The Implementation of Protective Measures and Communication of Cybersecurity Alerts in Germany - A Representative Survey of the Population

Marc-André Kaufhold
Julian Bäumler
Christian Reuter
Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC)
Darmstadt, Germany
{kaufhold,reuter}@peasec.tu-darmstadt.de
julian.baeumler@stud.tu-darmstadt.de

ABSTRACT

Despite the merits of digitization in private and professional spaces, critical infrastructures and societies are increasingly exposed to cyberattacks. We conducted a representative survey with German citizens (N=1,093) to examine how they assess the current and future cyber threat situation as well as possible protective measures in cyberspace. Furthermore, we asked what information and channels citizens need to be aware of cyber threats. Our findings indicate that large proportions of the German population feel inadequately informed about cyber threats and tend to only apply enforced security measures by programs (e.g., updates) and services (e.g., two-factor authentication). Furthermore, institutions such as state-level Computer Emergency Response Teams (CERTs) are relatively unknown among the population and respondents showed little confidence in German security authorities to cope with large-scale attacks and ultimately protect citizens. Still, our participants prefer to receive cybersecurity information via installed security applications, television channels, or emergency warning apps.

KEYWORDS

cyberthreat awareness, cybersecurity behavior, cybercrisis management, population warning, human-computer interaction

1 INTRODUCTION

Research into human-computer interaction (HCI) has driven the domain of crisis informatics, which is a multidisciplinary field "concerned with the ways in which information systems are entangled with socio-behavioral phenomena connected to disasters" [51, p. 2]. Despite acknowledging the impact of human-induced emergencies, most research so far has focused on collective and individual behavior in natural disasters [42, 46] and the use of social media in the context of crisis response [36, 56]. However, driven by the increasing digitization and interconnectedness of society, but also the growing frequency and professionalism of cyberattacks, citizens and states are faced with a multitude of challenges in both the physical and virtual realm [14]. This has been brought back to public attention not least by the 2015 Ukraine power grid attack, resulting in 225,000 people without electricity for a period from one to six hours [13], the 2017 WannaCry ransomware, which infected over 230,000 computers in over 150 countries [1], or the 2018/19 doxing of German politicians, journalists, and celebrities [7].

Such cyberattacks pose an increasing threat to socio-cultural infrastructures, as they can cause a breakdown of important social communication channels, the disclosure of personal data, and the failure of critical infrastructures [46, 50]. As a consequence, Computer Emergency Response Teams (CERTs) were established "to handle defence against cyber attacks, respond to IT security incidents and implement preventive measures" [19] across the German federal system, providing cybersecurity reports for ministries, consulting small- and medium-sized enterprises with regard to security incidents, or providing information on how to better protect against cyber threats for citizens.

Since Germany is considered a state-oriented risk culture, citizens' trust in state authorities is high and they are expected to prevent and manage incidents [47]. Moreover, citizens often show little knowledge and awareness of coping mechanisms and have a low confidence in their respective individual capabilities [12]. However, the general cyber threat perception, self-assessment of cybersecurity competence, and assessment of the state's cybersecurity competence have so far been surveyed only fragmentary in Germany. As the findings of such surveys might be an important building block to design and evaluate both guidelines and strategies enhancing citizens' preparedness and response to cyberthreats [33], we seek to answer the following research questions:

- How do German citizens assess the current and future threat situation and possible protective measures in cyberspace?
- What information and channels do German citizens need to be aware of cyber threats now and in the future?

This paper will present related work on the cybersecurity attitudes and behavior of German citizens (Section 2) before introducing the method consisting of survey design, questionnaire, data collection, and analysis (Section 3). Then, it will present the descriptive results of our representative survey (N=1,093) with German

Veröffentlicht durch die Gesellschaft für Informatik e.V.
in K. Marky, U. Grünefeld & T. Kosch (Hrsg.):
Mensch und Computer 2022 – Workshopband, 04.-07. September 2022, Darmstadt

https://doi.org/10.18420/muc2022-mci-ws01-228

citizens (Section 4). Finally it will discuss major findings in differentiation to similar surveys as well as from the perspectives of citizen behavior, information channels and types, and the visibility of and trust in German authorities (Section 5), before concluding with a summary of findings, limitations, and future work (Section 6).

2 RELATED WORK

2.1 Adapting Crisis Informatics Research to the Cybersecurity 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 [53, 56, 57], collection, processing, and refinement of social media data [2, 11, 32], system design and evaluation [3, 36, 43], as well as cumulative and longitudinal research [27, 42, 46]. 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 [42], only little domain-specific research considers the anthropogenic risks of cyberattacks [20]. 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 in response to cyber threats [26, 50]. Since CERTs are confronted with similar issues when analyzing open and social data, including information quality and information overload [45], it seems sensible to examine the adaptability of findings from crisis informatics to cybersecurity.

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 [48, 53]. 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 [52]. In the following years, VOSTs were deployed across the globe to assist emergency services by crowdsourcing emergency-related tasks [15]. This concept is also becoming more interesting for the domain of cybersecurity: 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 [28]. In terms of crisis communication, citizens increasingly use general-purpose social media and specialized warning apps during natural disasters [47, 54]. As a recent survey with German citizens highlights their interest in receiving warnings on anthropogenic risks (e.g., cybercrime) via warning apps [35], it seems worthwhile to examine the use of new media for cybersecurity warnings.

2.2 The Cybersecurity Attitudes and Behaviour of German Citizens

The attitudes and behavior of the German population with regard to cybersecurity and cybercrime have already been investigated in the context of several quantitative studies. In the state of Saxony, the research institute Forsa surveyed 1,000 people by phone in 2017 on behalf of the State Ministry of the Interior about their individual cybersecurity perceptions [17]. According to this study, 92% of Saxon Internet users believe that complete protection against cybercrime is impossible. At the same time, however, 69% of respondents feel sufficiently informed about protective measures against cybersecurity threats, while 28% would like to see extended information services, especially on secure internet usage, cybercrime and hacking, virus warnings, and securing data.

In an 2019 European Commission survey on attitudes towards cybercrime 27,607 citizens, 1,506 of them in Germany, were interviewed face-to-face [31]. Due to privacy and security concerns, 93% of EU-wide respondents state that they have changed their behavior, most frequently by opening emails exclusively from known contacts, using antivirus software, accessing only known and trusted websites, and using only own devices. While 56% of respondents in Germany claim to be well informed about cybercrime, 79% believe that the risk of falling victim is increasing. However, only slightly more than half of those surveyed (52%) believe they are can protect themselves adequately. Furthermore, it should be emphasized that four-fifths of the Germans surveyed are not aware of any official channel for reporting cybercrime or illegal online behavior.

Another survey was conducted in 2019 by Bitkom, the German industry association for the information and telecommunications sector, in which 1,225 people were questioned via phone about threat perceptions on the Internet and implemented protective measures [5]. The most significant perceived threats were malware (79%), misuse of personal data (70%), password and account theft (54%), data espionage (45%), and online banking fraud (30%). 35% of those surveyed indicated that they inform themselves about the security of devices before purchasing them; Friends and acquaintances (52%), manufacturer websites (36%), specialist stores (35%), and online customer reviews (20 %) were the most popular sources.

In April 2020, an online survey with 2,000 citizens about attitudes, experiences, and knowledge in the context of cybersecurity has been conducted on behalf of German federal authorities [6]. A quarter of respondents revealed that they already fell victim to cybercrime, most frequently by online shopping fraud (44%), unauthorized third-party access to online accounts (30%), phishing (17%), and malware (11%). When protective measures against cyber threats were implemented, the most common were antivirus programs (57%), strong passwords (48%), up-to-date firewalls (47%), and the use of two-factor authentication (33%). However, only one in ten actively follows recent security recommendations, while roughly half have already noticed them (55%) and nearly one-third (29%) have never consciously noticed them. In addition, a quarter of respondents stated that they never inform themselves about cybersecurity. People who do obtain information most often do so via computer and technology websites (35%), friends and acquaintances (33%), search engines (28%), and specialized journals (22%). In terms of information services, half of those already affected by cybercrime would like to be provided with a checklist on how to react in case of an emergency, and one third would like consultation services from the police, especially with regard to cyberbullying, cyberstalking, and online fraud.

Finally, in December 2019, the Federal Ministry of the Interior and the Federal Office for Information Security surveyed 20,001 people online about information or support requirements in specific

thematic cybersecurity areas [8]. It was found that 72% of respondents would like support or information in at least one of the areas. Online and mobile banking (35%), protection of end user devices (24%), protection of the smarthome (18%), and the secure use of online accounts (17%) and social networks (17%) were mentioned most frequently.

3 METHOD

3.1 Questionnaire Design

We conducted two creative workshops following the approach of [23] to design and refine the questionnaire. The approach was chosen to facilitate individual creativity (i.e., reflection phase) before a process of collective creativity (i.e., presentation and discussion phases) could influence individual ideas and thoughts [39]. Both workshops involved four cybersecurity practitioners from German state CERTs (team leader, incident manager, information security officer, and public safety answer point employee) and four interdisciplinary researchers (digital humanities, HCI, IT security, and political science). In a first workshop, we introduced the procedure for conducting a representative survey and the objective to generate a questionnaire. Then, we conducted a reflection phase where participants were instructed to note ideas or questions on a digital board. The workshop was closed with a presentation phase where participants presented their ideas and we subsequently arranged them thematically on the board. Based on this, we created a preliminary version of the questionnaire by translating loose ideas into questions and related items, refining existing questions, and grouping them into the three emerging categories of (1) cybersecurity behavior and perception, (2) open-source intelligence, as well as (3) communication of cyberthreats.

Later, we presented the questionnaire in a second workshops where participants discussed and refined existing questions and their items, generated new ones, and reflected upon their thematic grouping or relevance for the research project. Based on the inputs, we created a second draft of the questionnaire and distributed it via email to the participants for a final round of feedback, before we conducted a pre-test with 10 persons. During the rounds of feedback and pre-test, we focused on identifying terminology that may be incomprehensible to non-experts, as well as potential causes of response bias. This led to a final revision of the questionnaire in which, e.g., the terms for less known attack types, such as DDoS, doxing, or social engineering, were supplemented with explanations.

In the questionnaire (see Appendix), we obtain the consent for participation (Q1) and asked for the demographic variables of age, gender, education, region, and income (Q2-Q6). To answer RQ1, participants were asked on general perceptions of cyber threats (Q8), how familiar they are with cybersecurity institutions in Germany (Q9), how often they fell victim to specific cyberattacks in the past five years (Q10), how they estimate the risk of falling victim to different cyberattacks in the next five years (Q12), and how often they use security tools or measures on personal devices (Q13). While the questions on threat perception, cyber attack exposure, and risk estimation aim to collect data on the assessment of the current and future threat situation, the other two questions are designed to quantify the knowledge about and the assessment of protective measures and cybersecurity institutions. For RQ2, we asked participants on their use of internet devices (Q7), which channels they currently use to find cyber threat information (Q16), and which channels they would prefer in the future (Q17). Moreover, we asked which information types are particularly important (Q18). Data on the devices used and relevant information types allows an assessment of the current and future information needs of citizens, while the other two questions serve to identify suitable information channels for communicating these issues.

The full questionnaire included additional questions (Q11, Q14, Q15, Q19). Two questions focused on the actors that respondents would seek help from in case of a cyberattack (Q11), as well as their preferred information brokers for cybersecurity information (Q19). Due to the scope of our research questions, we decided to analyze them in future work. Additionally, we intended to gain insights into what disadvantages and advantages citizens see in the application of open-source intelligence for a separate study (Q14, Q15).

Most questions were designed as five-point verbal rating scales (VRS), with the exception of Q1 (binary consent), Q2 to Q6 (demographic variables), Q7 (four-point VRS), Q10 and Q12 (six-point VRS), and Q17 (multiple choice with up to three items). When designing the content related questions, emphasis was placed on achieving an ordinal scale level wherever possible so that potential correlations between variables could be investigated in future work on the basis of the obtained data set. In addition, five-point VRS were used where feasible to minimize irritation of respondents by changing the number of choices. Q7 is an exception; here, it seemed unreasonable to differentiate the usage times of devices any further. Q10 and Q12 also feature a "do not know/can not say" option in addition to the five ordinal scale response options, thereby enhancing data quality when querying respondents' assessment of their exposure to or anticipated risk of cyber attacks. Finally, Q17 is configured as a multiple choice question in order to prompt respondents to prioritize their preferred communication channels.

3.2 Mitigation of Biases

In order to minimize potential sources of bias, we have implemented a number of measures. The arrangement of questions may induce question order bias [29]. To mitigate this as far as possible, we firstly sought to minimize the priming of respondents during questionnaire design, for example by asking general questions prior to specific questions; secondly, we placed similar questions in thematic blocks; and thirdly, we checked during the pre-test whether the question order had an irritating effect on the respondents. While the questions were displayed in the same order for all participants, the order of rows in all matrix questions was randomized. Additionally, it was not feasible to retrieve the demographic information after the thematic questions, as the panel provider required this information beforehand to ensure the representativity of the sample.

To address the issues of unbalanced questions and scales [18], we first carefully formulated our questions and items as neutral and objective as possible and second used balanced scales (e.g., Likert scales with a neutral option) wherever possible. Furthermore, too extensive surveys can trigger so-called survey time fatigue among respondents, which may cause termination of the survey or inattentive responses [10]. To pre-empt this, first, the block

with questions on open-source intelligence (Q14-Q15) was placed between the two blocks with a cybersecurity focus (Q7-Q13 and Q16-Q19). Switching the thematic focus was intended to diversify the questionnaire and thus increase respondents' attention for the remainder of the survey. Second, during the pre-test, we determined the average completion time of 20 minutes to ensure that the survey time remains within reasonable limits. Third, as an attention check, we included an item on Q15 that asked for a specific response option.

Finally, social desirability bias [40] poses a major challenge to the measurement of cybersecurity behavior [16]. Here, this primarily concerns dishonest answers to Q13. This could only be slightly mitigated due to the chosen self-administered survey mode. Self-administration can increase respondents perception of privacy and anonymity, thus prompting more honest answers [37, 40]. However, since our survey generally relies on respondents' honest self-reporting and does not measure actual behavior, the possibility of biased results should be acknowledged.

3.3 Data Collection and Analysis

The study was conducted in accordance with the requirements of the ethics committee at our university. These include, among other things, avoiding unnecessary stress, excluding risk and harm, and anonymizing participants. The personal data collected was limited to age, gender, education, income, and region of residence. Participants were transparently informed about the procedure and goals of the study and subsequently gave their informed consent to participate. GapFish (Berlin), as the selected panel provider, is ISO-certified and ensures panel and data quality, security, and survey quality through various (segmentation) measurements for each survey within their panel of 500,000 active participants. We transmitted the questionnaire to GapFish who programmed and hosted the online survey. After final quality checks and mutual agreement, they invited participants from their panel to take part in the survey in September 2021. In this workshop paper, we present the descriptive results of our analysis and discuss recommendations for action based on our sample (1,093 participants with median survey completion time of 19.3 minutes) with the following demographic characteristics, which correspond to those of the general German population and thus ensure representativeness in this respect:

- **Age**: 18-24 (8.9%), 25-34 (14.6%), 35-44 (15.0%), 45-54 (16.7%), 55-64 (18.2%), 65+ (26.5%)
- **Gender**: Female (50.2%), male (49.6%), diverse (0.1%), not stated (0.1%)
- **Education**: Lower secondary education (28.5%), middle or high school (55.3%), academic degree (16.3%)
- **Income**: <1,500€ (24.5%), 1,500€-2,600€ (30.8%), 2,600€-4,500€ (28.9%), >4,500€ (15.7%)
- **State**: BB (2.6%), BE (4.5%), BW (13.4%), BY (15.9%), HB (0.8%), HE (7.6%), HH (2.3%), MV (1.6%), NI (9.7%), NW (21.7%), RP (4.9%), SH (3.6%), SL (1.2%), SN (4.9%), ST (2.7%), TH (2.6%) [1]

[1]Meaning of abbreviations: Brandenburg, Berlin, Baden Wurttemberg, Bavaria, Bremen, Hesse, Hamburg, Mecklenburg–Western Pomerania, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, Schleswig-Holstein, Saarland, Saxony, Saxony-Anhalt, Thuringia

4 RESULTS

4.1 General Perceptions of Cyber Threats on Individual and Societal Levels (Q8)

A large proportion of respondents evaluate the *current threat level* as quite high. About 46% agree that cyber threats pose a serious risk to them. Moreover, 70% support the assessment that without a firewall and virus scanner, internet usage should be avoided due to the risk of malware infection, and 60% state that they restrict their internet usage to commonly known websites to avoid cybercrime victimization. An even clearer pattern emerges with regard to the assessment of the *prospective threat level*. With regard to the next five years, 72% agree that the individual risk of cyber threat victimization will increase and 70% think a large-scale cyberattack on public infrastructure in Germany is a realistic scenario, while only 14% consider Germany as well prepared for large-scale cyberattacks on public infrastructure. This resonates with low *trust in governmental institutions*. Only 23% of respondents agree that German security authorities have the necessary competencies to adequately protect citizens from cyber threats and only 20% that cybercrime is adequately prosecuted and punished by the German law enforcement authorities and judiciary.

A clear majority of respondents (63%) think that wars will increasingly be fought digitally, but only 37% are generally afraid that a *cyberwar* could break out. Regarding the question whether Germany should retaliate against cyberattacks with own cyberattacks, the respondents are divided; 37% view this measure positively and 27% negatively. When it comes to assessing their own *cybersecurity competence*, a large proportion of respondents identify deficits. Only 38% see themselves clearly in a position to protect their own devices from threats, whereas more than 59% believe they would probably not recognize attempts to spy on them via the Internet. Overall, almost half (49%) feel insufficiently informed about cyber threats. Correspondingly, a *qualification demand* can be identified, i.e., 49% of interviewees state they don't know who to contact for information on protective measures and 34% lack knowledge about internet sources on up-to-date and reliable information for device protection. Thus, more than half of the respondents (55%) would like to educate themselves about protection on the internet.

4.2 The Use of Internet Devices and Security Measures (Q7, Q13)

With regard to the use of devices with internet access, almost all respondents (94%) state that they use a smartphone. Moreover, the majority of respondents (58%) use smartphones for more than 2 hours per day on average, while internet capable mobile phones without touchscreen are used by only 22%. A clear majority of respondents also use a notebook (76%), tablet (63%), or stationary PC (60%), while only 35% use internet-connected game consoles. Networked and smart IoT devices, however, have not yet become ubiquitous, with the exception of internet-enabled smart TVs, which are used by 73%. Smart speakers (34%) and watches (33%) are used slightly more frequently than smart lightning (20%), smart heating thermostats (11%), and interconnected cars (9%).

When it comes to the use of security tools and the implementation of security measures (see Figure 1), it is noticeable that a large

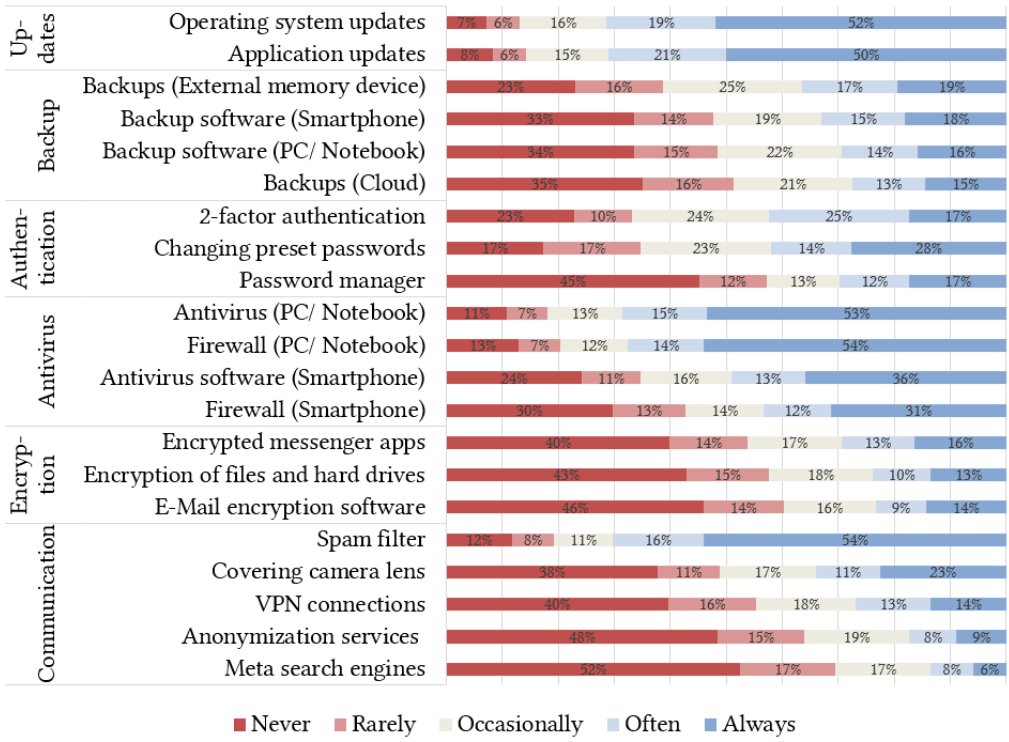

Figure 1: How often do you use the following security tools or measures on your personal devices to protect against cyber threats? (Q13)

number of respondents frequently or always use security solutions that have been configured once and are then permanently active, such as spam filters (70%), firewalls (68%), and antivirus software (68%) on the PC or laptop, as well as firewalls (43%) and antivirus software (49%) on the smartphone. Also common is regularly updating programs and apps (71%) as well as the operating system of devices (71%). Software for automatically creating backups is used regularly by fewer respondents, and it is worth noting that automatic backups on storage media (33%) are more popular than those on cloud services (30%). Additionally, 34% say they at least regularly physically cover camera lenses on their devices. Security measures that require regular user activity are significantly less common. As many as 42% of respondents say they often or always use two-factor authentication when logging into services, while only 29% say the same about password managers. Likewise, less than a third of respondents report to frequently or always use anonymization or encryption measures, such as encrypted messenger services (29%), encryption software for e-mails (23%), VPN services (27%), encryption software for files and data carriers (23%), anonymization services (17%), or metasearch engines (14%).

4.3 Current Status and Future Projection of Susceptibility to Cyberattacks (Q10, Q12)

As can be seen in Figure 2, spam, malware, and ransomware represent the most widespread threat types in Germany. As many as 70% of respondents say they had been affected by spam at least once in the last 5 years; indeed, 51% have been affected by it occasionally or frequently. 40% were affected by malware in the same period (10% occasionally or frequently) and 34% by ransomware (11% occasionally or frequently). In addition, 24% have already suffered *financial losses* due to online shopping fraud and 16% due to scareware. More serious types of *harassment* than spam also affected a fraction of respondents in the last five years. The fact that 16% have been affected by identity theft, 16% by cyberbullying, 14% by online threats or cyberstalking, and 12% by doxing shows that such attacks are by no means isolated incidents but constitute serious threats to a significant part of the population. Approximately one in five respondents has been affected by unauthorized third-party access to an online or social media account (21%) or a phishing attack (19%) at least once in the past five years, while exposure to the *privacy threats* of spyware (17%) and social engineering (9%) is less widespread. Finally, only a small proportion of respondents indicate that they have been affected by threats other than malware that *impair the functioning of a system*. Whereas 16% of respondents have been impacted by a distributed denial-of-service attack (DDoS) attack at least once in the last five years, this is the case for only 8% of respondents with regard to side-channel attacks, only 7% with regard to advanced persistent threats, and only 6% with regard to a theft of computing power, e.g., via cryptomining programs.

Asked for their risk perception of attack types within the next five years, more than one-fifth of respondents indicate that they perceive a rather high or very high personal risk with regard to the common cybersecurity threats spam (43%), malware (29%), spyware

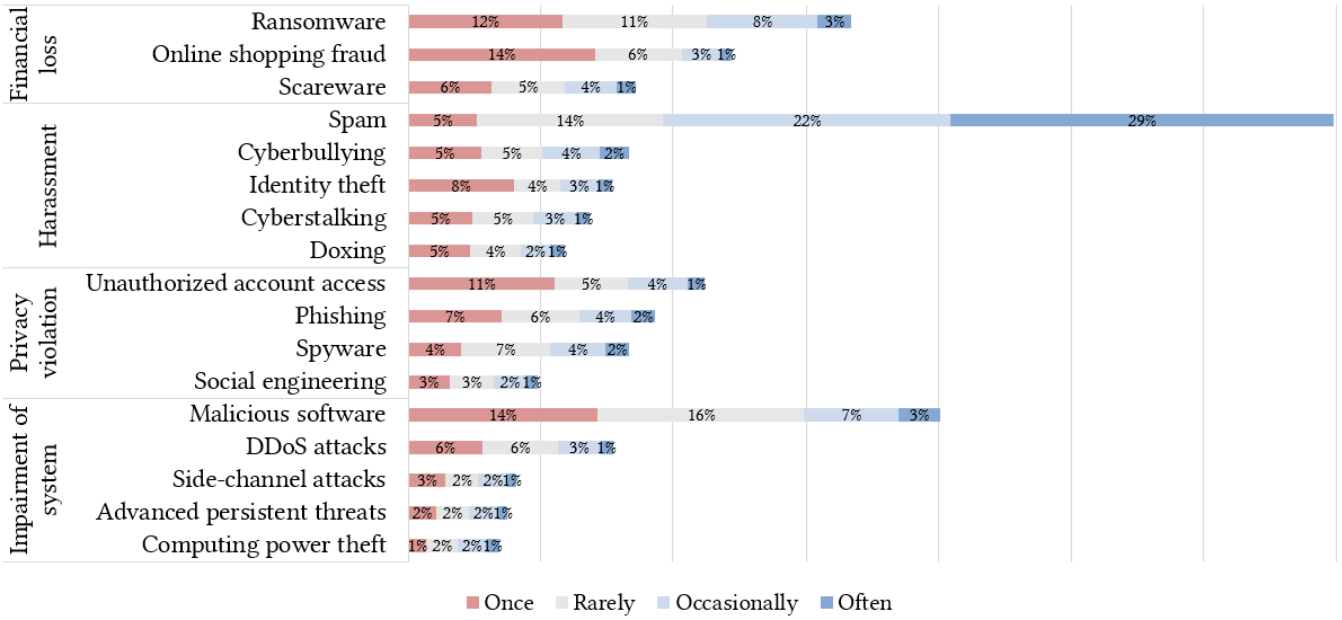

Figure 2: In the last five years, how often have you personally been a victim of the following types of cyber threats? (Q10) - Results for the response options ´Never' and ´Don't know' have been omitted to enhance readability.

(25%), and phishing (25%) as well as unauthorized third-party access to online and social media accounts (23%) and online shopping fraud (20%). In contrast, only a smaller proportion of interviewees have a comparable high risk awareness of the dangers posed by serious forms of online harassment (identity theft: 17%; doxing: 16%; cyberbullying: 14%; cyberstalking 14%). The same applies to scareware (15%) and social engineering (14%), as well as threats that are technically rather complex or abstract for average citizens, such as DDoS attacks (17%), advanced persistent threats (13%), theft of computing power (12%), and side-channel attacks (11%). Remarkable is the observation that even though ransomware constitutes one of the most frequent cyber threats, only 18% associate rather high or very high risks with it.

4.4 Awareness of Cybersecurity Institutions and Desired Types for Information (Q9, Q18)

Only a minority of respondents are aware of the functions and objectives of most of the institutions, platforms, and measures that contribute to cybersecurity in Germany. One exception are the police institutions Federal Criminal Police Office (BKA) and Europol, whose functions and goals are known to respectively 76% and 56% of respondents. The purposes of other government institutions such as the Federal Office for Information Security (BSI) (37%), the Police Crime Prevention of the States and the Federation (ProPK) (28%), the Central Office for Information Technology in the Security Sector (ZITiS) (18%), the National Cyber Defense Center (20%), and the European Union Agency for Cyber Security (ENISA) (14%) are known to less than half of the respondents. Although some of the CERTs in the German states also offer advisory services to citizens, only 16% of respondents are aware of their purpose. The orientation of research institutions is also rather unknown, with knowledge about the Max Planck Institute for Cybersecurity and Privacy Protection (24 %) being more widespread than, e.g., about the Helmholtz Center for Information Security (16%) or the National Research Center for Applied Cybersecurity ATHENE (14%). The goals of measures and campaigns to strengthen cybersecurity are also only known to a small proportion of respondents; in this context, knowledge about the 'Change your password day' is still most common (20%).

When asked which types of information about cyber threats or recommendations for *protective measures* are considered particularly relevant and warrant focused communication, all available response options are rated as rather relevant or definitely relevant by more than half of the respondents (see Figure 3). Information on preventive protective measures for particular areas is rated most frequently as being definitely relevant. Information on secure mobile and online banking (68%), device security (64%), and secure online shopping (59%) is of greatest interest, followed by information on secure e-mail communication (55%), secure use of online accounts (54%) and public networks (53%), and securing home networks (50%). In contrast, less than half of respondents consider information on the secure use of social networks (43%) and networked smart home devices (36%), as well as general recommendations and best practices for increasing cybersecurity (26%) to be definitely of relevance. As for communicating *cybersecurity-related news*, information on major software updates has clear relevance for the majority of respondents (51%); in addition, a significant proportion of respondents also request information on recent vulnerabilities in common software (41%), disclosed data leaks (40%), novel malware (37%), and current spam waves and phishing campaigns (29%). With regard to

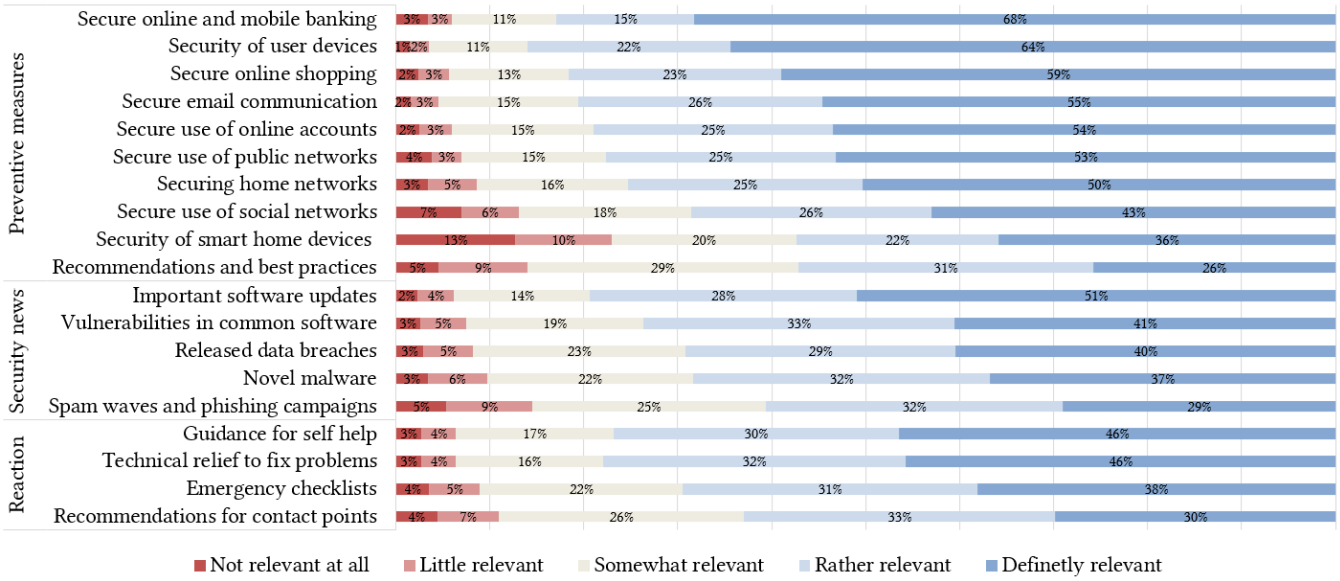

Figure 3: Which information on cyber threats and recommendations for protective measures are relevant to you? (Q18)

the *reaction* to incidents, almost half of respondents (46%) consider self-help instructions and technical assistance for remediation to be definitely relevant, while checklists in the event of an incident are relevant for 38%, and recommendations or links to responsible organizations or employees for 30%.

4.5 Current and Preferred Channels to Receive Cybersecurity Information (Q16, Q17)

When asked about the channels currently used to receive information about cyber threats, vulnerabilities, and solutions, more than half of respondents report that they sometimes or more frequently obtain information from family or friends (60%), installed security software (59%), television (56%), and security software vendor websites (51%). A slightly smaller proportion but still more than a third of respondents state that at least sometimes the websites of software or hardware manufacturers (44%), the radio (42%), messengers (36%), warning apps (34%), the school, university or workplace (34%), multimedia services like YouTube (33%), and newsletters (33%) are consulted to access cybersecurity information, while social networks (30%), security news websites (29%), specialized publications (28%), and security authority websites (26%) are named by more than a quarter of respondents. Blogs, podcasts, and microblogging services, such as Twitter, are mentioned only by a small proportion of respondents (19%, 16%, 15%) as occasional or frequent sources.

In Q17, we asked respondents to indicate their three preferred channels for receiving cyber threat, vulnerability, and problem resolution information in the future (see Figure 4). Altogether, television (35%), installed security software (33%), warning apps on the smartphone (27%), and the websites of security software manufacturers (22%) are mentioned most frequently. Other websites focusing on cybersecurity-related topics, such as those of hardware or software manufacturers (15%), security agencies (13%), and media specializing in security topics (12%), as well as specialized newsletters (12%), are less popular. Most traditional media, including press publications (16%), radio (15%), and specialized journals (6%), are only mentioned by a small proportion of respondents. The same is true of more novel channels such as messengers (14%), social networks (13%), and multimedia services (12%). It is interesting that 17% of respondents prefer to receive information directly from family members or friends, but only 9% articulate the same with regard to school, university, or workplace. Finally, blogs, podcasts, and microblogging services are hardly mentioned (2% each).

5 DISCUSSION

5.1 Current and Future Threat Situation and Protective Measures in Cyberspace (RQ1)

We found that large proportions of the population feel inadequately informed about cyber threats. It also became apparent that some security institutions, such as CERTs, are rather unknown to the German population. These findings suggest that security institutions should enhance their strategies for *information dissemination* [58], including the provision of resources, administrative news, or opinion-related messages. Furthermore, since our participants showed little confidence in German security authorities' ability to cope with large-scale attacks and to protect citizens, enhanced preparedness education as well as frequent dissemination of alerts, warnings, and advisories could help to increase trust into security institutions [58]. Such information for preparedness and response could be initiated by institutional campaigns and provided by guidelines [33] or warning apps [35], among others. Further trust-building measures could comprise the strategy of *conversations & coordinated action*, which includes measures such as one-to-one conversations, rumor management, or even crowdsourcing [58]. However, emergency managers of the cyber and other domains often struggle with such resource-intensive strategies due

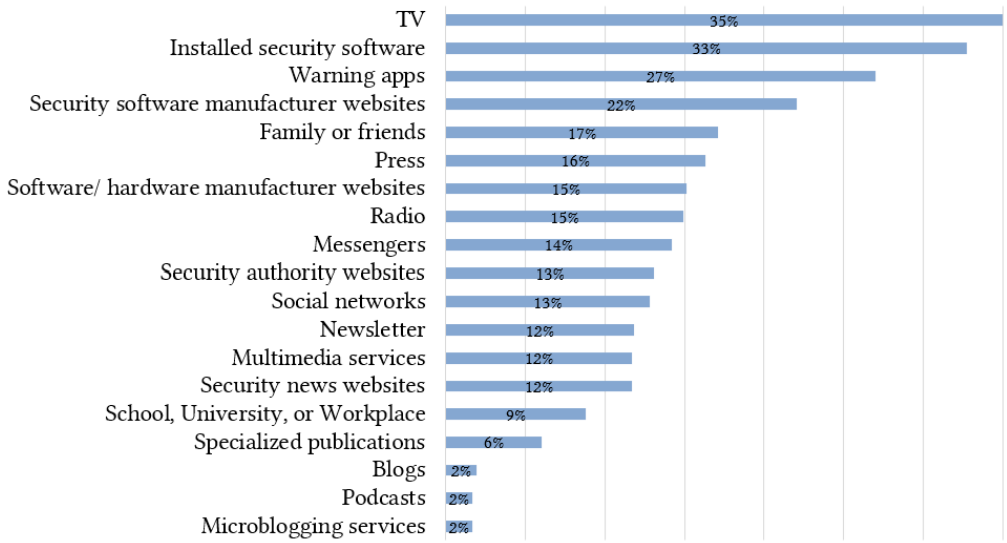

Figure 4: Which channels do you prefer to receive information on cyber threats, vulnerabilities and solutions in future? (Q17)

to a lack of personnel resources [49, 50]. In terms of citizen behavior, it became apparent that enforced security provisions (e.g., updates, two-factor authentication) are more commonly adopted than independently initiated measures. Besides enhanced information dissemination, another promising research direction seems to be the use of nudging to promote better security decisions of citizens [21, 22].

5.2 Required Information and Channels to Enhance Cyber Threat Awareness (RQ2)

The majority of our participants consider all types of information on cyber threats and protection mechanisms to be relatively relevant for future communication. With regard to *preventive measures*, information on secure mobile and online banking and on the protection of end user devices is seen as most relevant. However, *news*, especially on important software updates, and instructions for self-help as well as technical support in *reaction to incidents* are also in high demand. In order to increase citizens' awareness of cyber threats, it thus seems reasonable to incorporate information of all three areas into dissemination strategies. However, this poses the challenge of communicating appropriately to the respective target groups. As IT knowledge and skills vary in different demographic groups [25], wording and the level of detail of information in alerts need to be adapted [4]. The same should be the case for other communication products. Likewise, research on the impact of emotional appeals on different target groups could also be of relevance [30, 38, 44]. Television and warning apps are preferred *public channels* for disseminating cybersecurity information, while the installed security software and the websites of security software manufacturers are the preferred *commercial* or *private channels*. Thus, to reach citizens as effectively as possible and in line with their requirements, intensified cooperation between security authorities and IT security companies seems to make sense in prevention and education work as well as in the communication of threats. In addition, cybersecurity-related warnings should increasingly be distributed via warning apps on mobile devices. Work on integrating this type of information is still in its infancy, yet there is potential to build on existing empirical research on citizens' requirements for warning apps for other types of incidents, such as in [24, 35]. While 61% of German citizens find it quite or very important to add cybercrime-related warnings to established warning apps [35], the limited number of users of such apps pose a challenge; e.g., NINA, the warning app provided by the German Civil Protection, had only 8.8 million users in 2021 [9]. Although the COVID-19 pandemic likely had a positive impact on the adoption of warning apps [24], strategies for increasing the number of users must be developed simultaneously. Finally, studies document significant differences in media use in crisis situations for different demographic groups [34]. No comparable differentiation with regard to channels for cybersecurity information exists to date, yet it is a subject of ongoing research.

5.3 Comparison to Related Work

In light of similar studies, our work focuses on some topics not investigated with the German population so far, thereby providing novel insights. First, to date, no survey has examined the population's knowledge of institutions, platforms, and measures that contribute to cybersecurity in Germany. The lack of awareness of numerous state security institutions has thus remained undetected. Second, while other studies have examined the communication channels for cybersecurity information that are being used by the population [5, 6] or their preferred information types [8], preferences for future channels for communicating this information have not yet been systematically surveyed. Third, by providing more extensive response options and querying the frequency of affectedness or intensity of use, we were able to considerably expand the empirical findings on some of the attitudes and behaviors already examined by other studies, e.g., with regard to the victimization

by cyberthreats [5, 6, 17, 31] or the implementation of protective measures [5, 6, 17]. Similarly, the general threat perception, the self-perception of one's own cybersecurity competence, and the perception of state institutions' cybersecurity competence among the German population have only been surveyed in a very fragmentary manner in other studies to date [5, 31]; this study presents the first comprehensive insights in this regard.

Some results from other studies we were able to corroborate. For instance, the proportion of the German population expecting an increase in the risk of cybercrime victimization is 72% in September 2021, which is only slightly lower than the figure of 77% recorded in 2019 on behalf of the European Commission [31]. Additionally, as was also found in [8], we found that information on secure mobile and online banking and on the protection of end user devices is seen as most relevant by German citizens. Similarities with existing research can also be identified with regard to the risk perception of cyber threats. Analogous to a query of cyber threat scenarios in 2019 [5], malware and attacks aimed at unauthorized access to or misuse of passwords, personal data and accounts are among the five most frequently mentioned threat types in our study.

However, there were also differences with regard to other findings. While in 2019 half of Germans thought they could protect themselves adequately against cybercrime [31], in this survey only 38% clearly stated that they could protect their devices against threats. The level of insecurity among the German population has thus significantly increased in this regard. In addition, compared to a survey conducted in April 2020 [6], a larger proportion of our respondents stated that they implement certain protective measures. Although the previous survey did not differentiate between measures for different devices, considerably more respondents in our survey stated that they regularly or always use antivirus software (68% vs. 57%) and firewalls (68% vs. 47%) on their PCs/laptops, and two-factor authentication for online services (42% vs. 33%). Yet, numbers on the use of two-factor authentication must be considered with the caveat that it is mandatory for Germans to use it in online banking due to the Payment Services Directive (PSD2). This might have led to a positive distortion of the results, as different services were not differentiated in our survey and global adoption rates for social media are very low [41, 55].

6 CONCLUSION

We presented the descriptive results of a representative survey (N=1,093) on the implementation of protective measures and communication of cybersecurity alerts in Germany. Our findings reveal that large parts of the German population do not feel sufficiently informed about cyber threats and primarily adopt enforced security measures through programs (e.g., updates) and services (e.g., two-factor authentication). Additionally, institutions such as the CERTs of the German states are comparatively unknown among the population and the German security authorities as a whole are perceived as having little competence to cope with large-scale cyberattacks and effectively protect citizens. Finally, there is a great demand for all types of information about cyber threats and protective measures among respondents, which should preferably be disseminated via installed security applications, TV channels, or emergency warning apps. However, the present paper is subject to limitations and offers potentials for future research. First, since it only provides a descriptive analysis, it does not uncover relationships between statements and demographic variables or specific user groups. Thus, a statistical analysis will be conducted as a next step of this study. Second, the study was conducted using an online survey which might provide largely representative results with regard to some factors, but nonetheless only covers people who are willing to do online surveys; therefore, they are most likely more familiar with the internet and social media. Third, we only study citizens' perception in Germany, thus further surveys incorporating users of other risk cultures [12, 47] could provide additional interesting insights. Fourth, on the basis of this survey, we cannot provide explanations for the population's low level of confidence in the cybersecurity capabilities of German security authorities. An investigation of the reasons for this perception represents a promising avenue for future empirical research. Finally, citizens' perceptions and behaviors with regard to cybersecurity are subject to change, e.g., due to large-scale cyber incidents or the adoption of new technologies. Thus, we seek to conduct subsequent representative surveys to facilitate a longitudinal study with a temporal analysis of change.

ACKNOWLEDGMENTS

This research work has been funded by the German Federal Ministry for Education and Research (BMBF) in the project CYWARN (13N15407) 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, and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 (CROSSING) – 236615297.

REFERENCES

[1] Chris Adams. 2018. Learning the lessons of WannaCry. *Computer Fraud & Security* 2018, 9 (2018), 6–9. https://doi.org/10.1016/S1361-3723(18)30084-8

[2] 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 (2020), 288–318. https://doi.org/10.1080/0144929X.2019.1610908

[3] Michael Aupetit and Muhammad Imran. 2017. Interactive monitoring of critical situational information on social media. In *Proceedings of the 14th ISCRAM Conference* (Albi, France). ISCRAM, Brussels, Belgium, 673–683.

[4] Ali Sercan Basyurt, Jennifer Fromm, Philipp Kuehn, Marc-André Kaufhold, and Milad Mirabaie. 2022. Help Wanted - Challenges in Data Collection, Analysis and Communication of Cyber Threats in Security Operation Centers. In *Wirtschaftsinformatik 2022 Proceedings* (Nuremberg, Germany) *(WI)*. AIS, Atlanta, GA, USA.

[5] Bitkom Research. 2020. *Vertrauen & IT-Sicherheit.* Technical Report. Bitkom, Berlin. https://www.bitkom.org/sites/default/files/2020-02/bitkom_vertrauenitsicherheit2020.pdf

[6] Bundesamt für Sicherheit in der Informationstechnik and Polizeiliche Kriminalprävention der Länder und des Bundes. 2020. *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit.* Technical Report. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2020.pdf?__blob=publicationFile&v=1

[7] Bundeskriminalamt. 2019. Festnahme eines Tatverdächtigen im Ermittlungsverfahren wegen des Verdachts des Ausspähens und der unberechtigten Veröffentlichung personenbezogener Daten. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190108_FestnahmeDatenausspaehung.html

[8] Bundesministerium des Innern, für Bau und Heimat and Bundesamt für Sicherheit in der Informationstechnik. 2020. *Bundesweite Themenabfrage zur Internetsicherheit mit Civey.* Technical Report. Berlin. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2020/anlage-1-pm-sid.pdf;jsessionid=F267B0E2F27B93F8B813EEB00D569AEB.1_cid364?__blob=publicationFile&v=1

[9] Bundesregierung. 2021. Warn-App NINA mit lokalen Hinweisen zu Gefahrenlagen. https://www.bundesregierung.de/breg-de/aktuelles/warn-app-nina-

1942330
[10] Brendan Burchell and Catherine Marsh. 1992. The effect of questionnaire length on survey response. *Quality and quantity* 26, 3 (1992), 233–244. https://doi.org/10.1007/BF00172427
[11] Carlos Castillo. 2016. *Big Crisis Data: Social Media in Disasters and Time-Critical Situations.* Cambridge University Press, New York, NY, USA.
[12] Alessio Cornia, Kerstin Dressel, and Patricia Pfeil. 2016. Risk cultures and dominant approaches towards disasters in seven European countries. *Journal of Risk Research* 19, 3 (2016), 288–304. https://doi.org/10.1080/13669877.2014.961520
[13] Cybersecurity and Infrastructure Security Agency. 2016. ICS Alert (IR-ALERT-H-16-056-01). Cyber-Attack Against Ukrainian Critical Infrastructure. https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01
[14] 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.* Technical Report. RAND Corporation, Arlington, VA, USA. https://doi.org/10.7249/RR2081
[15] 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 (2020), 102174. https://doi.org/10.1016/j.ipm.2019.102174
[16] Tobias Fertig and Andreas Schütz. 2020. About the measuring of information security awareness: a systematic literature review *(HICSS).* HICSS, Honolulu, HI, USA, 6518–6527.
[17] Forsa Politik- und Sozialforschung GmbH. 2017. *Cybersicherheit in Sachsen. Ergebnisse einer repräsentativen Bevölkerungsbefragung.* Technical Report. Sächsisches Staatsministerium des Innern, Dresden. https://www.medienservice.sachsen.de/medien/medienobjekte/116129/download
[18] Hershey H Friedman and Taiwo Amoo. 1999. Rating the rating scales. *Friedman, Hershey H. and Amoo, Taiwo (1999)." Rating the Rating Scales." Journal of Marketing Management, Winter* (1999), 114–123.
[19] Bundesamt für Sicherheit in der Informationstechnik. 2018. *The State of IT Security in Germany 2018.* Technical Report. Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=1
[20] 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. In *Proceedings of the 54th Annual Hawaii International Conference on System Sciences* (Kauai, HI, USA). HICSS, Honolulu, HI, USA, 2036–2045.
[21] Katrin Hartwig and Christian Reuter. 2021. Nudge or Restraint: How do People Assess Nudging in Cybersecurity - A Representative Study in Germany. In *European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC).* ACM, New York, NY, USA, 141–150. https://doi.org/10.1145/3481357.3481514
[22] Katrin Hartwig and Christian Reuter. 2022. Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behaviour & Information Technology (BIT)* 41, 7 (2022), 1357–1380. https://doi.org/10.1080/0144929X.2021.1876167
[23] Jasmin Haunschild, Marc-André Kaufhold, and Christian Reuter. 2020. Sticking with Landlines? Citizens' and Police Social Media Use and Expectation During Emergencies. In *Proceedings of the International Conference on Wirtschaftsinformatik (WI) (Best Paper Social Impact Award).* AIS Electronic Library (AISel), Potsdam, Germany, 1–16. https://doi.org/10.30844/wi_2020_o2-haunschild
[24] Jasmin Haunschild, Marc-André Kaufhold, and Christian Reuter. 2022. Perceptions and Use of Warning Apps – Did Recent Crises Lead to Changes in Germany?. In *Mensch und Computer 2022 - Tagungsband.* ACM, New York.
[25] Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. 2020. Differences in IT Security Behavior and Knowledge of Private Users in Germany. In *Proceedings der 15. Internationalen Tagung Wirtschaftsinformatik 2020 - Community Tracks* (Potsdam, Germany) *(WI).* GITO, Berlin, Germany, 168–184. https://doi.org/10.26083/tuprints-00020742
[26] 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 (2020), 101367. https://doi.org/10.1016/j.ijdrr.2019.101367
[27] Muhammad Imran, Carlos Castillo, Fernando Diaz, and Sarah Vieweg. 2015. Processing Social Media Messages in Mass Emergency: A Survey. *ACM Comput. Surv.* 47, 4, Article 67 (2015), 38 pages. https://doi.org/10.1145/2771588
[28] Arbeitsgruppe Kritische Infrastrukturen. 2020. Das Cyber-Hilfswerk. Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen. https://ag.kritis.info/wp-content/uploads/2020/02/chw-konzept_v1.0.pdf
[29] Glenn D Israel and CL Taylor. 1990. Can response order bias evaluations? *Evaluation and Program Planning* 13, 4 (1990), 365–371. https://doi.org/10.1016/0149-7189(90)90021-N
[30] Allen C Johnston, Merrill Warkentin, Alan R Dennis, and Mikko Siponen. 2019. Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences* 50, 2 (2019), 245–284. https://doi.org/10.1111/deci.12328
[31] Kantar. 2020. *Special Eurobarometer 499. Europeans' attitudes towards cyber security.* Technical Report. European Commission, Brussels. https://op.europa.eu/en/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1
[32] Marc-André Kaufhold. 2021. *Information Refinement Technologies for Crisis Informatics: User Expectations and Design Principles for Social Media and Mobile Apps.* Springer Vieweg, Wiesbaden, Germany. https://doi.org/10.1007/978-3-658-33341-6
[33] Marc-André Kaufhold, Alexis Gizikis, Christian Reuter, Matthias Habdank, and Margarita Grinko. 2019. Avoiding Chaotic Use of Social Media before, during, and after Emergencies: Design and Evaluation of Citizens' Guidelines. *Journal of Contingencies and Crisis Management (JCCM)* 27, 3 (2019), 198–213. https://doi.org/10.1111/1468-5973.12249
[34] Marc-André Kaufhold, Margarita Grinko, Christian Reuter, Marén Schorch, Amanda Langer, Sascha Skudelny, and Matthias Hollick. 2019. Potentiale von IKT beim Ausfall kritischer Infrastrukturen: Erwartungen, Informationsgewinnung und Mediennutzung der Zivilbevölkerung in Deutschland. In *Wirtschaftsinformatik 2019 Proceedings (WI).* AIS, Atlanta, GA, USA, 1054–1068.
[35] Marc-André Kaufhold, Jasmin Haunschild, and Christian Reuter. 2020. Warning the Public: A Survey on Attitudes, Expectations and Use of Mobile Crisis Apps in Germany. In *Twenty-Eight European Conference on Information Systems* (Marrakesh, Morocco) *(ECIS).* AIS, Atlanta, GA, USA.
[36] Marc-André Kaufhold, Nicola Rupp, Christian Reuter, and Matthias Habdank. 2020. Mitigating Information Overload in Social Media during Conflicts and Crises: Design and Evaluation of a Cross-Platform Alerting System. *Behaviour & Information Technology (BIT)* 39, 3 (2020), 319–342. https://doi.org/10.1080/0144929X.2019.1620334
[37] Ivar Krumpal. 2013. Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & quantity* 47, 4 (2013), 2025–2047. https://doi.org/10.1007/s11135-011-9640-9
[38] Philip Menard, Gregory J Bott, and Robert E Crossler. 2017. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems* 34, 4 (2017), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083
[39] Csikszentmihalyi Mihaly. 2013. Creativity: The psychology of discovery and invention. *New York, Harperperennial Modern Classics* (2013).
[40] Anton J Nederhof. 1985. Methods of coping with social desirability bias: A review. *European journal of social psychology* 15, 3 (1985), 263–280. https://doi.org/10.1002/ejsp.2420150303
[41] Lily Hay Newman. 2021. Facebook will force more at-risk accounts to use two-factor. *Wired* (2 December 2021). https://www.wired.com/story/facebook-protect-two-factor-authentication-requirement/
[42] 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* (Vancouver, BC, Canada) *(CSCW '15).* ACM, New York, NY, USA, 994–1009. https://doi.org/10.1145/2675133.2675242
[43] Teresa Onorati, Paloma Díaz, and Belen Carrion. 2019. From social networks to emergency operation centers: A semantic visualization approach. *Future Generation Computer Systems* 95 (2019), 829–840. https://doi.org/10.1016/j.future.2018.01.052
[44] Miloslava Plachkinova and Philip Menard. 2019. An examination of gain-and loss-framed messaging on smart home security training programs. *Information Systems Frontiers* (2019), 1–22. https://doi.org/10.1007/s10796-019-09970-6
[45] 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 (2018), 367–381. https://doi.org/10.1080/10447318.2018.1427825
[46] 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 (2018), 41–57. https://doi.org/10.1111/1468-5973.12196
[47] Christian Reuter, Marc-André Kaufhold, Stefka Schmid, Thomas Spielhofer, and Anna Sophie Hahne. 2019. The Impact of Risk Cultures: Citizens' Perception of Social Media Use in Emergencies across Europe. *Technological Forecasting and Social Change* 148, 119724 (2019), 1–17. https://doi.org/10.1016/j.techfore.2019.119724
[48] Christian Reuter, Thomas Ludwig, Marc-André Kaufhold, and Volkmar Pipek. 2015. XHELP: Design of a Cross-Platform Social-Media Application to Support Volunteer Moderators in Disasters. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Korea) *(CHI'15).* ACM, Atlanta, GA, USA, 4093–4102. https://doi.org/10.1145/2702123.2702171
[49] Christian Reuter, Thomas Ludwig, Marc-André Kaufhold, and Thomas Spielhofer. 2016. Emergency Services Attitudes towards Social Media: A Quantitative and Qualitative Survey across Europe. *International Journal on Human-Computer Studies (IJHCS)* 95 (2016), 96–111. https://doi.org/10.1016/j.ijhcs.2016.03.005
[50] Thea Riebe, Marc-André Kaufhold, and Christian Reuter. 2021. The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. *Proceedings of the*

ACM on Human-Computer Interaction 5, CSCW2, Article 478 (oct 2021), 30 pages. https://doi.org/10.1145/3479865

[51] Robert Soden and Leysia Palen. 2018. Informating Crisis: Expanding Critical Perspectives in Crisis Informatics. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW, Article 162 (nov 2018), 22 pages. https://doi.org/10.1145/3274431

[52] 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 9th International ISCRAM Conference* (Vancouver, BC, Canada) *(ISCRAM)*, L. Rothkrantz, J. Ristvej, and Z. Franco (Eds.). ISCRAM, Brussels, Belgium, 1–10.

[53] Kate Starbird and Leysia Palen. 2011. "Voluntweeters": Self-Organizing by Digital Volunteers in Times of Crisis. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. ACM, New York, NY, USA, 1071–1080. https://doi.org/10.1145/1978942.1979102

[54] Marion Lara Tan, Raj Prasanna, Kristin Stock, Emma Hudson-Doyle, Graham Leonard, and David Johnston. 2017. Mobile applications in crisis informatics literature: A systematic review. *International Journal of Disaster Risk Reduction (IJDRR)* 24 (2017), 297–311. https://doi.org/10.1016/j.ijdrr.2017.06.009

[55] Twitter. 2021. Account Security. https://transparency.twitter.com/en/reports/account-security.html#2021-jan-jun

[56] Sarah Vieweg, Amanda L. Hughes, Kate Starbird, and Leysia Palen. 2010. Microblogging during Two Natural Hazards Events: What Twitter May Contribute to Situational Awareness. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, GA, USA) *(CHI '10)*. ACM, New York, NY, USA, 1079–1088. https://doi.org/10.1145/1753326.1753486

[57] 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 (2020), 101521. https://doi.org/10.1016/j.giq.2020.101521

[58] Clayton Wukich. 2015. Social media use in emergency management. *Journal of Emergency Management* 13, 4 (2015), 281–294. https://doi.org/10.5055/jem.2015.0242

A APPENDIX: QUESTIONNAIRE

This is the English translation of the German questionnaire used in the survey. To reduce the size of the appendix, the items assigned to the questions are not included, as they can be found in the description and illustrations in Section 4. The results for Q11, Q14, Q15, and Q19 were not analyzed in this paper.

Q1: I agree to complete this questionnaire for the CYWARN project, which asks about my attitudes toward cybersecurity, and that my participation is voluntary. The results of this survey will be further processed for scientific purposes only and not for commercial use; all information collected in this survey will be kept, retrieved, and analyzed by researchers only for the purpose of this project. My anonymity is assured and I will not be identified in publications or otherwise without my explicit written consent (Not Selected, Not Selected)

Q2: How old are you? (18-24, 25-34, 35-44, 45-54, 55-64, 65+)

Q3: You are... (male, female, diverse, not specified)

Q4: What is your highest educational qualification? (No degree, Hauptschulabschluss, Polytechnische Oberschule, Realschulabschluss, Fachabitur, Abitur, Fachhochschulabschluss, university degree, other degree)

Q5: In which federal state do you live? (Baden-Wuerttemberg, Bavaria, Berlin, Brandenburg, Bremen, Hamburg, Hesse, Mecklenburg-Western Pomerania, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, Saarland, Saxony, Saxony-Anhalt, Schleswig-Holstein, Thuringia)

Q6: If you add up all the incomes in your household: In which of the following income groups does your monthly household net income fall? (under 900 EUR, 900 EUR to under 1300 EUR, 1300 EUR to under 1500 EUR, 1500 EUR to under 2000 EUR, 2000 EUR to under 2600 EUR, 2600 EUR to under 3200 EUR, 3200 EUR to under 4500 EUR, 4500 EUR to under 6000 EUR, 6000 EUR and more)

Q7: Which of the following devices do you use to connect to the Internet at work and at home, and how often do you use them? (I do not own, Less than two hours a day, Less than four hours a day, More than four hours a day)

Q8: How much do you agree with the following statements regarding cyber threats, i.e., threats on the internet? Note: Cyber threats on the internet include, for example, malware such as computer viruses, data misuse, password and account theft, data espionage, online banking fraud, online shopping scams, insults and bullying, sexual harassment, and hate speech (Strongly disagree, Tend to disagree, Neutral, Tend to agree, Strongly agree)

Q9: How familiar are you with the following institutions, platforms, or measures that contribute to cybersecurity in Germany? (I don't know them at all or have never heard of them, I hardly know them but I have heard the name once, I only roughly know their function or goals, I know their function or goals fairly well, I know their function or goals very well)

Q10: In the last five years, how often have you personally been a victim of the following types of cyber threats? (Don't know, Never, Once, Rarely, Occasionally, Often)

Q11: Which people or organizations do you or would you seek help from if you were the victim of a cyberattack (e.g., malware)? (Never, Rarely, Occasionally, Often, Always)

Q12: How high do you estimate the risk of becoming a victim of one of the following types of cyberattacks in the next five years? (I cannot say, Very low, Rather low, Average, Rather high, Very high)

Q13: How continuously do you use the following security programs or security measures on your personal devices (computer, smartphone, etc.) to protect against cyber threats? (Never, Rarely, Occasionally, Often, Always)

Q14: How much do you agree with the following statements about the prevalence and use, as well as the impact of OSINT? Note: Authorities, governments, and companies collect and analyze information from publicly available sources such as blogs, Facebook, or Twitter in order to gain insights into critical cyber threats or crimes, among other things. Such activities are referred to below as Open-source intelligence (OSINT for short) (Strongly disagree, Tend to disagree, Neutral, Tend to agree, Strongly agree)

Q15: How would you assess the following statements about OSINT activities by security authorities? Note: Authorities, governments, and companies collect and analyze information from publicly available sources such as blogs, Facebook, or Twitter in order to gain insights into critical cyber threats or crimes, among other things. Such activities are referred to below as Open-source intelligence (OSINT for short) (Strongly disagree, Tend to disagree, Neutral, Tend to agree, Strongly agree)

Q16: Which channels do you currently use to find out about cyber threats, security vulnerabilities, and solutions to problems? (Never, Rarely, Occasionally, Often, Always)

Q17: Which channels would you prefer to receive information about cyber threats, vulnerabilities, and problem solutions in the future? Select up to three of the channels you consider most important (Not selected, Selected)

Q18: Which information on cyber threats and recommendations for protective measures are particularly relevant to you and should therefore be communicated with a focus? (Not relevant at all, Little relevant, Somewhat relevant, Rather relevant, Definetely relevant)

Q19: Through which people, programs, or organizations would you like to receive information about important cyber threats, vulnerabilities, and problem solutions in the future? (Strongly disagree, Tend to disagree, Neutral, Tend to agree, Strongly agree)