Cyber Crises and Disaster Preparation in Austria: A Survey of Research Projects

Bernhard Garn, Klaus Kieseberg, Dominik Schreiber, and Dimitris E. Simos

Abstract In this paper, we survey some recent applied research and development projects dealing with threat analysis and disaster scenario generation, preparation, management, and training funded by the security-focused funding scheme KIRAS by the Austrian government, which include efforts for the development and execution of serious games in the respective domains. In our analysis, we found multiple lines of multiyear, multi-project activities, which consistently improve and advance the technologies and capabilities available to the affected stakeholders. Based on this review of the state of the art, we identify areas of high-potential interest to direct future applied research and development efforts.

Keywords Disaster scenario generation · Serious game · Research project survey

1 Introduction

Over the course of the last decade, various reports in the media about *cyber incidents* have alerted the public to the pivotal role that information technology is playing today, everyday, in all of our lives. These days, serious vulnerabilities in software and hardware often feature a dedicated name, logo, and explanations for the layman. Motivations behind attacks are multifaceted and can serve multiple purposes against various individuals or organizations. *Cyber security* spans all across society; individuals, businesses, and governments are all being targeted in a 24/7, highly interconnected networked world. It is noteworthy that today – among all those nefarious activities online – credit card fraud rarely makes it to the news headlines anymore or is not even mentioned anymore as a major concern explicitly. The term ***comprehensive security*** (*COMPRSEC*) describes the goal of permanently guaranteeing a high level of quality and security for all members of

B. Garn · K. Kieseberg · D. Schreiber · D. E. Simos (✉)
SBA Research, Vienna, Austria
e-mail: bgarn@sba-research.org; kkieseberg@sba-research.org; dschreiber@sba-research.org; dsimos@sba-research.org

I. S. Kotsireas et al. (eds.), *Dynamics of Disasters*, Springer Optimization and Its Applications 169, https://doi.org/10.1007/978-3-030-64973-9_7

society. This broad concept of security includes many domains (e.g., water, food, healthcare system), in particular the **cyber domain**. Due to the pervasiveness of today's technology, the **cyber domain** is part of or plays a part in nearly every other domain captured by *COMPRSEC*. Ergo, its *critical importance* is obvious.

To assess the research landscape in terms of activities, endeavors, and projects that have been carried out to develop, prepare, and test *civil cyber crises* operations on a national level, we survey the publicly available list of official *cyber security research projects* funded by the Austrian[1] government within the *KIRAS* funding scheme [18]. These projects showcase the synergies between academia, subject matter experts (or domain experts), and the government in applied research projects. The goals of these projects is not only to mitigate or – in the best case – prevent primary impacts but also to consider on the same level of importance secondary impacts over all different aspects of society. Several of these projects have led to simulations of disaster scenarios, with some of them being realized in the form of a serious game [54].

Contribution. In particular, this paper makes the following contributions:

- Survey-analysis of applied research projects for cyber crises and disasters within a security-focused funding scheme of the Austrian government for consortia consisting of collaborations between academia, industry, and government;
- Identification of areas and best practices for potentially promising future work for the enhancement of cyber security preparedness, resilience, and capabilities as part of *COMPRSEC*.

This paper is structured as follows. We discuss related activities in Sect. 2, both for cyber-specific serious game exercises and funding schemes. In Sect. 3, we take a look at some of the KIRAS research projects regarding crisis management and disaster response, which outline the current state and the direction of future research in this area. In Sect. 4, we focus our analysis on a series of projects dealing with the modeling of cyber incidents and – in particular – cyber incident scenario training exercises or simulations targeting a nationwide response. We list and comment on some of the extracted best practices in Sect. 5. Finally, with an outlook for potential promising directions future work, we conclude the paper in Sect. 6.

2 Related Activities

The importance of cyber disaster preparation and training gets more and more important, because of the ever-increasing connectivity of our world. Most countries have already witnessed that, through cyberattacks on their government or organizations, which are especially devastating if critical infrastructure is targeted. This

[1] The Republic of Austria is a landlocked East Alpine country in the southern part of central Europe and a member of the European Union.

chapter presents related activities in the field of cyber disaster preparation and training from different countries, to give an overview of the state of the art.

2.1 Department of Homeland Security: Cyber Storm [27]

Cyber Storm is the name of an event, which is hosted by the Department of Homeland Security every 2 years, to exercise how to respond to cyber threats to government networks and other critical infrastructure. The scenarios are specifically crafted, so that no single organization can solve the entire situation, to promote data exchange and cooperation between participants. The last event that was held (Cyber Storm VI) brought together more than 1000 members of the private industry, government, and international partners and took place over a period of 3 days.

2.2 ENISA: Cyber Exercises [28]

ENISA is a European organization managing a wide range of exercises in the field of cyber crises management.

- Cyber Europe: Is an EU-level event held every 2 years, in which cyber incident and crises management exercises for both the public and private sectors from the EU and EFTA Member States are practiced. The presented incidents are inspired by real-life events and developed by European cyber security experts and involve over 1000 participants from across Europe.
- Cyber Exercise Platform (CEP): Is a platform to manage complex exercises and to bring closer the exercise community. It contains information about forthcoming and past exercises and an exercise playground that imitates reality.
- Training and Exercises: ENISA offers cyber incident training and exercises and developed a guide on planning and conducting national exercises. It also conducts surveys on global efforts on this topic.

2.3 EU Horizon [29]

EU Horizon is a research grant of the European Union with a call for proposals to enhance the resilience of our society against natural and man-made disasters, through various methods and tools. Two calls mentioning the development of scenario simulation and exercise tools are:

- Protecting the infrastructure of Europe and the people in the European smart cities.
- Security.

2.4 European Cyber Security Organization [15]

The European Cyber Security Organization is a fully self-financed nonprofit organization. Their goal is to develop a competitive European cyber security ecosystem, to protect the European Digital Single Market, and to provide innovative and trustworthy cyber security solutions to the public and private sector.

2.5 EU NIS Directive [25]

The Directive on security of network and information systems (NIS Directive) is an EU-wide legislation from 2016 that provides legal measures to enhance the overall state of cyber security in the EU. The main points that had to be passed into law by August 2018 by all European countries were:

- Member States are required to be appropriately equipped, e.g., via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.
- Member States have to cooperate with each other by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among them. They also need to set up a CSIRT Network, for operational cooperation on specific cyber security incidents and sharing of information about risks.
- Businesses in sectors that are identified by the Member States as operators of essential services (energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure) have to take appropriate security measures and notify national authorities of serious incidents that get detected.

2.6 NATO CCD CoE [3]

The NATO Cooperative Cyber Defense Center of Excellence is a multinational and interdisciplinary cyber defense hub. They provide their members with continually improving training and exercises on the topic of cyber incident response. Some of their exercises include:

- Locked shield: a unique international cyber defense exercise offering the most complex technical live-fire challenge in the world.
- Crossed Swords: technical red teaming cyber exercise organized by the CCD-COE since 2016.

While some of their training courses include:

- Strategic Level Training: Executive Cyber Seminar.
- Operational Level Training: Integration Cyber Considerations into Operational Planning Course, Operational Cyber Threat Intelligence Course, Critical Information Infrastructure Protection Course.
- Legal Training: International Law of Cyber Operations Course.

2.7 CyberROAD [13]

CyberROAD is a research project funded by the European Commission. It aims to identify the research gaps needed to enhance the security of individuals and society as a whole against forms of crime and terrorism conducted via and within cyberspace. This research addresses current technologies to some extent, but its main challenge is to anticipate tomorrow's world of interconnected living, in particular the dangers and challenges arising from the further incorporation of the digital world into our offline life.

3 General Crisis Management and Natural Disasters

The funding scheme KIRAS is focused on *security research*, whereby this expression is to be understood in the most general interpretation, taking a multidimensional, long-term, multidisciplinary, and holistic point of view. As a result, many research domains fall within this broad research program, and the list of topics of interest ranges from security and threat analysis to dedicated product developments. Critical infrastructure sectors include energy, water, and food supply; health and financial system; public safety; traffic and transportation; scientific infrastructure; and communication and information systems. The strategic goals of the KIRAS funding scheme are:

- Increase of the security and security awareness of citizens;
- Generation of required political security policy knowledge;
- Achieve a leap toward the next generation in terms of science, processes, and technology;
- Growth of national security businesses;
- Creation and expansion of excellence in the domain of *security research*.

It is important to point out that these goals are not regarded as purely technical goals, but are also considered within the context of social and humanities sciences. Hence, an additional goal is the consideration the societal impact of any aspect of *security research*.

The general problems concerning the management of critical situations as well as most aspects of natural disasters have been researched and prototypically implemented over a wide range of applied research projects in this area. These projects range from general crisis management to solutions to specific types of emergencies, for example, caused by system failures, technical defects, scarcity of vital materials, or natural disasters and cover both proactive measures like risk analysis and threat modeling and reactive measures.

In recent years, a lot of research effort has gone into the development of tools and solutions for risk assessment and risk management in critical infrastructure. The KIRAS project **MetaRisk** [20], for example, introduces a sensor -based risk analysis and management system, which, in the course of the project, is implemented in a software demonstrator[41]. Another project **Cerberus** [4] presents a novel approach to identify interdependencies potential cascading effects within a network of critical infrastructures [44].

In crisis management, effective communication and information management play an important role, and a lot of work has been conducted in ensuring and improving the distribution of information needed for a successful outcome. Here, a big challenge lies in the successful coordination of all the actors involved, especially cooperation between military and nonmilitary organizations proves often difficult, due to the different organizational structures and the use of highly specialized ICT (information and communications technology) infrastructure among armed forces [39]. The KIRAS project **INKA** [16] provides a solution for this problem, introducing an interoperability interface for authorities and organizations tasked with disaster management that supports standardized IT-supported information and communication channels. The integration of the Austrian Armed Forces in this information network helps improving the cross-organizational information exchange and aids the collaboration between civil crisis response organizations and public security organizations [33]. Assuring efficient communication between crisis management centers and the public is topic of the project **Public Warning and Alert System for Austria** (**PASA**) [22]. Here, the authors introduce a novel system for alerting the public via the means of different types of media [43].

Regarding disaster management, one of the biggest challenges is guaranteeing the continued supply of the area affected with goods as well as with food, power, and water. The project **Risiko- und Krisenmanagement für die Ernährungsvorsorge in Österreich** (**EV-A**) [23] analyzes the role of private producers and retailers in the case of disaster relief and elaborate on potential policy plans for guaranteeing food supply in Austria in case of disaster situations. Similarly, the project **Providentia** [21] provides (public) procurers with a catalog of measures which could help in ensuring the security of supply in times of crisis and natural disasters. Another project concerning the distribution of goods in disaster situations is **LMK-MUSE** [19]. Here, the authors introduce a cloud-based framework designed to help coordinate last-mile distribution of food and goods to disaster-stricken areas between multiple organizations, both private and public. A specially developed simulation and operations research toolkit allows to identify real-time schedules of relief shipments, leading to a more efficient disaster relief [26]. The toolkit also aids decision-makers by providing a detailed overview of the situation at hand and, additionally, features an integrated agent-based simulation framework that could be used for training purposes.

4 Cyber Crises

A *cyber crisis* or a *cyber incident* belongs to the specific concept of *cyber security*, as part of the general *COMPRSEC* domain. Many different issues have also already been considered in this domain. Conducted project nearly covers the complete range of information technology that thoroughly permeates our modern society.

Activities include the behavior-based anomaly detection in cyber-physical systems [9], a study focusing on for Austria relevant stakeholders as basis for the generation of recommendations for guaranteeing cyber security in transportation systems in Austria [14]. Moreover, special attention was given to the mitigation of *social problems* in cyberspace. To this end, one goal of the project **Cyber Heroes** [12] was the specific promotion of widespread use of *counter speech*, i.e., employing targeted and selective counter messages with the goal of delegitimization of the originally problematic content online and subsequently to incite changes in the discourse norms. Furthermore, the project **(K)ein Raum** [17] aims to describe the various different forms and impacts of cyberattacks against women, who were victims of domestic abuse, often caused by ex-partners. The results of the conducted study will be used to create foundations for the demand and potential ways to support and protect affected women. To be able to illustratively quantify the prevalence of activities relevant to criminal investigations occurring in social media online, the project **Cyber Crime** [11] conducted a representative qualitative survey of Austrian social media users.

A lot of research efforts have been dedicated toward the analysis of cyber crises, responses and preparatory measures as well as the generation of training scenarios in the form of serious games with corresponding interactive simulation environments (i.e., game play infrastructure).

In 2012, the **Computer Emergency Response Team Kommunikations-Modell** (**CERT-Komm**) [5] project was started. It is the first project in a planned series of projects funded by the Austrian government, to analyze the current state of the art of communication between CERTs and their partners, together with their requirements and problems. Since CERTs have to react to various kinds of emergencies, affecting different kinds of industry sectors and companies, reliable and easy-to-use communication systems are of paramount importance. The results of their findings were used as a basis for follow-up projects.

Two years later in 2014, the **Computer Emergency Response Team Kommuni kations-Modell II** (**CERT-Komm II**) [6] project began, which is the follow-up project of **CERT-Komm**. The results from the studies conducted during the first project were used to create communication models for CERTs and their partners, to efficiently persist and exchange information among each other. This collectively managed information can then be used to detect or defend against cyber threats easier. For implementation of the communication models developed in this project, another follow-up project was planned [34, 35].

Starting in 2010, the goal of the project **Cyber Attack Information System** (**CAIS**) [2] was to develop two tools as foundational basis for a comprehensive cyber attack information system for the analysis and assessment of cyber attacks. The focus was on the development of a framework incorporating modeling, analysis, and simulation capabilities for IT infrastructure and – in particular – their interdependencies. This framework was designed to be able to quickly identify problems and to subsequently immediately simulate threats as guidance for the development of counter measures. In addition, another tool was developed with the capabilities for analysis and assessment of current attacks and anomalies based on multiple data sources [50, 51, 37, 38].

One year later, in 2011, the project **SCUDO** [24] started, which had the goal of testing an optimized emergency response training process, which had been specifically adapted to the requirements of Austrian businesses and to derive recommendations based upon it. Additionally, an evaluation of international standards regarding their applicability in Austria was conducted. Several emergency training scenarios were developed with project partners, which were subsequently executed with company partners representing critical infrastructures [36].

In 2012, the growing interdependencies between networks and the use of standard ICT products resulted in a increasing number of cyber security issues in critical infrastructures. In order to improve the resilience of critical systems against cyber attacks, the KIRAS project **Cyber Incident Information Sharing** (**CIIS**) [7] has been introduced. Its aim was the development of mechanisms used to analyze information about activities and attacks in ICT networks belonging to critical infrastructures, as well as the development of methods and technologies for the exchange of information regarding cyber-incidents across organizational borders [31, 47, 48, 32, 53, 55, 45].

Based upon a consistent fusion of existing research activities [42], the **Cyber Incident Situational Awareness** (**CISA**) [8] project started in 2014 to develop a process to establish cyber situational awareness as a scientifically sound concept. It was recognized that solutions – at the operational and technical level – already existed for collecting and aggregating of information concerning cyber threats, as well as for the strategic level existing research had already dealt with the assessment and subsequent handling of cyber threats based upon cyber situational awareness pictures [53]. However, it turned out that there was a knowledge gap concerning how – specifically – the technical information should be processed, presented, and integrated into the cyber situational awareness picture. Therefore, one goal of the **CISA** project was to develop a holistic definition of the expression of *cyber situational awareness* for both a military and a civilian perspective. Moreover, the involvement of legal experts will ensure a legislative view on all considered concepts and the specific demonstrators. Particular attention was given to legal implications and regulations, including issues of data protection, privacy, and liability [40].

Widespread reports about security incidents in 2016 exemplified the complexity of occurring cyber attacks (e.g., phishing, ransomware, DDoS, etc.). These events suggest that a nationwide cyber incident targeting some aspects or functionality of critical infrastructure is only a matter of time. Simultaneously, calls to enhance the cyber resilience via real-time security training simulations are being issued from various sources, including the EU NIS Directive or ENISA cyber Europe. Based on these observations, starting in 2017, the **Austrian Cyber Crises Support Activities** (**ACCSA**) [1] project prepared for cyber crises with comprehensive training, exercise, and evaluation concepts for all stakeholders in the cyber crisis management, thereby reducing response times and error rates in the event of a real cyber crisis [52]. The envisioned concepts, processes, and methods were supported by the implementation of an accompanying software toolbox [30]. This system for software-supported training and exercise spans over several communication levels (e.g., engineering, management, first responders, policy makers) [46, 49]. In addition, the project team included legal experts to examine and evaluate the options and actions developed or proposed in complex nationwide cyber incident scenarios and to assess whether the taken decisions actually also comply with the applicable legal framework (e.g., NIS Directive, GDPR, etc.).

Continuing the successful line of work regarding cyber security incident training and simulation, starting in 2019, the **Cyber security exercise concept and framework** (**CURSOR**) [10] project aims for the conception of a national cyber exercise program and their analysis. A cyber exercise platform will be specified, and a proof-of-concept exercise calendar will be implemented. The **CURSOR** project will develop a nationwide exercise program, taking into account nationwide and sector-specific program exercises. The integrative design of the exercise platform will enable the measurement and comparison of different exercises. The envisioned results of this project are expected to strengthen the strategic coordination of cyber exercises and, consequently, increase Austria's resilience against the potentially serious impacts of cyber attacks on critical infrastructures.

5 Findings & Insights

In this section, we formulate several goals as general outline for future projects and activities addressing cyber disasters. These insights are based upon the observations that have arisen as part of our survey.

Repetition: A recurrently carried out training exercise and a carefully planned evaluation of the prepared response plans is crucial to guarantee its functionality when needed.

Diversification: A diverse group of participants (regarding background, qualifications, and skills) in training exercises leads to a more representative and accurate depiction of real-life emergency cases. Including experts from multiple organizations and different business sectors will also improve cooperation and information sharing skills. Only through cooperation of experts from different sectors can effective, technically sound, useful, and lawfully solutions be newly found in emergency situations or selected from an already available, agreed-upon, accepted, ex-ante generated list.

Level of detail: It is necessary to consider scenarios at different levels of abstraction. Although many actions on the lowest level are direct consequences of higher-level decisions, one should always be aware that ultimately actions at the lowest level have to be *performed*, which requires – at least – the formal legal authority to execute them. Even if higher-level policies are legally sound, this does not necessarily mean that all derived actions (independent of their level in the "chain of command") inherit this justification. A failure at the lowest level should also be treated as such.

Scale and scope: Training exercises should increase in scale and scope, both in terms of participants and training scenarios, to deal with the difficulties of information exchange and the always increasing connectivity and complexity of the world.

Continuing evaluation: Training courses, scenarios, and exercises should regularly be re-evaluated to take new technologies, infrastructure, and other developments into account.

Abstract modelings: Make use of well-established modeling and formalization methods for scenario generation. Build abstract models, and use mathematical and statistical approaches both for the generation and the evaluation of results.

Automation: Automation of scenario generation and exercise environment reduces time and cost.

6 Conclusion

In this work, we surveyed some of the applied research projects carried out within the KIRAS funding scheme in Austria dealing with the preparation for cyber crises and disasters on a national level in Austria. In our analysis, we paid particular attention to disaster simulation and training efforts, as well as to the development and usage of serious games within these projects.

A key finding is that some projects together form a coherent timeline resulting in an incremental increase of knowledge via building on top of each other in terms of achieved research results, insights, and produced software artifacts.

While generally a lot has been done so far, based on the results of our conducted analysis surveying these projects, we have identified potential areas of interest to focus future efforts on, which could benefit from more research, planning, and field testing to ensure the optimal preparedness of all stakeholders involved for a better, more resilient, and safer Austria in the future.

Acknowledgments SBA Research (SBA-K1) is a COMET Center within the framework of COMET – Competence Centers for Excellent Technologies Program – and funded by BMK, BMDW, and the federal state of Vienna. The COMET Program is managed by FFG.

References

1. ACCSA. https://www.kiras.at/gefoerderte-projekte/detail/d/accsa-austrian-cyber-crises-support-activities/. Accessed: 2020-09-22.
2. CAIS. https://www.kiras.at/gefoerderte-projekte/detail/d/cais-cyber-attack-information-system/. Accessed: 2020-09-23.
3. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. https://ccdcoe.org/. Accessed: 2020-09-22.
4. Cerberus. https://www.kiras.at/gefoerderte-projekte/detail/d/cerberus/. Accessed: 2020-09-23.
5. CERT-Komm. https://www.kiras.at/gefoerderte-projekte/detail/d/cert-komm/. Accessed: 2020-09-23.
6. CERT-Komm II. https://www.kiras.at/gefoerderte-projekte/detail/d/cert-komm-ii/. Accessed: 2020-09-23.
7. CIIS. https://www.kiras.at/gefoerderte-projekte/detail/d/ciis-cyber-incident-information-sharing/. Accessed: 2020-09-22.
8. CISA. https://www.kiras.at/gefoerderte-projekte/detail/d/cisa-cyber-incident-situational-awareness/. Accessed: 2020-09-22.
9. CPS-Security. https://www.kiras.at/gefoerderte-projekte/detail/d/cps-security/. Accessed: 2020-09-22.
10. CURSOR. https://www.kiras.at/en/financed-proposals/detail/d/cursor-cyber-security-exercise-concept-and-framework/. Accessed: 2020-09-22.
11. Cyber Crime. https://www.kiras.at/gefoerderte-projekte/detail/d/cyber-crime/. Accessed: 2020-09-22.
12. Cyber Heroes. https://www.kiras.at/gefoerderte-projekte/detail/d/cyber-heroes/. Accessed: 2020-09-22.
13. CyberRoad: Home. http://www.cyberroad-project.eu/. Accessed: 2020-09-22.
14. CybSiVerkehr. https://www.kiras.at/gefoerderte-projekte/detail/d/cybsiverkehr/. Accessed: 2020-09-22.
15. ECSO - European Cyber Security Organisation. https://www.ecs-org.eu/. Accessed: 2020-09-22.
16. INKA. https://www.kiras.at/gefoerderte-projekte/detail/d/inka/. Accessed: 2020-09-23.
17. (K)ein Raum. https://www.kiras.at/gefoerderte-projekte/detail/d/kein-raum-cyber-gewalt-gegen-frauen-in-ex-beziehungen/. Accessed: 2020-09-22.
18. KIRAS - Security Research. https://www.kiras.at/en/home/. Accessed: 2020-09-22.
19. LMK-MUSE. https://www.kiras.at/gefoerderte-projekte/detail/d/lmk-muse/. Accessed: 2020-09-22.
20. MetaRisk. https://www.kiras.at/gefoerderte-projekte/detail/d/metarisk/. Accessed: 2020-09-23.
21. Providentia. https://www.kiras.at/gefoerderte-projekte/detail/d/providentia-erhoehung-des-sicherheitsniveaus-oesterreichs-durch-sichere-beschaffung/. Accessed: 2020-09-23.
22. Public Warning and Alert System for Austria. https://www.kiras.at/gefoerderte-projekte/detail/d/pasa/. Accessed: 2020-09-22.
23. Risiko- und Krisenmanagement für die Ernährungsvorsorge in Österreich. https://www.kiras.at/gefoerderte-projekte/detail/d/risiko-und-krisenmanagement-fuer-die-ernaehrungsvorsorge-in-oesterreich-ev-a/. Accessed: 2020-09-22.
24. SCUDO. https://www.kiras.at/gefoerderte-projekte/detail/d/scudo/. Accessed: 2020-09-22.

25. The Directive on security of network and information systems (NIS Directive) | Shaping Europe's digital future. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. Accessed: 2020-09-22.
26. Romana Berariu, Christian Fikar, Manfred Gronalt, and Patrick Hirsch. Understanding the impact of cascade effects of natural disasters on disaster relief operations. *International Journal of Disaster Risk Reduction*, 12:350 – 356, 2015.
27. Cybersecurity & Infrastructure Security Agency, Department of Homeland Security, The White House. Cyber Storm. https://www.cisa.gov/cyber-storm-securing-cyber-space. Accessed: 2020-09-22.
28. ENISA. Cyber Exercises. https://www.enisa.europa.eu/topics/cyber-exercises. Accessed: 2020-09-22.
29. EU. Secure societies – Protecting freedom and security of Europe and its citizens. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens. Accessed: 2020-09-22.
30. M. Frank, M. Leitner, and T. Pahi. Design considerations for cyber security testbeds: A case study on a cyber security testbed for education. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, pages 38–46, 2017.
31. Ivo Friedberg, Florian Skopik, and Roman Fiedler. Cyber situational awareness through network anomaly detection: state of the art and new approaches. *e & i Elektrotechnik und Informationstechnik*, 132(2):101–105, 2015.
32. Ivo Friedberg, Florian Skopik, Giuseppe Settanni, and Roman Fiedler. Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, 48:35–57, 2015.
33. Ivan Gojmerac, Christoph Ruggenthaler, Maria Egly, Wolfgang Vorraber, Julia Brugger, Helmut Aschbacher, Katrin Panzenbock, and Markus Christian. Advanced information systems for enhanced civil-military interoperability in austria. pages 1–8, 12 2016.
34. Otto Hellwig, Gerald Quirchmayr, Edith Huber, Timo Mischitz, and Markus Huber. Towards a cert-communication model as basis to software assurance. In *2015 10th International Conference on Availability, Reliability and Security*, pages 481–485. IEEE, 2015.
35. Edith Huber. *Sicherheit in Cyber-Netzwerken: Computer Emergency Response Teams und ihre Kommunikation*. Springer-Verlag, 2015.
36. Peter Kieseberg. Research and innovation. *Augmented R ealit y*, page 28.
37. Helmut Leopold. Cyber situational awareness. *e & i Elektrotechnik und Informationstechnik*, 132(2):97–100, 2015.
38. Helmut Leopold, Florian Skopik, Thomas Bleier, Josef Schröfl, Mike Fandler, Roland Ledinger, and Timo Mischitz. Einleitung zum cyber attack information system. In *Cyber Attack Information System*, pages 1–12. Springer, 2015.
39. G. Lichtenegger, W. Vorraber, I. Gojmerac, A. Sporer, J. Brugger, E. Exner, H. Aschbacher, M. Christian, and S. Voessner. Identification of information gaps in civil-military cooperation in disaster management. In *2015 2nd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pages 122–129, 2015.
40. Bernd Malle, Peter Kieseberg, Edgar Weippl, and Andreas Holzinger. The right to be forgotten: Towards machine learning on perturbed knowledge bases. In *Availability, Reliability, and Security in Information Systems*, 2016.
41. Christian Meurers, Johannes Göllner, Stefan Schauer, Stefan Schiebeck, Andreas Peer, and Martin Stierle. Meta risk model for critical infrastructures. In *European Meetings on Cybernetics and Systems Research 2014*, pages 616–621, 2014.
42. Timea Pahi, Maria Leitner, and Florian Skopik. Analysis and assessment of situational awareness models for national cyber security centers. pages 334–345, 01 2017.
43. A. Preinerstorfer, M. Egly, I. Gojmerac, C. Hochwarter, C. Schuster, and R. Stocker. Requirements for the next generation public warning and alert system for austria. In *2017 14th International Conference on Telecommunications (ConTEL)*, pages 115–122, 2017.

44. S. Schauer, S. Rass, S. König, Thomas Grafenauer, and Martin Latzenhofer. Analyzing cascading effects among critical infrastructures. In *ISCRAM*, 2018.
45. Giuseppe Settanni., Florian Skopik., Yegor Shovgenya., and Roman Fiedler. A collaborative analysis system for cross-organization cyber incident handling. In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy - Volume 1: ICISSP,*, pages 105–116. INSTICC, SciTePress, 2016.
46. F. Skopik and S. Filip. Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–8, 2019.
47. F. Skopik, G. Settanni, R. Fiedler, and I. Friedberg. Semi-synthetic data set generation for security software evaluation. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, pages 156–163, 2014.
48. F. Skopik, M. Wurzenberger, G. Settanni, and R. Fiedler. Establishing national cyber situational awareness through incident information clustering. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–8, 2015.
49. Florian Skopik. The limitations of national cyber security sensor networks debunked: Why the human factor matters. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019*, page 405. Academic Conferences and publishing limited, 2019.
50. Florian Skopik, Thomas Bleier, and Roman Fiedler. Information management and sharing for national cyber situational awareness. In *ISSE 2012 Securing Electronic Business Processes*, pages 217–227. Springer, 2012.
51. Florian Skopik, Roman Fiedler, and Otmar Lendl. Cyber attack information sharing. *Datenschutz und Datensicherheit-DuD*, 38(4):251–256, 2014.
52. Florian Skopik, Tímea Páhi, and Maria Leitner. *Cyber Situational Awareness in Public-Private-Partnerships*. Springer.
53. Florian Skopik, Giuseppe Settanni, and Roman Fiedler. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 60:154–176, 2016.
54. Aleksandra Solinska-Nowak, Piotr Magnuszewski, Margot Curl, Adam French, Adriana Keating, Junko Mochizuki, Wei Liu, Reinhard Mechler, Michalina Kulakowska, and Lukasz Jarzabek. An overview of serious games for disaster risk management – prospects and limitations for informing actions to arrest increasing risk. *International Journal of Disaster Risk Reduction*, 31:1013 – 1029, 2018.
55. M. Wurzenberger, F. Skopik, G. Settanni, and R. Fiedler. Beyond gut instincts: Understanding, rating and comparing self-learning idss. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–1, 2015.