attempt to generalize ICT use of German state CERTs is depicted in Figure 1. The process can be roughly divided into the steps of acquisition, analysis, and response. First, incidents are either reported by customers (via mail or telephone) or detected by software (such as intrusion detection). After initial information about the incident is gathered, CERTs use a ticketing and reporting system to collect their evidence for incident response. Second, this evidence is collected and analyzed using awareness-focused (e.g., manufacturer websites, security advisory feeds, and social media channels) and collaboration-oriented (e.g., malware information sharing platforms, the VCV collaborative chat) channels. Third, the collected evidence is then used to inform a certain stakeholder with specific recommendations, to provide (daily) reports for selected stakeholders (e.g., a daily vulnerability report for ministries), or to issue a general warning for multiple stakeholders (in case larger-scaled ICT infrastructures are threatened).

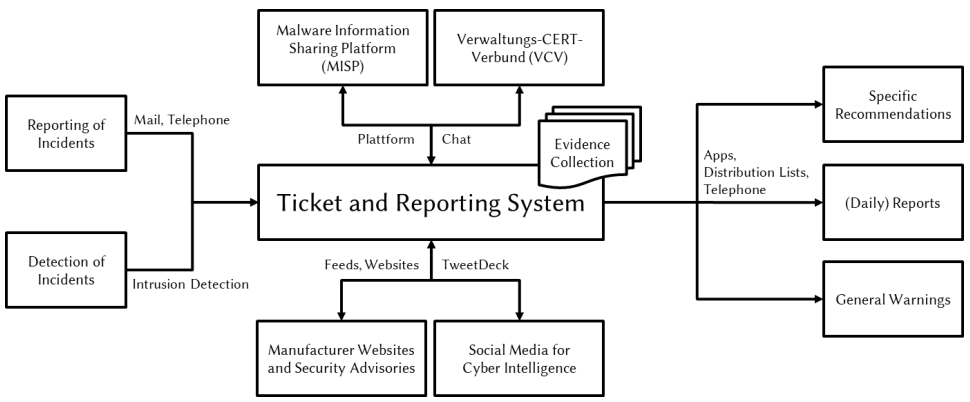

Figure 1. Example of a state-level CERT information and communication technology infrastructure.

The acquisition of information about incidents differs among CERTs. For instance, while one of the CERTs relies only on the reporting of incidents, another uses an intrusion detection software (IDS) to monitor their state administration network (I10, I11). In order to structure incident reporting, two CERTs defined a list of required information for further processing and damage assessment, of which the latter one is based on the RFC2350 specification. However, to reduce entry barriers, in the first contact usually only the most important information is discussed:

> "We try to set a relatively low inhibition threshold so that people report at all. You can't ask for all when there is a security incident and people are nervous. Then it is actually enough for us if they pick up the phone and inform us" (I10).

While incident reports were previously managed in Excel sheets, some CERTs implemented ticketing and reporting systems, such as OTRS, with a new ticket opened for each incident report (I12). These systems are then used to collect awareness-based or collaboration-based evidence or information on the reported incidents before response activities are conducted.

In terms of awareness-based evidence, the backbone of CERT activities lies in analyzing manufacturer websites and security advisories to identify Indicators of Compromise (IOCs). While manufacturer websites report incidents on their specific hardware or software (e.g., Apple, Cisco Systems, Google, IBM), security advisories are often curated feeds of security organizations (e.g., BSI, DFN-CERT, US-CERT) that integrate incident information across different sources. However, there are multiple issues with collecting open source information. First, they are provided in different and regularly changing formats, which makes it hard to maintain software for structured acquisition. Second, as a consequence, CERTs have to manually check manufacturer websites and security advisories on a daily basis for their reporting, which can consume up to two hours daily (I10, I12). Third, as multiple security advisories are used for gathering information, CERTs are confronted with the issue of redundant information, currently requiring a manual deduplication of entries or information. Furthermore, some CERTs actively monitor social media to identify IOCs (I1, I3, I5, I6). Their main approach is to follow and monitor Twitter accounts of security experts and organizations, which is occasionally combined with topic-specific searches. One of the CERTs used TweetDeck to support the semi-automatic monitoring of Twitter accounts and a more automated monitoring of further social media is generally desired. However, a major part of Twitter monitoring is still conducted manually due to legal challenges and lack of tailored technology:

> "We monitor social media using the best effort principle. Currently, we do not have the capacities to monitor all media. We would benefit from a higher degree of automation, however, we are thwarted a bit by our lawyers, because we need the legal foundations before" (I1).

Furthermore, VOST-THW uses the tool ScatterBlogs for monitoring and analyzing social media, which however is limited to Twitter and not tailored according to CERT requirements (I09). When using automation for gathering public data, data minimization, protection, and privacy regulations of individual organizations and states must be considered (I09, I15). Two further CERTs do not monitor social media, but either receive the information from a different state division or other organizations, such as the BSI, VCV, or in bidirectional cooperation with a different CERT.

In terms of collaboration-focused evidence acquisition, according to our interviewees, physical distance does not hinder collaboration as *exchange platforms* and modern technologies

facilitate communication in near real-time (I4). Besides common communication channels, such as e-mails and telephones, a chat and a wiki page were set up to reduce knowledge gaps (I3). Especially the chat tool is seen as a measure to avoid unnecessary duplication of work and is appreciated for the possibility of real-time exchange in urgent cases: "We are in direct contact with the colleagues without going through the official channels when immediate incidents such as massive spam waves occur" (I1). However, the utility of the chat may not always be very reliable as the reporting is left to the employees' discretion and because of a lack of time resources (I1, I2). Therefore, one interviewee suggested the idea of automated data exchange between CERTs:

> "But there is certainly potential for improvement, i.e., the timely exchange of technical safety-relevant information is still done manually between teams today. There is a clear potential for improvement" (I3).

Besides collaboration in the VCV, IOCs are collected using a shared instance of the Malware Information Sharing Platform (MISP), which is an open source platform for threat intelligence collection and sharing. Amongst others, MISP allows the provision of structured malware information which can be imported into IDS software to enhance their detection capabilities and it "works better than solutions using pattern detection" (I10). However, if IOCs are detected by multiple CERTs, there is a risk for redundant entries:

> "In the VCV, we talk about IOCs and check [manually] if they were already entered twice or threefold [into MISP]. The redundancy check is not yet automated" (I6).

In this way, technological shortcomings are compensated by the collaborative practices among CERTs. Still, interviewees considered the redundancy of security advisories as "an unsolved problem in the CERT community" (I10), which could be relieved by automated redundancy handling algorithms (I10, I14).

Based on these infrastructures, CERTs are able to offer their alerting, reporting, and advisory services (Table 4). In terms of alerting, CERTs provide recommendations for action to allow their target groups to respond to cyber incidents. If a security vulnerability could potentially affect multiple organizations or target groups, a warning with preventative information is sent via e-mail distribution lists. Besides individual incident handling, CERTs create daily vulnerability reports to sharpen the security awareness of their target groups. In summary, alerting contact points in the administration or the target groups is at the core task of all CERTs. Other communicative practices of CERTs are advisory services and education of stakeholders, such as citizens, ministries, municipalities, or small and medium-sized enterprises. However, some CERTs are highly specialized and have a more specialized division of labor, than others. They focus on incident management, while outsourcing communication aspects such as awareness and education raising to other departments. In contrast to the organizational structure, Table 4 indicates that technologies and services for cyber incident response are less, but still well established across different CERTs (avg. 79%-88%). However, an aspect that is not covered by our initial coding scheme is the lack of supportive technology for gathering open source intelligence (OSINT) from manufacturer websites, security advisories, and social media. This issue implicates a lot of manual *intraorganizational* work, which can only be partly alleviated by *interorganizational* collaborative practices due to different requirements and technologies used across state administrations, SMEs, or other clients (I10, I12). In ministry CERTs, their advisory and alerting functions appear to be somewhat more strongly developed due to the focus on the overall situational awareness reports.

Table 4. Categories (representing capabilities or services) and anonymized CERT scores (percentage-based, cf. Table 2) in terms of technology

Categories	Service CERTs	Ministry CERTs	Observations and identified challenges	Design or policy implications
Use of exchange platforms	93 %	93%	• All CERTs participate in the exchange platforms by the VCV, in a Wiki and a Chat, but there is a lack of tools for gathering OSINT	• Design of tools to increase automation and reduce redundancies when gathering OSINT for incident and threat processing and sharing
Alerting and reporting service	86%	100%	• All CERTs inform their target groups on vulnerabilities, however some CERTs (mostly in ministries) produce regular additional vulnerability reports	• An alerting and reporting tool should be able to generate vulnerability reports, design should also consider possibilities for automatization of generation of alerts, threat and incident data analysis and reporting
Advisory service	57%	71%	• As ministry CERTs address more target groups, their advisory services seem to focus on a broader spectrum of groups	• Further investigation on the possibilities of automation of standard cases • Improve the pooling and sharing of expertise for complex incidents

4.3 Collaboration Among CERTs and External Stakeholders

Both organizational structure and technology shape the collaboration among CERTs. Our interview participants especially valued the mutual exchange in the VCV network. The regular meetings of the VCV are an essential part of the communication (I4) and CERTs are highly intrinsically motivated to participate in the meetings that normally take place twice a year (I1) and are used to guide upcoming collaboration (I3). The CERTs can benefit from synergies within the VCV, for example, by sharing forms that follow the incident report standard (I3). The meetings of the VCV help to build relationships and networks on a personal level (I3):

> "Over the years, we have established something like a web of trust which comprises trustworthy people and, for instance, helps to verify information gathered online" (I10).

Furthermore, the VCV allows employees of CERTs to visit other institutions (I5) so that knowledge is shared and they can "immerse into the daily operations on-site and learn how they live, how the information appears. This form of communication is very versatile, a whole range of possibilities to learn from each other and the CERT-Bund" (I5). However, due to varying organizational guidelines among CERTs, such as slight variations of the TLP confidentiality levels, the acting individuals have a great responsibility to assess the confidentiality of exchanged information and prevent their unintended disclosure (I3). Furthermore, the VCV provides the possibility to request resources from other CERTs but only in a non-binding manner:

> "But it is not binding, when [another state] says they have a new Sand Box solution, they cannot say 'please send all our malicious software to them' […]. It is an offer, we can accept it or decline it, but we will not reach a binding decision in the VCV except for standards for reporting and other such things" (I2).

The network is also used to establish bilateral cooperation to facilitate knowledge sharing or service exchange. For instance, due to limited financial resources, smaller CERTs may not be able to deliver all required services (I4). To address this problem of lacking resources, in one case tasks were delegated to a different state CERT:

> "Yes, we are not a complete CERT but cooperate with (anonymized state). This also means that tasks that should be carried out by us are covered by the CERT of (anonymized state)" (I4).

This cooperation shows that also smaller states with less resources can enhance their capabilities in the context of cyber security and can therefore contribute to the security measures against cyberattacks (I2, I4). In this specific case, the cooperation affects tasks such as the creation and distribution of warning reports, tickets, and guidelines as well as the checking of suspicious e-mails (I4). In terms of *information access*, some CERTs state that are not oriented towards the CERT-Bund with its unique position at federal level but rather focus on mutual observation and learning of other state CERTs as they take on similar tasks that need to be adjusted to local peculiarities (I5). However, as a challenge, bilateral cooperation can be subject to asymmetrical information flows:

> "The (anonymized CERT) is sufficiently different from us, we have nothing to do with them technically, we do not really know who they are associated with, they simply get our information, but the return flow is low" (I3).

The nature of collaboration is further influenced by the different types of public ministerial and service CERTs. This has an impact on the specific expertise of the recruited personnel: "This makes a difference, the CERTs of an IT service provider are organized in a technical way, they are usually technicians. There often are people who are less technically experienced in the ministries" (I2). Especially different profiles of expertise, regular exchange, and generation of trust are crucial for networking:

> "The personal contact, knowing who you are dealing with, developing bonds of trust beat all formalities, beat all regulations, because if there is a will, there is a way. And with this model of personally getting to know each other this will is built, a network of personally known actors. When you need help or have limited resources, as a first step, you rely on those who you have a good relationship with" (I5).

The collaboration among CERTs can also be viewed from the perspective of *public-private partnerships*. In contrast to their ministry-embedded counterparts, service provider CERTs of some states are based in economic state companies. In this case, the activities and coordination of the BSI and VCV facilitate intensified and formalized cooperation between ministry and service CERTs:

> "The cooperation between states is encouraged by the BSI, because they want to reduce their effort of consulting. Therefore, we try to coordinate ourselves in the VCV before requesting help from the BSI. But the support of all sides and also from the BSI is

excellent. We usually get an answer on the same working day if it is particularly important and urgent" (I1).

However, regardless of their organizational embedding, state CERTs compete with CERTs in the private sector, which are part of bigger enterprises:

"The labor market offers almost no personnel, the teams cannibalize each other, which is admittedly not constructive. [In] the state CERTs, fluctuation, and lots of migration between the CERTs take place. This is not good" (I3).

There are huge differences in employer attractiveness of either public or private CERTs. While state CERTs are bound to the tariff agreements for the civil service of the states, the salary of employees in the private sector tends to be higher, thus attracting higher numbers of applicants (I3).

Table 5. Categories (representing capabilities or services) and anonymized CERT scores (percentage-based, cf. Table 2) in terms of collaboration

Categories	Service CERTs	Ministry CERTs	Observations and identified challenges	Design or policy implications
Information access	50%	57%	• Information access depends on the organizational structure: beside the incident notification, CERTs collect information from various sources. Access to more open sources can be considered	• Inclusion of open access sources, like social media expert communities, into automated system, which gathers incident relevant information
Coordination competence	43%	79%	• Ministry CERTs seem to be more capable of coordinating tasks between CERTs and other organizations. The allocation of resources between CERTs seems to be unequal	• The unequal distribution of resources can be addressed by (semi)automation of standard tasks, as well as by pooling expertise and resources
Public-private partnerships	50%	50%	• Due to protection of sensitive data, the collaboration with private CERTs is equally limited	• Tools supporting collaboration between public sector and private sector CERTs need to consider legal restrictions regarding privacy and sensitive information
Information Interface Emergency Services	50%	64%	• The contact to other authorities seems to be stronger for ministry CERTs	• The design should support the information exchange with emergency services for cross-organizational incidents response

As highlighted in Table 5, collaborative features of state CERTs are less developed than organizational and communicative features, achieving rather mediocre scores (avg. 54%-70%). Both ministry and service CERTs indicate that information dissemination is very well or at least moderately developed. It can also be seen that their access to information scores considerably lower, which however could be due to the fact that some tasks are outsourced to other organizational units. Only about half of the CERTs mentioned that they maintain public-private partnerships. However, there are regular and important exchanges and partnerships between ministry and service CERTs in at least two cases, incidents are collaborated on to improve their effectiveness. Coordination competences and information interfaces to emergency services are higher in ministry CERTs, probably due to easier access and exchange with other authoritative units, such as emergency management or police.

5 DISCUSSION AND CONCLUSION

In this paper, we investigated the organizational structures, technology use, and cross-organizational collaboration of German federal and state CERTs. Existing literature on the topic highlighted a lack of empirical research on collaboration among CERTs [51]. Our multi-method empirical study, which comprises semi-structured interviews (N=15) and supplementary document analyses (N=25), provides findings to answer our research question: *How do the organizational structure, technology use, and cross-organizational collaboration contribute to cyber incident response of German state-level CERTs?* In the following, we discuss our findings, implications for design and policy, as well as limitations and opportunities for future work.

5.1 Discussion of Findings

First, in terms of organization, German state CERTs have been established either as part of state ministries or in external service companies. In both cases, their aim is to provide preventative and reactive security measures securing the ICT infrastructures of their respective target groups, such as public administrations, small and medium-sized enterprises, or citizens [54, 55, 83, 88]. Due to the digitalization of the administration (e.g., establishment of e-governments), critical infrastructures and enterprises (e.g., deployment of IoT), and society (e.g., use of mobile devices), their tasks of monitoring, analyzing, communicating, and responding to cyber threats and security incidents are becoming more complex [62]. However, in some state CERTs, a lack of personnel and resources impair a functional division of labor and successful delivery of their services [27]. One issue lies in the competition between state CERTs, which are bound to collective wage agreements, and private sector CERTs that can provide higher wages. This is partly alleviated by an increasing cross-organizational collaboration, involving a multitude of actors, such as other CERTs and IT security appointees in other authorities and organizations. Especially the collaboration among state CERTs, which was established in the VCV network, has been highlighted as the most important aspect of effective incident management.

Second, we saw that CERTs use a variety of *technologies* to support the acquisition, analysis, and reporting of information related to cyber security incidents (Figure 1). As a starting point, incidents are either reported by customers or detected by software. Subsequently, some CERTs use a ticketing and reporting system to collect and analyze evidence for incident response. On the one hand, this evidence is gathered from publicly available data, such as manufacturer websites, security advisories, or social media. On the other hand, further evidence is gathered by collaboration using shared platforms, such as MISP or the VCV. For example, a chat and wiki are used in the VCV to facilitate collaboration between federal and state CERTs. However, the

divergent allocation of resources negatively influences the participation of some CERTs within the chat. Trusting relationships between individuals needs to be supported by a reliable system based on common understandings and practices [34, 49, 83], such as the common use of protocols for confidentially (e.g., traffic light protocol, TLP) of security-relevant information and for documenting cyber threats. Similar to our study, Van der Kleij et al. [51] have found that the communication of threats and "in-depth technical communication" needs more support by formalization and communication tools, which should be supported by threat intelligence standards, such as STIX and MEAC. This is also important because monitoring and diagnosing security threats otherwise often relies on the tacit knowledge of practitioners, which is difficult to share [97]. Such a formalization would support the development of explicit expert knowledge, which in turn would benefit the efficiency of communication between CERTs and external actors [12, 88]. Still, once enough evidence is collected via awareness-focused and collaboration-oriented channels, a report is generated that either provides specific recommendations for a certain stakeholder or general warnings for multiple stakeholders.

Third, the interviews showed that there is strong bilateral collaboration between CERTs, especially between ministry and service CERTs, as their different access to IT services and communication infrastructures can lead to useful exchange of expertise, knowledge, and services. We observed that there are specialized skills in every CERT that are shared within the CERT community using the VCV as a platform. Generally, cooperation between CERTs is organized within the VCV, which is considered essential as it combines the perspectives of ministry and service CERTs, offering added value for all actors and serving as a web of trust. One value that was frequently highlighted is the mutual learning within the VCV; this is in accordance with the suggestion of Ahmad et al. [1] to implement "double-loop learning", which is not only focusing on learning from the individual incidents but also reflecting on systematic corrective actions. This is achieved through mutual support and exchange between state CERTs in the areas of awareness raising, response strategies, and technology, such as anti-phishing campaigns to raise awareness and shared sand boxes to analyze malware. Regular VCV meetings also have a social component, which later forms a basis for collaboration and the use of shared technology for information and service exchange. In the case of ad hoc incident responses, it was pointed out that individual trust and informal contacts, based on formal contacts, are key to a fast and effective response. The federal level, represented by the BSI, has more extensive tasks and competences, including the provision of security-relevant information to state CERTs. In comparison, the BSI's technical and organizational infrastructure is significantly more advanced due to division of labor into separate departments for situational awareness and response capabilities. This feature is used for a distribution of tasks between the federal and the state level that supports the regular monitoring and exchange of threat information. However, the sharing of information between CERTs and non-CERT actors is sometimes limited due to privacy and confidentiality restrictions [96] and different legal frameworks for ministry and service CERTs.

5.2 Implications for Design, Policy, and Research

Based on our key observations and identified challenges, we propose design and policy implications (Table 6) to support the cross-organizational collaboration of German state CERTs and to increase cyber situational awareness [35]. First, we saw that the *organization*, structure, and work processes of CERTs are based on legal regulations and organizational embedding, which shaped different perspectives and service portfolios across CERTs. Thus, when developing ICT, an interoperable and modular architecture to address the different focuses and

services of CERTs should be provided, while still maintaining the extended need for collaboration. From a policy perspective, a shift from loose cooperation towards service level agreements should facilitate the organizational and technological development of work since a lack of liabilities and regulations for daily work in interorganizational exchange was observed.

Second, a variety of different *technologies* and practices for communication among CERTs was observed. While regular meetings were perceived as working measures for collaboration, knowledge sharing, and relationship building, a lack of technology support for analysis and communication became apparent. In order to address these issues, ICT should facilitate a mainly automated but privacy-preserving [40] cross-platform monitoring and analysis of incident data, including blogs, databases, social media, or websites. Moreover, deduplication techniques and standardized threat exchange formats would help to prevent redundant IOCs and to increase efficiency of operations in shared threat intelligence platforms. Third, in terms of *collaboration*, we identified strong bilateral collaborations and delegations of tasks among CERTs but also multilateral coordination in conjunctions with the BSI, CERT-Bund, and VCV. Still, a lack of financial, human, and time resources was identified as a barrier for extensive collaboration and operation. By utilizing the benefits of (semi-)automation of monitoring and reporting processes, functional and useable ICT could help to further alleviate such resource constraints. Furthermore, an asymmetry of information, power, and size across CERTs was identified as a challenge for collaboration. Here, transparent reporting and tool structures could help to enhance awareness and trust among CERTs.

In the past, crisis informatics research has focused on the use of prominent social media, such as Facebook or Twitter. Soden and Palen [84] suggested to broaden the scope of crisis informatics and look "beyond social media", including domains such as participatory mapping. In light of the increasing interconnectedness of real and virtual realms, first, we suggest crisis informatics research to also tackle the issues of cyberattacks, which threaten critical infrastructures and society. Our study highlights the need for intense collaboration between relevant stakeholders to monitor and respond to cyberattacks. Second, it became apparent that besides social media, other open source information based on expert blogs, security advisory feeds, or manufacturer websites are important sources of insight for cyber incident response. In our study, the co-creation of knowledge was implemented in an interplay of establishing cyber situational awareness (e.g., monitoring of available open and social information) and cross-organizational collaboration (e.g., exchange of expertise, provision of shared services, and verification of information).

In terms of situational awareness, crisis informatics leveraged the advent of social media analytics tools designed according to the needs of emergency services [48, 65, 90]. While they are certainly not tailored to the requirements of CERTs and do not account for significance of other OSINT sources, the knowledge created and shared around these tools can be used – in combination with empirical studies such as ours – to inform the design of specific CERT technologies. Our interview participants expressed a positive attitude towards the established cross-organizational collaboration between CERTs. Still, since the above-mentioned technology seems promising to reduce the time strain of daily routine (monitoring) tasks, this would open up further opportunities to conduct other (collaborative) tasks with higher standards of quality. Moreover, tools facilitating the creation and dissemination of reports and warnings could help to improve the collaboration among CERTs and interaction with customers.

Table 6. Summary of observed behaviors, identified challenges, and design or policy implications

	Key observations	Identified challenges	Design or policy implications
Organization	• Organizational structure is driven by federal characteristics, directives, and laws • Embeddings shape different ministry- and technology-focused perspectives	• Lack of standards and regulations for the daily work, which are required to remain sustainable • Lack of liabilities in interorganizational exchange	• Interoperable and modular architecture for different CERT focuses and services • Shift from loose cooperation towards service level agreements
Technology	• Use of a variety of different tools for communication among CERTs • Regular meetings for improved collaboration, knowledge sharing, and relationship building	• Lack of automatization in the monitoring of open, public, or social data • Privacy regulations and data minimization • Communication and reporting redundancies of IOCs	• Privacy-preserving cross-platform monitoring and analysis of incident data • Use of deduplication techniques and standardized threat exchange formats
Collaboration	• Bilateral collaboration and delegation of tasks among CERTs • Coordination of collaborative actions by the BSI and VCV	• Lack of financial, personnel, and time resources • Asymmetry of information, power, and size • Competition between public and private sectors	• Reduction of resource costs by (semi-)automation of monitoring and reporting processes • Transparent reporting and tool structures for trusted information exchange

5.3 Limitations and Future Work

The analysis of the interviews showed that the form and the type of association of CERTs can substantially influence their work. In contrast to the content analysis of official documents, the interviews allowed a different kind of insight into the informal practices of CERTs. The former did not provide information on the networks between the CERTs but only on formal aspects, such as the organizational structure, target group definition, task portfolio, and reporting templates for cyber security incidents. Hence, the part of the analysis that focuses on technology and collaboration strongly relies on information extracted from the interviews. Furthermore, more ministry CERT employees agreed to be interviewed than those from service CERTs. This might have influenced the imbalance between the coding based on the interviews and the documents, causing the higher scores of the ministry CERTs as presented in Tables 2-4. As every CERT has differences regarding its service portfolio and tasks, the comparison might be biased towards the interviewed CERTs as well as towards CERTs with a broader spectrum of tasks and less division of labor. If some tasks, such as the communication of cyber threats, are not realized in CERTs but in a different state organization, this is not reflected in the study design. However, the more resources organizations allocate to incident response, the more

likely they are to change the organization of the division of labor of monitoring, response, and communication. Still, most of the CERTs studied (12 of 14) combined the tasks within the CERT.

When discussing the generalizability of results, several aspects need to be considered. On the one hand, our data is based on an empirical study with German CERTs, which is why we cannot provide a grounded assessment on the situation in other nations. Differences in national capabilities and legislations likely influence the activity, permissions, and privacy-preserving behavior of CERTs [9, 16]. Further in-depth research would be required to compare different analytical technologies (e.g., the degrees of automation and modularity) and collaborative practices (e.g., cooperations or service level agreements) across nations on a fine-grained level. On the other hand, cyber emergency response is a global problem requiring extensive collaboration across CERTs on both national and international level [71, 83]. On average, more than ten CERTs are established per European nation [24], highlighting the necessity for standardized threat intelligence exchange, transparency, and trust among teams. This is further emphasized in international collaboration, which is required in large-scale cyberattacks, such as the 2017 WannaCry ransomware attack that infected over 200,000 victims across 150 countries [7]. Furthermore, the 2021 Microsoft Exchange vulnerabilities have been exploited by a variety of professional criminal groups, and which led to the BSI reaching out directly to 9,000 possibly affected enterprises in Germany [11]. To respond to the professionalization of cyber criminals, CERTs increase their capacities and their interorganizational collaboration. Thus, we assume that our design and policy implications are viable requirements across international CERTs that require different implementations based on national capabilities and legislation. However, in the next step of our national research project, we intend to use the framework of design case studies [99] in order to complement our empirical findings with other stakeholders views and translate them into more fine-grained requirements to iteratively design and evaluate a ICT demonstrator facilitating the data analysis and collaboration practices among state-level CERTs in Germany.

ACKNOWLEDGMENTS

This work was supported by the German Federal Ministry for Education and Research (BMBF) in the projects CYWARN (13N15407) and KontiKat (13N14351), as well as by the BMBF and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. We would like to thank the anonymous reviewers for their valuable and constructive comments.

A DOCUMENTS

Our appendix comprises an overview of analyzed documents, the codebook used for our empirical study, and anonymized CERT scores based on our analysis.

Table 7. Overview of analyzed documents with references (see Section 3)

Name	Doc.-Nr.	Reference	
CERT Berlin	D01-D03	D01:	ITDZ Berlin, "IT Infrastructure: Security, [IT-Infrastruktur: Sicherheit]," 2020.
		D02:	ITDZ Berlin, "Range of services [Leistungsspektrum]," 2020.
		D03:	Committee on Digital Administration Privacy and Freedom of Information [Ausschuss für Digitale Verwaltung Datenschutz und Informationsfreiheit], "Word and Content Record [Wort-und

			Inhaltsprotokoll].” [Online]. Available: https://www.parlament-berlin.de/ados/17/ITDat/protokoll/it17-068-ip.pdf.
CERT-Brandenburg	D04-D06	D04:	Brandenburg IT service provider [Brandenburgischer IT-Dienstleister], “CERT-Brandenburg.” 2020.
		D05:	Land Brandenburg, “Response of the State Government to Minor Inquiry No. 1522 by Dr. Saskia Ludwig, Member of the CDU Parliamentary Group, printed matter 6/3705 [Antwort der Landesregierung auf die Kleine Anfrage Nr. 1522 der Abgeordneten Dr. Saskia Ludwig CDU-Fraktion Drucksache 6/3705].” 2016.
		D06:	Land Brandenburg, “IT Security [IT-Sicherheit].” 2020.
CERT BWL	D07-D10	D07:	State Parliament of Baden-Württemberg [Landtag von Baden-Württemberg], “Statement of the Ministry of the Interior, Digitization and Migration: The so-called cyber defense in the state's security architecture [Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Die sogenannte Cyberwehr in der Sicherheitsarchitektur des Landes],” 2017.
		D08:	State Parliament of Baden-Württemberg [Landtag von Baden-Württemberg], “Statement by the Ministry of the Interior, Digitization and Migration: Prevention and Detection of Cybercrime [Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten],” 2019.
		D09:	Cyberwehr, “Cyberwehr – Homepage [Cyberwehr – Startseite],” 2020.
		D10:	Cyberwehr, “Impressum Cyberwehr,” 2020.
CERT M-V	D11-D13	D11:	Ministry of the Interior and Sports [Ministerium für Inneres und Sport], “IS Guideline M-V: Guideline for Ensuring Information Security in the State Administration of Mecklenburg-Pomerania [IS-Leitlinie M-V: Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern],” May 2014.
		D12:	DVZ M-V, “IT Security [IT-Sicherheit].” .
		D13:	CERT M-V, “Description according to RFC 2350 [Beschreibung nach RFC 2350].” 2020.
CERT Nord	D14, D15	D14:	CERT Nord, “CERT Nord.” 2020.
		D15	Saxony-Anhalt State Parliament [Landtag von Sachsen-Anhalt], “Minor Inquiry - KA 7/1554: Attacks on information technology and the data network of the state of Saxony-Anhalt [Kleine Anfrage - KA 7/1554: Angriffe auf die Informationstechnik und das Datennetzwerk des Landes Sachsen -Anhalt].” Apr. 2018.
CERT NRW	D16-D19	D16:	State company IT.NRW [Landesbetrieb IT.NRW], “Information Security for the State Administration of North Rhine-Westphalia [Informationssicherheit für die Landesverwaltung NRW].” 2020.
		D17:	WIRTSCHAFT.NRW, “Security in Information Technology [Sicherheit in der Informationstechnik].” 2020.
		D18:	D. and E. of the L. N.-W. Ministry of Economy, Innovation [D. und E. des L. N.-W. Ministerium für Wirtschaft, Innovation], “Meeting of the Digitization and Innovation Committee on March 15, 2018 [Sitzung des Ausschusses für Digitalisierung und Innovation am 15. März 2018].” 2018.
		D19:	CERT NRW, “Responsible Disclosure Policy CERT NRW.” 2016.
SAX.CERT	D20-D23	D20:	SAX.CERT, “Vulnerability Advisory Service,” 2020.
		D21:	SAX.CERT, “Cooperations [Kooperationen],” 2020.
		D22:	SAX.CERT, “Description according to RFC 2350 [Beschreibung nach RFC 2350].” Feb. 2020.
		D23:	Freistaat Sachsen, “Minor Inquiry of the Member of Parliament Valentin Lippmann, Parliamentary Group BÜNDNIS 90/DIE GRÜNEN: Hacker Attacks at Saxony's Police and Office for the Protection of the Constitution [Kleine Anfrage des Abgeordneten

			Valentin Lippmann, Fraktion BÜNDNIS 90/DIE GRÜNEN: Hackerangriffe bei Sachsens Polizei und Verfassungsschutz],” 2016.
ThüringenCERT	D24, D25	D24:	Freistaat Thüringen, “Not without protection: Information Security Thuringia CERT [Nicht ohne Schutz: Informationssicherheit Thüringen CERT],” 2018.
		D25:	Freistaat Thüringen, “ThüringenCERT Description according to RFC 2350 [Beschreibung nach RFC 2350],” Aug. 2019.

B CODEBOOK

Table 8. Codebook with categories, definitions, examples, and coding rules

Category	Definition	Example	Coding rule
CERT association member (VCV)	The CERT is part of the VCV and operates within and through it with other CERTs. The CERT enters into confidentiality agreements with external partners	"With external communication partners, such as municipalities, we handle things differently; we have them sign confidentiality agreements and then file them accordingly.” (I01)	1 = Part of a cross-CERT alliance 0.5 = Cooperation with cross-institutional networks, but no overarching institutionalization 0 = No institutionalization exists, the CERT primarily acts alone without cross-organizational structures.
Defined protocols for cross-organizational communication (such as TLP)	The work of the CERT is regulated by predefined protocols that determine and influence its working process	“So, it is assumed that every information that is passed on in written form in the VCV is also classified according to TLP. So that's how it's handled by default." (I01)	1 = The CERT operates on the basis of predefined protocols that regulate its work process. TLP are classified 0.5 = The CERT works and operates on the basis of customary rules that govern its work process, but does not explicitly operate on the basis of protocols 0 = There is no evidence of protocols regulating the work process
Distinct target group definition for incident reporting	The CERT works and interacts with a previously defined target group/ works in a target group-specific way Target groups: State administration, municipal administration, Citizens, Companies /CI operators	"There are with us, we have different target groups, our primary target group is the state administration, meanwhile also more or less the municipal administration [...]" (I01)	1 = The CERT works with many target groups and acts in accordance with their specific needs 0.5 = There are recurring groups that the CERT addresses, but no specifically defined target groups 0 = The CERT does not have defined target groups

Use of exchange platforms	The CERT participates in the exchange of information There is a central exchange platform for the different CERTs The CERT participates in exchange meetings of the VCV	"We have different types of communication, we have regular working meetings with the entire administrative CERT network and all the state CERTs plus the federal CERT meet at least twice a year and exchange information with presentations and workshops on specialist topics. We talk on the phone regularly, we exchange e-mails regularly, we have set up a wiki where we exchange information, exchange documents, across states." (I01)	1 = The CERT is part of various exchange platforms and communication channels as well as exchange meetings through which it stays informed about current developments, topics, etc. and can exchange ideas and information 0.5 = Exchange happens mostly within the CERT, mostly in-house platforms are used 0 = The CERT is not part of any exchange platforms
Alerting and reporting service	The CERT prepares and forwards status and vulnerability reports on the current cyber situation The CERT forwards alert messages to affected entities The CERT forwards notifications of acute security vulnerabilities to affected entities and provides advice	"[...] Situation reports and vulnerability reports daily and also this new cyber situation report which is only a leadership information, that is such a Din A4 page in horizontal format, where also with traffic light colors is represented, how the situation presents itself from the point of view of the cyber security area of Hessen3C just for this day, also divided into Hessian municipalities, Hessian State administration Internet etc." (I01)	1 = The CERT is responsible for writing status and vulnerability reports on the cyber situation and sending security alerts to affected entities 0.5 = CERT forwards specific security alerts to affected entities 0 = CERT is not responsible for security alerts
Advisory service	The CERT provides advice to public authorities, citizens, private companies, politicians and members of parliament In the case of acute alerts, the CERT provides advice to the affected parties The role of CERT is to provide information and advice.	"Yes, we have a broad block of recommendations that we give to external parties, we create various products for our customers. These are, on the one hand, a situation report, a vulnerability report and, more recently, a cyber situation report, where we try to provide information for different levels in a way that is appropriate to the target group and the client, I would say." (I01)	1 = The CERT advises all (authorities, citizens, (private sector) companies, politicians/members of parliament (3/3)) 0.5 = The CERT does not provide advice to all stakeholders 0 = The CERT does not have an advisory function
Information access	The CERT collects information from various sources The CERT monitors compliance with the confidentiality requested by information providers	"The CERT is notified, usually by telephone or by e-mail, which is still here within the state administration. In general, these are the two media that are used 99.9% of the time. We can also be reached by fax, but that is not really used anymore these days. For very serious matters, there is of course also a cryptofax." (I01)	1 = The CERT has access to information via various sources and works closely with its partners; there are clearly defined rules for obtaining information, it monitors and receives information (active access) 0.5 = The CERT is neither active nor passive 0 = There is no clear access to information and information gathering is not clearly regulated

Coordination competence	The CERT distributes tasks among other CERTs on the accordance of different competences (based on experience) Tasks are distributed among the CERTs inter alia by the VCV	"In any case, and it's also the case that between the states, as I said, cooperation is also now being pushed by the BSI, they of course also want to relieve themselves, because all the states approach the BSI and say advice please, here and there and because of this tool and that tool and they are then overwhelmed, even if they have a lot of staff, but the states are not their only cooperation partner. And that's why we in the VCV are trying to coordinate with our colleagues from the federal states before we go to the BSI and ask them." (I01)	1 = The CERT is part of a clearly defined competence distribution strategy, e.g., within the framework of the VCV, and actively participates in the coordination of tasks, e.g., in the event of an incident 0 = The CERT does not participate in any distribution of competencies but works only for itself
Public-private partnerships	The CERT cooperates with external entities/private companies CERT commissions companies for the (technical) execution of tasks	"[...] because there are also many data that you don't want to give to the external e.g., if we now come from the political area or from the management area, it is always very difficult to work together with external parties, that is also always a trust issue." (I01)	1 = The CERT works explicitly with external or private-sector entities and outsources the technical execution of tasks 0.5 = The CERT accepts requests from the private sector, but does not work together with them in the sense of cooperation and division of competencies 0 = The CERT operates only in a government context and has no connections to the private sector.
Information Interface ES	The CERT takes on a connecting and a separating role by advising and mediating between agencies The CERT liaises with other ES	"For us, however, it is important that the cyber security and CERT department is of course not an agency of the police or the Federal Office for the Protection of the Constitution, even if we cooperate with them. In fact, we have completely different tasks; we want to carry out technical analyses. We don't do forensics, even if some slides say so. [...]" (I01)	1 = The CERT operates in an intentionally embedded connecting role with other ES such as the Federal Office for the Protection of the Constitution and the police 0.5 = In individual cases, the CERT may cooperate with organizations such as the Federal Office for the Protection of the Constitution or the police, but it does not have a permanent role in them 0 = The CERT works completely independently of other agencies such as the police or the Federal Office for the Protection of the Constitution and has no connection whatsoever with them

C LIST OF ACRONYMS

Table 9. Overview of Acronyms

Acronym	Description
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CERT	Computer Emergency Response Team
CRSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
OSINT	Open Source Intelligence

SME	Small and Medium-Sized Enterprise
TLP	Traffic Light Protocol
VCV	Verwaltungs-CERT-Verbund (Administrative CERT Network)

REFERENCES

[1] 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.

[2] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers and Security*, 74, 144–166. DOI: 10.1016/j.cose.2018.01.001.

[3] 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.

[4] Arbeitsgruppe Kritische Infrastrukturen. 2020. The Cyber Relief Agency: Concept for Increasing the Response Capabilities in Major Cyber Incidents. , 1–33.

[5] Michael Aupetit and Muhammad Imran. 2017. Interactive monitoring of critical situational information on social media. In *Proceedings of the International Conference on Information Systems for Crisis Response and Management (ISCRAM)*. , 673–683.

[6] Riza Azmi, William Tibben, and Khin Than Win. 2016. Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. *ACIS 2016 Proceedings*.

[7] Maria Bada and Jason R. C. Nurse. 2020. Chapter 4 - The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*. Vladlena Benson and John Mcalaney (Eds.). Academic Press, 73–92. DOI: https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

[8] 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.

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

[10] BSI. 2020. Die Lage der IT-Sicherheit in Deutschland 2019. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7.

[11] BSI. 2021. BSI warnt: Kritische Schwachstellen in Exchange-Servern., *Press Release*. Retrieved from: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html;jsessionid=DE068173A2E227CE673422F7675FB3FE.internet481?nn=893136.

[12] Norbou Buchler, Prashanth Rajivanb, Laura R. Marusicha, Lewis Lightnerc, and Cleotilde Gonzalezb. 2018. Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition. *Computers & Security*, 73, March, 114–136. DOI: 10.1016/j.cose.2017.10.013.

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

[14] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. 2012. NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide Recommendations. *NIST Special Publication*, . DOI: 10.6028/NIST.SP.800-61r2.

[15] Camille Cobb, Ted McCarthy, Annuska Perkins, Ankitha Bharadwaj, Jared Comis, Brian Do, and Kate Starbird. 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)*, Baltimore, USA, USA, 888–899. DOI: 10.1145/2531602.2531712.

[16] 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.). Springer International Publishing, Basel, 187–212. DOI: 10.1007/978-3-319-45300-2_9.

[17] 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.

[18] 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. RAND Corporation.

[19] Lise Ann St. Denis, Amanda Lee Hughes, and Leysia Palen. 2012. Trial by Fire: The Deployment of Trusted Digital Volunteers in the 2011 Shadow Lake Fire. In *Proceedings of the International Conference on Information Systems for Crisis Response and Management (ISCRAM)*. L. Rothkrantz, J. Ristvej, and Z. Franco (Eds.). ISCRAM, Vancouver, Canada, 1–10.

[20] Deutscher Bundestag. 2009. Gesetz zur Änderung des Grundgesetzes (Artikel 91c, 91d, 104b, 109, 109a, 115, 143d). Berlin. Retrived from: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/ITPlanungsrat/Staatsvertrag/Gesetz_zur_Aenderung_des_Grundgeset

zes.pdf?__blob=publicationFile&v=5.
[21] 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.
[22] Jesse M. Ehrenfeld. 2017. WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems*, 41, 7, 10916. DOI: 10.1007/s10916-017-0752-1.
[23] ENISA. 2018. Cyber Europe 2018: After Action Report. December. DOI: 10.2824/369640. Retrived from: https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report.
[24] ENISA. 2021. CSIRTs by Country - Interactive Map. Retrived from: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.
[25] 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.
[26] Federal Office for Information Security. 2019. The State of IT Security in Germany 2018., *IT-Security Situation*. Retrieved from: https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html.
[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*, 104, 102229. DOI: 10.1016/j.cose.2021.102229.
[28] Ulrik Franke and Joel Brynielsson. 2014. Cyber situational awareness - A systematic review of the literature. *Computers and Security* 46, 18–31. Elsevier Ltd, , 18–31. DOI: 10.1016/j.cose.2014.06.008.
[29] Kira Gedris, Kayla Bowman, Aatish Neupane, Amanda Lee Hughes, Elizabeth Bonsignore, Ryan W. West, Jon Balzotti, and Derek L. Hansen. 2021. Simulating Municipal Cybersecurity Incidents: Recommendations from Expert Interviews Kira. In *Proceedings of the 54th Hawaii International Conference on System Sciences 2021.* , 2036–2045.
[30] Jochen Gläser and Grit Laudel. 2010. *Experteninterviews und qualitative Inhaltsanalyse*. VS Verlag für Sozialwissenschaften, Wiesbaden.
[31] Annemijn F. van Gorp. 2014. Integration of Volunteer and Technical Communities into the Humanitarian Aid Sector: Barriers to Collaboration. In *Proceedings of the International Conference on Information Systems for Crisis Response and Management (ISCRAM)* , May. , 620–629.
[32] George Grispos, William Glisson, and Tim Storer. 2019. How Good is Your Data? Investigating the Quality of Data Generated During Security Incident Response Investigations. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 6, 7156–7165. DOI: 10.24251/hicss.2019.859.
[33] 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.
[34] Otto Hellwig. 2015. Organisation, Rahmenbedingungen und Kommunikation bei CERTs. In *Sicherheit in Cyber-Netzwerken*. Edith Huber (Ed.). Springer VS, Wiesbaden, 559–574.
[35] Alan R. Hevner. 2007. A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, 19, 2, 87–92. DOI: http://aisel.aisnet.org/sjis/vol19/iss2/4.
[36] Starr Roxanne Hiltz, Amanda Lee Hughes, Muhammad Imran, Linda Plotnick, Robert Power, and Murray Turoff. 2020. Exploring the usefulness and feasibility of software requirements for social media use in emergency management. *International Journal of Disaster Risk Reduction (IJDDR)*, 42, January, 101367. DOI: 10.1016/j.ijdrr.2019.101367.
[37] Cathrine Hove, Marte Tarnes, Maria B. Line, and Karin Bernsmed. 2014. Information security incident management: Identified practice in large organizations. *Proceedings - 8th International Conference on IT Security Incident Management and IT Forensics, IMF 2014*, , 27–46. DOI: 10.1109/IMF.2014.9.
[38] Edith Huber. 2015. *Sicherheit in Cyber-Netzwerken*. Springer Fachmedien Wiesbaden, Wiesbaden.
[39] Muhammad Imran, Carlos Castillo, Fernando Diaz, and Sarah Vieweg. 2015. *Processing Social Media Messages in Mass Emergency: A Survey* 47, 4. ACM, New York, NY DOI: 10.1145/2771588.
[40] Muhammad Imran, Patrick Meier, and Kees Boersma. 2018. The use of social media for crisis management: a privacy by design approach. In *Big Data, Surveillance and Crisis Management*. Routledge.
[41] 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.
[42] IT-Planungsrat. 2013. Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung- Hauptdokument. Retrived from: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html. [43] IT-Planungsrat. 2016. Kooperation der CERTs im Verwaltungs-CERT-Verbund (VCV). Berlin. Retrived from: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Fachkongress/4FK2016/2Mai_FI_Cybersicherheit_01-1_VCV.pdf?__blob=publicationFile&v=2.
[44] Robert Kaiser. 2014. *Qualitative Experteninterviews. Konzeptionelle Grundlagen und praktische Durchführung*. Springer VS, Wiesbaden DOI: http://dx.doi.org/10.1007/978-3-658-02479-6.
[45] Hanna Kallio, Anna Maija Pietilä, Martin Johnson, and Mari Kangasniemi. 2016. Systematic methodological

review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72, 12, 2954–2965. DOI: 10.1111/jan.13031.

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

[47] Marc-André Kaufhold et al. 2021. CYWARN: Strategy and Technology Development for Cross-Platform Cyber Situational Awareness and Actor-Specific Cyber Threat Communication. In *Workshop-Proceedings Mensch und Computer 2021.* , 1–9.

[48] Marc-André Kaufhold, Nicola Rupp, Christian Reuter, and Matthias Habdank. 2019. 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.

[49] 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*. ACM Press, New York, New York, USA, 38. DOI: 10.1145/1527017.1527023.

[50] 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.

[51] 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.

[52] 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 (CSCW)*, 2. DOI: 10.1145/3274361.

[53] Farzan Kolini and Lech Janczewski. 2017. Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies. *PACIS 2017 Proceedings*.

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

[55] Klaus-Peter Kossakowski and Caroline Neufert. 2012. CERT-Dienstleistungen für Land und Kommunen in Hessen. Wiesbaden.

[56] 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.

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

[58] 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.

[59] Philipp Mayring. 2000. Qualitative Content Analysis. *Forum: Qualitative Social Research*, 1, 2.

[60] D. Mendonca, G. E. Beroggi, and W. A. Wallace. 2001. Decision support for improvisation during emergency response operations. *International journal of emergency management*, 1, 1, 30–38.

[61] 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.

[62] Sarandis Mitropoulos, Dimitrios Patsos, and Christos Douligeris. 2006. On Incident Handling and Response: A state-of-the-art approach. *Computers and Security*, 25, 5, 351–370. DOI: 10.1016/j.cose.2005.09.006.

[63] NIS Directive. 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *OJ L*, 194, 19.7, 2016. Retrived from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.

[64] 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*. ACM, New York, USA, 994–1009. DOI: 10.1145/2675133.2675242.

[65] Teresa Onorati, Paloma Díaz, and Belen Carrion. 2018. From social networks to emergency operation centers: A semantic visualization approach. *Future Generation Computer Systems*, . DOI: 10.1016/j.future.2018.01.052.

[66] 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.

[67] Leysia Palen and Kenneth M. Anderson. 2016. Crisis informatics: New data for extraordinary times. *Science*, 353, 6296, 224–225.

[68] Spyridon Papastergiou, Haralambos Mouratidis, and Eleni Maria Kalogeraki. 2019. Cyber security incident handling, warning and response system for the european critical information infrastructures (cyberSANE). *Communications in Computer and Information Science*, 1000, 476–487. DOI: 10.1007/978-3-030-20257-6_41.

[69] Theresa A. Pardo, Anthony M. Cresswell, Sharon S. Dawes, and G. Brian Burke. 2004. Modeling the social & technical processes of interorganizational information integration. *Proceedings of the Hawaii International Conference on System Sciences*, 37, C, 1905–1912. DOI: 10.1109/hicss.2004.1265307.

[70] Theresa A. Pardo, Anthony M. Cresswell, Fiona Thompson, and Jing Zhang. 2006. Knowledge sharing in cross-boundary information system development in the public sector. *Information Technology and Management*, 7, 4, 293–313. DOI: 10.1007/s10799-006-0278-6.

[71] Richard D. Pethia and Kenneth R. van Wyk. 1990. Computer Emergency Response - An International Problem. Pittsburgh, Pa.: CERT Coordination Center., Software Engineering Institute, Carnegie Mellon University.

[72] Gabriel Pimenta Rodrigues, Robson de Oliveira Albuquerque, Flávio Gomes de Deus, Rafael de Sousa Jr., Gildásio de Oliveira Júnior, Luis García Villalba, and Tai-Hoon Kim. 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.

[73] 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.

[74] Christian Reuter, Oliver Heger, and Volkmar Pipek. 2013. Combining Real and Virtual Volunteers through Social Media. In *Proceedings of the International Conference on Information Systems for Crisis Response and Management (ISCRAM)*. T. Comes, F. Fiedrich, S. Fortier, J. Geldermann, and Tim Müller (Eds.). , Baden-Baden, Germany, Germany, 780–790. DOI: 10.1126/science.1060143.

[75] Christian Reuter, Amanda Lee Hughes, and Marc-André Kaufhold. 2018. Social Media in Crisis Management: An Evaluation and Analysis of Crisis Informatics Research. *International Journal on Human-Computer Interaction (IJHCI)*, 34, 4, 280–294. DOI: 10.1080/10447318.2018.1427832.

[76] 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.

[77] Christian Reuter, Marc-André Kaufhold, Thomas Spielhofer, and Anna Sophie Hahne. 2017. Social Media in Emergencies: A Representative Study on Citizens' Perception in Germany. *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing*, 1, 2, 1–19. DOI: 10.1145/3134725.

[78] 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.

[79] 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.

[80] Wendy A. Schafer, Craig H. Ganoe, and John M. Carroll. 2007. Supporting Community Emergency Management Planning through a Geocollaboration Software Architecture. *Computer Supported Cooperative Work (CSCW)*, 16, 4–5, 501–537. DOI: 10.1007/s10606-007-9050-7.

[81] Giuseppe Settanni, Florian Skopik, Yegor Shovgenya, and Roman Fiedler. 2016. A collaborative analysis system for cross-organization cyber incident handling. *ICISSP 2016 - Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, , Icissp, 105–116. DOI: 10.5220/0005688301050116.

[82] 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*, 60, 154–176. DOI: 10.1016/j.cose.2016.04.003.

[83] 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.

[84] Robert Soden and Leysia Palen. 2018. Informating Crisis: Expanding Critical Perspectives in Crisis Informatics. In *Proceedings of the ACM on Human-Computer Interaction* 2. , 1–22.

[85] Kate Starbird and Leysia Palen. 2011. Voluntweeters: Self-Organizing by Digital Volunteers in Times of Crisis. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM-Press, Vancouver, Canada.

[86] 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)*. .

[87] Stiftung Neue Verantwortung. 2019. Staatliche Cyber-Sicherheitsarchitektur Version 3, 4. Retrived from: https://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur9.pdf.

[88] Sathya Chandran Sundaramurthy, John McHugh, Xinming Simon Ou, S. Raj Rajagopalan, and Michael Wesch. 2014. An anthropological approach to studying CSIRTs. *IEEE Security and Privacy*, 12, 5, 52–60. DOI: 10.1109/MSP.2014.84.

[89] Techtarget Network. computer security incident response team (CSIRT). Retrieved from: https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT.

[90] Dennis Thom, Robert Krüger, and Thomas Ertl. 2016. Can twitter save lives? A broad-scale study on visual social media analytics for public safety. *IEEE Transactions on Visualization and Computer Graphics*, 22, 7, 1816–1829. DOI: 10.1109/TVCG.2015.2511733.

[91] 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.

[92] Sarah Vieweg, Amanda L. Hughes, Kate Starbird, and Leysia Palen. 2010. Microblogging during two natural hazards events. *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, , 1079. DOI: 10.1145/1753326.1753486.

[93] Sarah Vieweg, Amanda Lee Hughes, Kate Starbird, and Leysia Palen. 2010. Microblogging During Two Natural Hazards Events: What Twitter May Contribute to Situational Awareness. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, Atlanta, USA, 1079–1088.

[94] Julián Villodre and J. Ignacio Criado. 2020. User roles for emergency management in social media: Understanding actors' behavior during the 2018 Majorca Island flash floods. *Government Information Quarterly*, 37, 4, 101521. DOI: 10.1016/j.giq.2020.101521.
[95] James R. Wallace, Saba Oji, and Craig Anslow. 2017. Technologies, methods, and values: Changes in empirical research at CSCW 1990 - 2015. *Proceedings of the ACM on Human-Computer Interaction*, 1, CSCW. DOI: 10.1145/3134741.
[96] Michael Weatherseed. 2018. Being More Effective Through Information Sharing and Cooperation. In *Cybersecurity Best Practices*. Michael Bartsch and Stefanie Frey (Eds.). Springer Vieweg, Wiesbaden, 517–521. DOI: https://doi.org/10.1007/978-3-658-21655-9_5.
[97] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2010. Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management and Computer Security*, 18, 1, 26–42. DOI: 10.1108/09685221011035241.
[98] Johannes Wiik, Jose J. Gonzalez, and Klaus-Peter Kossakowski. 2006. Effectiveness of Proactive CSIRT Services. *FIRST Conference*, , 2–11.
[99] 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)*. ACM Press, Hangzhou, China, 505–512.
[100] Himanshu Zade, Kushal Shah, Vaibhavi Rangarajan, Priyanka Kshirsagar, Muhammad Imran, and Kate Starbird. 2018. From Situational Awareness to Actionability: Towards Improving the Utility of Social Media Data for Crisis Response. *Proceedings of the ACM on Human-Computer Interaction*, 2, November.
[101] Florian Skopik, Timea Pahi, and Maria Leitner, Eds. 2018. *Cyber Situational Awareness in Public-Private-Partnerships*. Springer Vieweg, Berlin DOI: 10.1007/978-3-662-56084-6.
[102] 2021. German CERT Association (Deutscher CERT-Verbnd). Retrieved from: https://www.cert-verbund.de/index.html.

Received April 2021; accepted July 2021.