Towards Secure Urban Infrastructures: Cyber Security Challenges for Information and Communication Technology in Smart Cities

Christian Reuter
Science and Technology for
Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt Hesse Germany

Jasmin Haunschild
Science and Technology for
Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt Hesse Germany

Matthias Hollick
Secure Mobile Networking (SEEMOO)
Technical University of Darmstadt
Darmstadt Hesse Germany

Max Mühlhäuser
Telecooperation (TK)
Technical University of Darmstadt
Darmstadt Hesse Germany

Joachim Vogt
Work and Engineering
Psychology (FAI)
Technical University of Darmstadt
Darmstadt Hesse Germany

Michael Kreutzer
Fraunhofer SIT
Darmstadt Hesse Germany

ABSTRACT

The growth of cities continues to be a global megatrend. As more and more people live in urban areas and urban services and infrastructures are under growing strain, technologies are increasingly being researched and used to make city life more efficient and comfortable. As a result, so-called "Smart Cities" have complex IT infrastructures and cyber-physical systems such as sensor/actuator networks for the general population and are developing worldwide. Urban infrastructure must be secured against attacks, ensuring reliable and resilient services for citizens as well as privacy and data security. This paper introduces selected challenges faced by infrastructure providers, citizens and decision-makers in handling attacks aimed at information and communication technologies (ICT) of urban infrastructures and presents current research avenues for tackling cyberattacks and for developing tools for creating, portraying and disseminating actionable information as one important response to security challenges. It then presents findings from a representative survey conducted in Germany (N=1091) on the experiences and perceptions of citizens concerning the relevance of cyberattacks will be presented.

CCS CONCEPTS

• Human-centered computing -> Collaborative and social computing
• Security and privacy -> Human and societal aspects of security and privacy

Proceedings of the Mensch und Computer 2020 Workshop on «7. Workshop Mensch-Maschine-Interaktion in sicherheitskritischen Systemen».
© Copyright held by the owner/author(s). https://doi.org/10.18420/muc2020-ws117-408

KEYWORDS

Urban infrastructure, Cybersecurity, Smart City, IoT

1. Motivation: Future Cities are Smart Cities

To date, the availability of infrastructure, economic opportunities and easy mobility have led about 50% of the world's population to live in cities. It is predicted that this proportion will rise to 68% worldwide by 2050 [68]. Though the main drivers are to be found in Asia and Africa, this trend is also evident in European and German metropolitan regions [68, 69], leading to increased pressure on city infrastructure. Digitization can help to meet the high demands placed on cities, to make infrastructure more efficient, cities competitive and sustainable and to improve quality of life for urban citizens [4, 20] as well as for citizens in connected and smart regions [5, 38]. Typically, data is collected and used to optimize processes in order to reduce inefficient activity, improve services and increase convenience. Examples are the optimization of traffic flow, matching public transportation demands, sensing of filling levels in waste collection, assisting drivers to find available parking spots, digitization of public administration, etc. Digital infrastructure will thus become a core element of the cities of the future, ranging from communication, mobility and transport, health, energy and smart homes [40] to critical infrastructure (CI).

Current trends in digitalization include the striving for Smart Cities, which can be described as "a place where traditional networks and services are made more flexible, efficient, and sustainable with the use of information, digital and telecommunication technologies, to improve its operations for the benefit of its inhabitants" [41]. Smart cities are further characterized by the capture of large amounts of real-time data (instrumentation), the integration of different data sources (interconnectedness) and the drawing of conclusions from the data (intelligence) [16]. Other definitions encompass social, economic and environmental characteristics, including equitable access to improvements, social capital, high-tech and creative industries or environmental sustainability [9].

In technical terms, this vision means that vast amounts of data are captured, processed, communicated and stored across different systems and devices on different city levels, from households and buildings to city infrastructures, often without human intermediaries (Machine to Machine) and through the internet (incl. Internet of Things (IoT)). These trends depict a city that is both efficient and worth living in, although concerns regarding privacy are also very visible.

However, due to the interconnectedness of devices through ICT, urban infrastructures also constitute a vast attack surface for cyberattacks, that can cascade from one system to another, escalating negative effects. Vulnerabilities affect both private and household devices as well as urban infrastructures [28, 71]. Studies have shown that traffic signalling systems, for example, can be easily manipulated by disruption attacks and ransomware which in turn affects safety on public roads [46]. While much research is directed towards security devices and various infrastructures [63], aiming for robustness, persistence and dependability as well as self-adaptation in response to shocks [20], the current Covid-19 pandemic has again shown that not all challenges can be foreseen or technically solved. In dynamic situations of insecurity, such as when faced with a cyberattack, surveillance of the situation as it unfolds and informed decision making are crucial.

In this paper, we analyse the particular challenges of smart urban infrastructures, looking at the attack surface and cyber-physical interdependencies (Section 2). Giving on overview of current tools for providing actionable information and enhancing the understandability of security challenges (Section 3), we present selected preliminary findings from a representative survey of the German population about citizens' perceptions of infrastructure failures and targets of cyberattacks (Section 4). We end by discussing the implications for future research on actionable information to counter attacks against smart urban infrastructures (Section 5).

2. Challenges for Secure Urban Infrastructures: Attack Surfaces and Cyber-Physical Interdependencies

Despite the development of improved early warning systems [53], the safety challenges to infrastructures, e.g. by storms, earthquakes or tsunamis, remain vulnerabilities for both rural and urban areas. Examples from countries like Indonesia demonstrate that some regions or countries are particularly disaster-prone [64]. To increase preparedness and limit harm, early warning systems are essential–not only with regard to natural disasters but also with regard to cyberattacks. In times of hybrid wars involving not only states but also private actors[50], more and more countries are preparing for such attacks and are therefore systematically working on their own national cyberattack early warning systems [50, 60]. However, cyberattacks differ markedly: in contrast to natural events, they are performed by humans reacting to incentive structures, with the aim of financial or political gain. In addition, they are often caused by weak security implementation, human error or unmaintained systems [48]. Indeed, the existence of cyberattack types is often well-known, but security is not implemented for various reasons [18]. The potential of early warning measures is therefore limited for many types of attacks.

At the same time, infrastructures in interconnected cities are becoming ever more attractive targets for cyberattacks: The global growth of urban centres [68] puts strains on cities, which must provide housing, transportation, healthcare etc. for a growing number of people. In these contexts, the use of IoT devices promises to alleviate the burden on cities through data-based efficiency gains, e.g. in traffic optimization [4]. In the context of large-scale IoT use, particular challenges are posed by the interconnectedness of devices and cyber-physical interdependencies.

The various devices used and their interconnections lead to the presence of a large attack surface with many technical vulnerabilities and the possibility of attacking the "weakest link" in the chain of connected devices [6, 29, 66]. Furthermore, there are numerous cyber-physical interdependencies both between infrastructures and between end users and infrastructures. This means that physical technologies enable cyber infrastructure, while at the same time cyber infrastructure enables physical infrastructures.

These factors make digital cities particularly vulnerable to attacks [37]. Securing the IT systems of smart cities against attacks is a central and complex concern, on the one hand because it affects the many citizens, but on the other hand also because of the centrality of metropolitan areas for regional administration and economy. An attack on a city can therefore have grave impacts on the city and beyond [26], shaking the trust of urban citizens and potentially also politics and the economy. In particular, critical infrastructures, which are central to the running of the smart city as a whole can be affected. At the same time, both important and digitalized cities are particularly attractive targets [12, 62].

Attacks can aim to manipulate gateways between the Data Acquisition Layer and the Connectivity Layer, firewalls can be overcome where data is transmitted to the Data Management Layer, or they can overcome access controls at the Data Application Layer [36]. Attacks can jeopardize the availability of services (availability attack), data and information privacy (confidentiality attack) and the integrity of systems (integrity attack) [37]. Cyberattacks can exploit several vulnerabilities: weak software security and data encryption; use of insecure legacy systems and poor maintenance; human error and deliberate malfeasance; interdependencies and large and complex attack surfaces; and cascade effects [28, 54], which are disruptions of one system that are transmitted to other systems and may also escalated as they disrupt more systems [54]. Important research efforts are enhancing encryption, integrating old and new systems and incorporating humans through usable security. However, despite this important work, on the one hand, security can never be fully attained, nor can the failure of important IT functions be tolerated. Especially in highly digital urban infrastructures, attack surfaces are large and cascading effects prevalent. Therefore, further research is needed, focusing on urban vulnerabilities and ways of reacting in case of cyberattacks.

To make infrastructures resilient, consideration needs to be given to how citizens, as end-users, interact with the technologies [49] and how infrastructure providers and city stakeholders can contribute to infrastructure security. Thus, aspects of safety–referring to the error-free functioning of a system, which might be impaired by natural events or human maloperation–must be considered [57], as well as critical infrastructure reliability and resilience. It is therefore important to build systems that have inbuild redundancies to ensure that attacks' harm is limited and can be repaired efficiently to achieve overall resilience [55]. In order to achieve adequate responses to security attacks, agencies responsible for providing security have to be enabled to correctly assess and react to security threats.

3. Tools for Understandable Attacks and Communication of Actionable Information

Due to the importance of providing essential goods and services and due to the increasing number of cyberattacks on critical infrastructures, there are already numerous empirical and scientific projects addressing a wide variety of issues such as security, geopolitics and economics. In order to gain insight into the existing challenges, a wide range of stakeholders such as engineers, government agencies and scientists have studied risk relationships and cascading effects, relying on simulations in order to gain insights on how infrastructure systems might respond to specific scenarios and how they possibly cascade into another. In this section, research approaches to counter cyberattacks are presented, as well as tools to make reactions to such events understandable and action-oriented. While it is not possible to present all current research approaches and tools developed, we give an overview of current research directions and tools developed for practitioners.

Experiences in recent years have shown that energy supply in particular is critical for the maintenance of other infrastructures. For this reason, projects such as the EU-funded project "Smart Grid Protection Against Cyber Attacks SPARKS", are aimed at risk assessment and ensuring cybersecurity and resilience of smart grids [67]. Another avenue, exemplified by the *European Control System Security Incident Analysis Network* (ECOSSIAN), carried out under the *European Program for Critical Infrastructure Protection* (EPCIP), develops preventive risk management tools such as early warning and anomaly detection. Other research focuses on stress testing, such as the project "InfraStress", funded by the European Union´s Horizon 2020 research and innovation program, which aims to improve resilience of sensitive industry facilities and infrastructure exposed to cyber-physical risks through a testbed. Methods are currently being developed by a consortium of 27 partners from 11 countries. Based on the results, a culture of participatory security will be created and new insights will be trained in free, open online courses in order to involve stakeholders such as workers, public authorities, companies and civil society [22]. Further aspects of training and exchange of technical experience on critical infrastructure can be found in the report "ERNCIP training for professionals in critical infrastructure protection: from risk management to resilience" from the European Commission (2017) [34]. In addition, some companies, that are potential targets of cyberattacks, offer a certain amount of training on the security awareness of their employees in times of growing number of attacks and intrusions. Those trainings can take the form of "web-based classrooms, teleconferencing, instructor led training, thematic cybersecurity events, newsletters and awards/incentives programs" [2]. However, it appears that many trainings are limited to very basic information, which indicates that there is still a great need for training in order to better protect companies against cyberattacks.

Other projects focus on cascade effects: One example is "Risk Relationship and Cascade Effects in Critical Infrastructures" (2015) with focus on the 2011 Japanese triple disaster (earthquake, tsunami and nuclear accident). Together with the *United Nations Office for Disaster Risk Reduction* (UNDRR) different (inter)national actors identified five priority areas concerning disaster risk reduction. In order to gain a better understanding of the key factors, the participating actors identified linkages across key CI sectors and how they relate to each other. To capture and visualize existing relationships, a causal loop diagram and a disaster timeline were created. Afterwards, they examined how such dependencies triggered cascading effects in the context of an actual incident. During the process it became clear that some factors were influencing essential sectors such as telecommunications, banking and transportation and that they have a far-reaching impact on societies. As some interactions have significant implications e.g. on a specific population group (vulnerable people) it is important to keep that in mind during the analysis. By mapping possible cascades, aspects can be identified that will enable people to anticipate what can be done in case of further attacks or disasters. This pre-disaster public awareness will help to decrease damages [39].

With regard to natural events, the concept of resilience also plays an important role. The study "critical infrastructure cascading effects: Disaster resilience assessment for floods affecting city of Cologne and Rhein-Erft-Kreis" (2020) exemplarily demonstrates the viability and limitations "of analyzing lifeline features of interest for disaster risk and emergency management" [14]. Another case study regarding urban flooding in "Torbay", England, seeks to support coastal communities facing upcoming incidents by using proposed methodology from the EU CIRCLE, a pan-European framework for strengthening CI resilience to climate change. Methodological approaches based on various (non-) technical indicators, help to target specific needs [15]. In sum, those studies underline the importance of analysing local risks and resilience characteristics by making cascade effects and CI unambiguous. Local examples may not only help regional actors to allocate their resources better, but also to connect researchers and key decision makers worldwide by exchanging their assessments and findings, doing comparative analyses [52]. Even though there have been and still are several projects on critical infrastructure, further research projects that in particular focus on ICT as the web spanning private households and all urban infrastructures are necessary to understand and communicate the potential security risks.

4. Preliminary Findings: Citizens' Underestimating their Role as Targets

Although previous studies have studied e.g. citizens' perceptions during infrastructure breakdowns [23], a distinction between different reasons was not part of that study. In order to assess the relevance of cyber incidents in comparison to other challenges for citizens, we conducted a survey of the German population (N=1091) that was representative regarding age, gender and formal education, asking about experiences with cyberattacks, as well as about their judgements concerning the likelihood of different types of attacks on different targets.

Our aim was to investigate whether a focus on cybersecurity is in line with citizens' perceptions of the threats urban infrastructures are facing or whether they perceived other factors as more relevant to the continuity of infrastructure. In order to gain a deeper understanding of their reasoning, we wanted to know how these perceptions regarding Germany would differ in comparison to other countries. We chose India as an example of an IT-innovative and growing BRICS country, but low-income country of the Global South. As a second case, we chose the United States of America (US) as another high-income country that is culturally and geographically different from most European countries but politically and economically powerful.

We therefore asked about the perceived problems each in Germany, the US and India as viewed by Germans: "What do you consider to be the probable reasons for an infrastructure failure in [Germany/the US/India]? Please sort by descending probability, starting with the most probable reason." (Figure 1). The results reveal that Germans consider cybercrime, cyberattacks from abroad as well as technical failures as the most likely reasons for infrastructure disruptions in Germany, followed by human failures and natural disasters. This differs from the expectations towards failures in the US, which are deemed to be more likely to be caused by cyber and physical attacks from abroad, while technical and human failures are less expected. Expectations about the likely causes of failures again vary markedly regarding India: Here, Germans assume that damages due to natural disasters occur, while cyberattacks and cybercrime are deemed less critical. Interestingly, civil war is also seen as a markedly more probable cause of failure, while politically motivated terrorism is deemed less likely than in Germany.

While these findings are also interesting regarding an international comparison of actual causes of failures, is it evident that regarding Germany the focus on cyber incidents and security challenges is in line with the perceived urgency of these challenges among the German population, although safety challenges are also considered important.

In addition to ease of use, convenience and affordance, cybersecurity and data protection are keys to society's acceptance of urban infrastructure solutions [30, 31], e.g. as demonstrated by the resistance against smart meters due to privacy concerns [19]. If systems are hacked or data from citizens are "lost", citizens' support for the digitalization efforts suffers. At the political level, adequate consideration of cybersecurity and data protection issues are services of public interest and ensuring that they are provided is a prerequisite for reducing risk-related reputational damage.

This is particularly challenging, as it has been shown that citizens are not always well informed about how to behave online. Even those knowledgeable about IT security behaviour do not always put that knowledge into practice [18]. A similar paradox is found regarding privacy [1, 47].

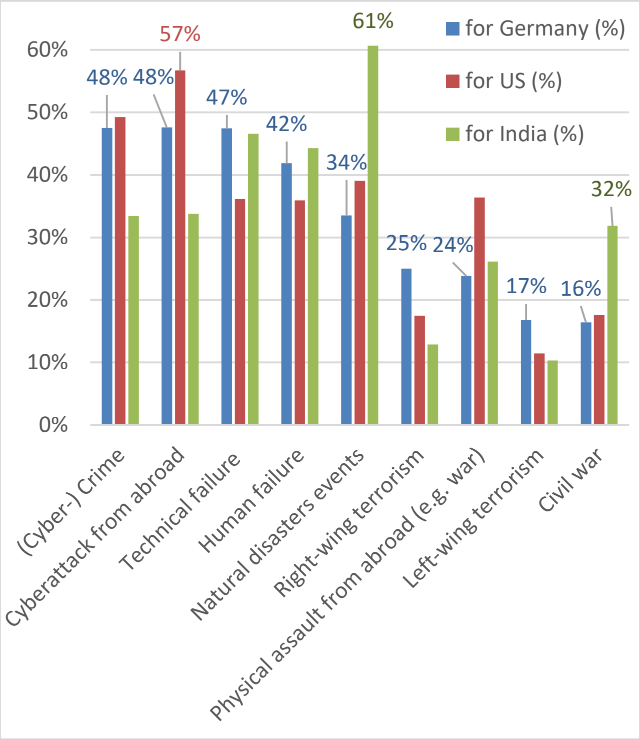

Figure 1: Perceived likely reasons for infrastructure failure as viewed by Germans (Percentage of respondents ranking reason as rank 1, 2 or 3.)

We also wanted to know more about German citizens' experiences and whether their experiences as victims influence their judgement of what constitute attractive targets for cyberattacks. We therefore asked citizens whether they had any personal experience with a list of widespread cyberattacks, which we phrased in the question in laypersons' terms (Figure 2). Almost two thirds had received phishing emails, around one third had downloaded a virus, and one fifth had had an account hacked. 20 % had experience with cyberattacks affecting their work. Overall, only 15 % had not experienced any of these attacks.

When we also asked about the likelihood of a security and privacy attack on the IT of different targets in the near or distant future or ever, a paradox occurred: While this overwhelming majority of the participants reported having been victims of various cyberattacks, less than 10 % thought that they might be the victims of a cyberattack on their private home devices in the next five years, while over 40 % expected an attack on individual politicians.

Our research thus suggests that private users are easy targets for cyberattacks, because they report having been widely targeted and often successfully, while they also appear to underestimate the likelihood of being a target of future cyberattacks. Other studies also show that users rather trust that the producers ensure the privacy of their devices [70], which further reduces the likelihood that citizens will take steps to protect their devices. These findings support other research that identifies end-users as relevant actors in successful attacks [33] and has shown a lack of security awareness, such as optimistic bias [58]. This cognitive bias explains why individuals believe that they have a lower risk of experiencing a negative event compared to others. In the context of information security, this means that despite an increased vulnerability to information security breaches, awareness and commitment regarding information security threats remain low [58]. Nevertheless, user awareness plays an important role in preventing victimization [61]. This finding can be explained by the optimistic bias: The optimism about online privacy breaches is negatively related to the adoption of privacy protective behaviour [7], which makes the individual an easy target for attacks. The optimistic bias is also used to explain the privacy paradox discussed above. So far it has been shown that the experience of infringements of privacy reduces optimism about the personal risk of privacy breaches [7, 11]. However, our results indicate that the risk of others (particularly political actors) is considered high compared to the perception of one's own risk, even though the majority of participants have already experienced various cyberattacks.

We therefore support calls for a stronger focus of research on the behaviour of practitioners and private users with regard to IT security and privacy [35] and suggest that as the use of networked IoT devices increases, private users and infrastructure providers should also be viewed as being interconnected in security attacks.

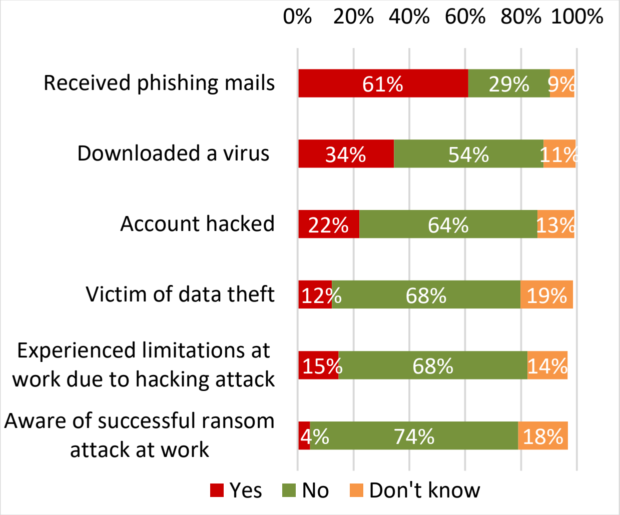

Figure 2: Personal and work-related experience with cyberattacks

5. Discussion: The Connecting Element ICT

The analysis of cities shows their attractiveness as targets of cyberattacks as well as the high likelihood of cyberattacks occurring in cities due to the number of devices available there. The drive towards smart city initiatives as well as the increasing application of sensors and smart devices stands to increase the attack surface further. The operation of smart urban infrastructure is at peril if the availability of secure information and communication systems cannot be guaranteed. To be able to collect, process, and disseminate the vast amount of data generated in both critical infrastructures as well as in other urban cyber-physical infrastructures, communication networks are of utmost importance. Hence, the secure and resilient operation of the critical infrastructure *Information and Communication* is the basis for operation of all other critical infrastructures: Energy, Finance and Insurances, Food, Government and Public Administration, Health, Media and Culture, Transport and Traffic, and Water [20, 45].

In addition, while some differentiate digital security threats either as infrastructure security, meaning the ability to deliver services reliably, or as data/information security [3], there is a significant overlap between the two, with weaknesses in the system exposing data and information and exposed data and information being exploited to interfere with infrastructure [28]. Yet, it is unclear how exactly data and information security interact with infrastructure security. Research should explore the connections between availability attacks, confidentiality attacks and integrity attacks [28]. Both data/information security and infrastructure security should be considered as elements of urban digital security, that ensure the continuous infrastructure services as well as citizens' willingness to engage with them.

Our initial findings underline the relevance of these issues to citizens. They also show that the optimistic bias makes citizens potential weak links as they underestimate their own role as attractive targets for cyberattacks. Despite widespread experiences with different cyberattacks, citizens need additional support in order to receive a realistic impression of likely targets of attacks. Without this shift, citizens are unlikely to adapt their security behaviour accordingly. While our results, based on an online survey, are biased towards people who have at least a minimal level of computer literacy. Surveys show that only 13 % of the German population do not use the internet [13] and are therefore likely not to have any personal experience with cyberattacks and cybercrime. We therefore hold that even though an online survey is not completely representative, particularly regarding internet use, it still provides a very good picture of the overall experiences of the German population.

Providing decision makers with information and tools for information processing, such as visualizations and simulations, should be a core feature in the handling of security incidents. Given the interconnected nature of systems, such information should go beyond individual infrastructures and companies and include considerations of interconnected systems. Technical tools should thus enable such a broader picture, as well as communication with other stakeholders.

Considering the complex interconnections and dependencies between urban infrastructures, understanding and gauging the implications of disruptions on ones' own and other systems, as well as those of end-users is central for taking adequate action.

Securing smart urban infrastructures should therefore include several aims: Firstly, to increase the reliability of ICT in such a way that providers of critical infrastructure can continue to operate without grave limitations. The second aspect should be to empower city stakeholders to understand, act, communicate and collaborate in cases of security infringements, enabling urban stakeholders to identify attacks and to take preventive and reactive measures. The technocratic view of project management of urban digitization projects "[...] typically treats the city as a coherent, rational machine, rather than a complex system full of wicked problems and competing interests" [27]. To do this complexity justice, practitioners and citizens need new tools and practices to assess, monitor and react to security threats and attacks. ICT should be considered as being at the heart of urban infrastructure security issues, not only because it is among the nine critical infrastructures identified by the Federal Office of Civil Protection and Disaster Assistance [20], but also because it spans private household, public spaces and critical infrastructures and has thus some of the greatest potentials to produce cascading effects.

While understanding of security risks and the ability to prepare for and react to attacks has increased through automated warnings and scenarios [51], information sharing [65], as well as through innovation in crisis communication [63], more research should be directed towards visualizing interconnectedness and enabling crosscutting communication in emergencies [59].

Such research should be interdisciplinary to include technical innovation, while doing justice to psychological and organizational realities. For our ATHENE mission "Secure Urban Infrastructures", we will integrate these insights by investigating the relevance of different types of security attacks for urban infrastructure providers and citizens. We will assess the barriers to understanding the implications and effects of different cyberattacks, focusing on technical, organizational, as well as psychological challenges in reacting to such attacks. Our solutions will aim to enable infrastructure providers to consider the effects on other infrastructures and citizens and to respond in a manner that includes communication between all relevant parties.

ACKNOWLEDGMENTS

This work has been funded by the German Federal Ministry of Education and Research (BMBF) and the Hessen State Ministry for Higher Education, Research and Arts (HMKW) within the SecUrban mission of the National Research Center for Applied Cybersecurity ATHENE. This work has also been funded by the LOEWE initiative (Hesse, Germany) within the emergenCITY centre.

REFERENCES

[1] Acquisti, A. et al. 2015. Privacy and human behavior in the age of information. *Science.* 347, 6221 (2015), 509–514.

[2] Adams, M. and Makramalla, M. 2015. Cybersecurity Skills Training : An Attacker-Centric Gamified Approach. Technology Innovation Management Review, January (2015), 5–14.

[3] Aldairi, A. and Tawalbeh, L. 2017. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science.* 109, 2016 (2017), 1086–1091. DOI:https://doi.org/10.1016/j.procs.2017.05.391.

[4] Anagnostopoulos, T. et al. 2015. Robust waste collection exploiting cost efficiency of IoT potentiality in Smart Cities. *2015 International Conference on Recent Advances in Internet of Things, RIoT 2015.* April (2015), 1–6. DOI:https://doi.org/10.1109/RIOT.2015.7104901.

[5] Anthopoulos, L.G. and Vakali, A. 2012. Urban Planning and Smart Cities: Interrelations and Reciprocities Urban Planning: Principles and Dimensions. *The Future Internet Assembly.* (2012), 178–189.

[6] Arabo, A. 2015. Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science.* 61, 0 (2015), 227–232. DOI:https://doi.org/10.1016/j.procs.2015.09.201.

[7] Baek, Y.M. et al. 2014. My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior.* 31, (2014), 48–56. DOI:https://doi.org/https://doi.org/10.1016/j.chb.2013.10.010.

[8] Bunker, D. and Smith, S. 2009. Disaster management and Community Warning (CW) systems: Inter-organisational collaboration and ICT innovation. *PACIS 2009 - 13th Pacific Asia Conference on Information Systems: IT Services in a Global Environment* (2009), 36–48.

[9] Caragliu, A. et al. 2011. Smart cities in Europe. *Journal of Urban Technology.* 18, 2 (2011), 65–82. DOI:https://doi.org/10.1080/10630732.2011.601117.

[10] Chatfield, A.T. et al. 2013. Tsunami early warnings via Twitter in government: Net-savvy citizens' co-production of time-critical public information services. *Government Information Quarterly.* 30, 4 (2013), 377–386. DOI:https://doi.org/10.1016/j.giq.2013.05.021.

[11] Cho, H. et al. 2010. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior.* 26, 5 (2010), 987–995. DOI:https://doi.org/https://doi.org/10.1016/j.chb.2010.02.012.

[12] Eun, Y.-S. and Aßmann, J.S. 2016. Cyberwar: Taking Stock of Security and Warfare in the Digital Age. *International Studies Perspectives.* 17, 3 (2016), 343–360. DOI:https://doi.org/10.1111/insp.12073.

[13] European Commission 2020. *Europeans ' attitudes towards cyber security October 2019, https://op.europa.eu/en/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1.*

[14] Fekete, A. 2020. Critical infrastructure cascading effects. Disaster resilience assessment for floods affecting city of Cologne and Rhein-Erft-Kreis. *Journal of Flood Risk Management.* 13, 2 (2020), 1-9.

[15] Gibson;, M.J. et al. 2020. Case study of the cascading effects on critical infrastructure in Torbay coastal/pluvial flooding with climate change and 3D visualisation. *Journal of Hydroinformatics.* 22, 1 (2020), 77–92.

[16] Harrison, C. et al. 2010. Foundations for Smarter Cities. *IBM Journal of Research and Development.* 54, 4 (2010), 1–16.

[17] Hayat, P. 2016. Smart cities: A global perspective. *India Quarterly.* 72, 2 (2016), 177–191. DOI:https://doi.org/10.1177/0974928416637930.

[18] Herbert, F. et al. 2020. Differences in IT Security Behavior and Knowledge of Private Users in Germany. *Proceedings of the International Conference on Wirtschaftsinformatik (WI)* (Potsdam, Germany, 2020), 1–16.

[19] Hess, D.J. 2014. Smart meters and public acceptance: comparative analysis and governance implications. *Health, Risk & Society.* 16, 3 (2014), 243–258. DOI:https://doi.org/10.1080/13698575.2014.911821.

[20] Hollick, M. and Katzenbeisser, S. 2019. Resilient Critical Infrastructures. *Information Technology for Peace and Security.* Springer Fachmedien Wiesbaden. 305–318.

[21] Hughes, A.L. and Palen, L. Social Media in Emergency Management: Academic Perspective. 349–392.

[22] InfraStress 2020: Who we are, www.infrastress.eu/who-we-are.

[23] Kaufhold, M.-A. et al. 2019. Potentiale von IKT beim Ausfall kritischer Infrastrukturen: Erwartungen, Informationsgewinnung und Mediennutzung der Zivilbevölkerung in Deutschland. *Proceedings of the International Conference on Wirtschaftsinformatik (WI)* (Siegen, Germany, 2019), 1054–1068.

[24] Kaufhold, M.-A. et al. 2020. Rapid relevance classification of social media posts in disasters and emergencies: A system and evaluation featuring active, incremental and online learning. *Information Processing & Management.* 57, 1 (2020), 102132. DOI:https://doi.org/10.1016/j.ipm.2019.102132.

[25] Kaufhold, M.A. et al. 2018. Avoiding chaotic use of social media before, during, and after emergencies: Design and evaluation of citizens' guidelines. *Journal of Contingencies and Crisis Management.* (2018), 198–213. DOI:https://doi.org/10.1111/1468-5973.12249.

[26] Kimani, K. et al. 2019. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection.* 25, (2019), 36–49. DOI:https://doi.org/https://doi.org/10.1016/j.ijcip.2019.01.001.

[27] Kitchin, R. 2016. *Reframing, reimagining and remaking smart cities, The Programmable City Working Paper 20.*

[28] Kitchin, R. and Dodge, M. 2019. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology.* 26, 2 (Apr. 2019), 47–65. DOI:https://doi.org/10.1080/10630732.2017.1408002.

[29] Kolias, C. et al. 2017. DDoS in the IoT. *Computer.* 50, 7 (2017), 80–84. DOI:https://doi.org/10.1109/MC.2017.201.

[30] Lai, P. 2017. the Literature Review of Technology Adoption Models and

Theories for the Novelty Technology. *Journal of Information Systems and Technology Management.* 14, 1 (2017), 21–38. DOI:https://doi.org/10.4301/s1807-17752017000100002.

[31] Lancelot Miltgen, C. et al. 2013. Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. *Decision Support Systems.* 56, 1 (2013), 103–114. DOI:https://doi.org/10.1016/j.dss.2013.05.010.

[33] Lau, L. 2017. Mobile Security: End Users are the Weakest Link in the System. *Mobile Security and Privacy Advances, Challenges and Future Research Directions.* M.H. Au and K.-K.R. Choo, eds. Syngress. 57–66.

[34] Lazari, A. 2017. *ERNCIP training for professionals in critical infrastructure protection: from risk management to resilience.* Publications Office of the European Union, Luxembourg, JRC105204, doi:10.2760/932771,

[35] Li, H. and Van Ryzin, G.G. 2017. A systematic review of experimental studies in public management journals. *Experiments in Public Management Research: Challenges and Contributions.* (2017), 20–36. DOI:https://doi.org/10.1017/9781316676912.003.

[36] Maheswaran, M. and Badidi, E. eds. 2018. *Handbook of Smart Cities. Software Services and Cyber Infrastructure.* Springer.

[37] Makhdoom, I. et al. 2019. Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys and Tutorials.* 21, 2 (2019), 1636–1675. DOI:https://doi.org/10.1109/COMST.2018.2874978.

[38] Mccann, P. and Ortega-argile, R. 2014. Smart specialisation in European regions : issues of strategy , institutions and implementation. 17, 4 (2014), 409–427. DOI:https://doi.org/10.1108/EJIM-05-2014-0052.

[39] McGee, S. 2015. *Risk Relationships and cascading effects in critical infrastructures: Implications for the Hyogo Framework .UNISDR Input Paper.*

[40] Mehmood, Y. et al. 2017. Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE COMMUNICATIONS MAGAZINE.* 55, 9 (Sep. 2017), 16–24. DOI:https://doi.org/10.1109/MCOM.2017.1600514.

[41] Mohanty, S.P. et al. 2016. Everything You Wanted to Know About Smart Cities The Internet of Things is the backbone. *IEEE CONSUMER ELECTRONICS MAGAZINE.* 5, 3 (Jul. 2016), 60–70. DOI:https://doi.org/10.1109/MCE.2016.2556879.

[42] Monfaredzadeh, T. and Berardi, U. 2015. Beneath the smart city: dichotomy between sustainability and competitiveness. *International Journal of Sustainable Building Technology and Urban Development.* 6, 3 (Jul. 2015), 140–156. DOI:https://doi.org/10.1080/2093761X.2015.1057875.

[43] Monzon, A. 2015. Smart Cities Concept and Challenges. *2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS).* (2015), 17–31. DOI:https://doi.org/10.1007/978-3-642-33489-4_4.

[44] Nakashima, E. 2018. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *Washington Post.* (2018), 1–7.

[45] National Strategy for the Protection of Critical Infrastructures (KRITIS-Strategie): 2009. *https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html.*

[46] Ning, Z. et al. 2019. Understanding the Security of Traffic Signal Infrastructure. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, Cham, 154–174.

[47] Norberg, P.A. et al. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs.* 41, 1 (2007), 100–126. DOI:https://doi.org/10.1111/j.1745-6606.2006.00070.x.

[48] Norris, D. et al. 2015. Cybersecurity challenges to American state and local governments. *15th European Conference on eGovernment* (2015), 196–202.

[49] Payne, B.D. and Edwards, W.K. 2008. A brief introduction to usable security. *IEEE Internet Computing.* 12, 3 (2008), 13–21.

[50] Petrenko, S.A. et al. 2017. Problem of developing an early-warning cybersecurity system for critically important governmental information assets. *CEUR Workshop Proceedings.* 2081, (2017), 112–117.

[51] Piskorski, J. et al. 2013. Exploiting Twitter for Border Security-Related Intelligence Gathering. *2013 European Intelligence and Security Informatics Conference* (2013), 239–246.

[52] Priest, S. 2019. Shared roles and responsibilities in flood risk management. *Journal of Flood Risk Management.* 12, 1 (2019).

[53] Wächter, J. and Usländer, T. 2014. The role of information and communication technology in the development of early warning systems for geological disasters: The Tsunami show case. *Early Warning for Geological Disasters.* Springer, Berlin, Heidelberg, 227-252. DOI:https://doi.org/10.1007/978-3-642-12233-0.

[54] Reduction, D. et al. 2015. A definition of cascading disasters and cascading effects : Going beyond the " toppling dominos " metaphor. *Planet@ risk*, 3, 1 (2015), 58–67.

[55] Reuter, C. et al. 2016. Kooperative Resilienz – ein soziotechnischer Ansatz durch Kooperationstechnologien im Krisenmanagement. *Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO).* 47, 2 (2016), 159–169. DOI:https://doi.org/10.1007/s11612-016-0317-7.

[56] Reuter, C. and Kaufhold, M.-A. 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. DOI:https://doi.org/10.1111/1468-5973.12196.

[57] Reuter, C. and Kaufhold, M.-A. 2018. Usable Safety Engineering sicherheitskritischer interaktiver Systeme. *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement.* C. Reuter, ed. Springer Vieweg. 19–40.

[58] Rhee, H.S. et al. 2012. Unrealistic optimism on information security management. *Computers and Security.* 31, 2 (2012), 221–232. DOI:https://doi.org/10.1016/j.cose.2011.12.001.

[59] Rinaldi, S.M. 2004. Modeling and simulating critical infrastructures and their interdependencies. *Proceedings of the Hawaii International Conference on System Sciences.* 37, C (2004), 873–880. DOI:https://doi.org/10.1109/hicss.2004.1265180.

[60] Ruhmann, I. and Bernhardt, U. 2019. Information Warfare–From Doctrine to Permanent Conflict. *Information Technology for Peace and Security.* Springer. 63–82.

[61] Saridakis, G. et al. 2016. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change.* 102, (2016), 320–330. DOI:https://doi.org/10.1016/j.techfore.2015.08.012.

[62] Savitc, H. V. 2005. An anatomy of urban terror: Lessons from Jerusalem and elsewhere. *Urban Studies.* 42, 3 (2005), 361–395. DOI:https://doi.org/10.1080/00420980500034801.

[63] Schulman, P. and Roe, E. 2016. *Reliability and risk: The challenge of managing interconnected infrastructures.* Stanford University Press.

[64] Septia, A.Q. and Indartono, S. 2019. Earthquake Vulnerability in West Nusa Tenggara: Risk Perception, Previous Experience and Preparedness. 323, ICoSSCE 2018 (2019), 207–213. DOI:https://doi.org/10.2991/icossce-icsmc-18.2019.39.

[65] Skopik, F. et al. 2016. A problem shared is a problem halved : A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security.* 60, (2016), 154–176. DOI:https://doi.org/10.1016/j.cose.2016.04.003.

[66] Stellios, I. et al. 2018. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys and Tutorials.* 20, 4 (2018), 3453–3495. DOI:https://doi.org/10.1109/COMST.2018.2855563.

[67] The SPARKS Project, Smart Grid Protection Against Cyber Attack, https://project-sparks.eu.

[68] United Nations 2018. *World Urbanization Prospects: The 2018 Revision.* United Nations Department of Economic and Social Affairs.

[69] Vergleich der Metropolregionen in Deutschland, 2019, Amt für Stadtforschung und Statistikfür Nürnberg und Fürth. *https://www.nuernberg.de/imperia/md/statistik/dokumente/veroeffentlichungen/berichte/sonderberichte/sonderbericht_2016_s252_vergleich_der_metropolregionen_in_deutschland.pdf.*

[70] Zheng, S. et al. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction.* 2, CSCW (2018). DOI:https://doi.org/10.1145/3274469.

[71] Zimmerman, R. and Restrepo, C.E. 2006. The next step: Quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructures.* 2, 2–3 (2006), 215–230. DOI:https://doi.org/10.1504/IJCIS.2006.009439.