CIP-NCT: Critical Infrastructure Protection – Novel Concepts and Technologies

SECURWARE 2017: The Eleventh International Conference on
Emerging Security Information, Systems and Technologies
http://www.iaria.org/conferences2017/SECURWARE17.html

Stefan Schauer
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
e-mail: stefan.schauer@ait.ac.at

Martin Latzenhofer
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
e-mail: martin.latzenhofer@ait.ac.at

***Abstract*— Critical Infrastructures together with their utility networks play a crucial role in the societal and individual day-to-day life. A failure within critical infrastructures might have huge impacts on the economy, environment, population and society in general. Thus, the estimation of potential threats and security issues as well as an appropriate assessment of the respective risks is a core duty of critical infrastructure providers. In this special track, we want to focus on novel methodologies, concepts and tools especially for the protection of critical infrastructures. The objective is to discuss novel approaches from different fields of application, i.e., physical aspects, cyber aspects and societal aspects. In this context, this special track provides a platform for introducing conceptual work (e.g., frameworks and best practices), technical solutions (e.g., tools and prototypes) as well as empirical studies.**

Keywords- critical infrastructure; cybersecurity; uncertainty representation; expert elicitation; soft systems methodology; socio-technological analysis; stochastic interdependencies analysis.

I. INTRODUCTION

The aim of this CIP-NCT special session is to provide a platform for researchers in Information and Communication Technologies (ICT) as well as risk management working on the specific field of critical infrastructure protection. This area came more and more into focus of the general public as well as the scientific community. Nowadays, Critical Infrastructures (CI) are maintaining the backbone supply chains of modern society. For instance, electrical power generation and distribution, water supply and gas plants, as well as telecommunication networks, amongst others, are essential for general public's everyday life. Additionally, a CI is highly interdependent on other CIs. A possible failure of such a critical infrastructure has a significant impact on general public's everyday life and welfare. Their protection is considered to be essential for the orderly functioning of a society, its economy and national sovereignty [1].

The CIs apply physical and cyber-based systems to monitor and control their underlying utility networks. Hence, these organizations are heavily relying on ICT systems as well as Industrial Control Systems (ICS) used in utility networks for the monitoring, control and automation of operational plants for providing their services. Over the last years, utility providers have moved more and more into the target of hackers, cyber criminals and cyber terrorists and the number of attacks on utility providers has significantly increased [2]. In general, the attack types involving the human factor as the weakest link, e.g., social engineering, phishing as well as malware (and especially the spreading of ransomware) seem to be most successful, which has been shown during the recent global ransomware infections with WannaCry [3][4] and (Not)Petya [5][6][7]. In particular, those attacks are also applied in the course of highly targeted attacks like advanced persistent threats (APTs). Such APT attacks on utility providers have severe effects on the general operation of their utility networks, as recent events have shown in Ukraine [8][9][10][11] and Japan [12][13].

Providing protection in terms of security, safety and resilience in utility networks is inherently considered to be of vital importance. This is also due to the fact that in the past few decades a significantly increased demand on utilities has been experienced, which led to resulting in an increased rate of automation in network controls and interconnections. This also resulted in growing number of dependencies amongst various kinds of utility networks. Due to the importance of critical infrastructures, the European Commission introduced an action plan [14], where it proposes the development of a framework consisting of five pillars, namely: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; criteria for the ICT sector. Additionally, the U.S. Department of Home Security defined the need for a resilience framework in CIs [15], focused on the abilities of robustness, resourcefulness, rapid recovery, and adaptability. In the US, the need for protection of critical infrastructure has further been recognized and the National Infrastructure Protection Plan [16] has been introduced to help critical infrastructure communities developing technologies, tools and process that address near-term needs for the security and resilience. Recently in Europe, the "Directive on Security of Network and Information Systems" (also known as the NIS Directive) [17] was launched to ensure a high level of network and information security, improve the security of provider of critical services and digital contents.

For this special track, we received interesting contributions covering especially the earlier stages in the risk management lifecycle. The first two articles discuss some issues setting up the process in order to perform scoping and risk data elicitation. The third one focuses on the complexity of interconnected networks and the task of assessing the interdependencies among different CIs.

II. SUBMISSIONS

One of the main starting points in the operative risk management life cycle is the first estimation of the risk factors, usually performed by many different persons with different skills, attitudes and expert knowledge. The first article "Visual Risk Specification and Aggregation" by Jasmin Wachter, Thomas Grafenauer, and Stefan Rass discusses new ideas dealing with the inherent subjectivity of the risk managers when estimating impacts and likelihoods regarding threats [18]. Both quantities are usually uncertain, subjective and therefore difficult to estimate in a quantitative manner. Hence, risk assessments are often done in categorical terms, which avoid the necessity of finding numeric figures where there is typically no accuracy but rather a significant amount of uncertainty or fuzziness not transparently shown by the final selection. Additionally, there is a need to cope with multiple diverging opinions on the same risk as well. Wachter, Grafenauer, and Rass propose a graphical approach to tackle both issues on a single ground, by casting a common visual risk representation form into a visual risk specification system. The introduced method supports the specification of risk parameters under uncertainty, as well as opinion pooling based on the so-obtained results.

The second work is proposed by Thomas Schaberreiter, Chris Willis, Gerald Quirchmayr, and Juha Röning and is entitled "Addressing Complex Problem Situations in Critical Infrastructures using Soft Systems Analysis: The CS-AWARE Approach" [19]. It focuses on the immanent difficulties to scope the risk operation field appropriately. Complex cybersecurity solutions require a holistic approach to provide comprehensive security to their users. The paper introduces a new way of thinking about cybersecurity, also pursued by the upcoming NIS Directive of the European Union: cooperation and collaboration among individual actors as a way to improve the security situation for society and economy. In this article, Schaberreiter, Willis, Quirchmayr, and Röning present a system and dependency analysis based on soft systems thinking that is able to capture the relations between assets and its internal and external dependencies in the complex systems of organizations like critical infrastructures. The analysis is performed in a socio-technological manner, the human aspect of the systems is considered as important as the technical or organizational aspects. As a use case, the authors present the European Horizon 2020 project CS-AWARE, which relies on the presented approach as a core concept.

Finally, the third contribution is "Stochastic Dependencies between Critical Infrastructures" written by Sandra König and Stefan Rass [20]. The paper concentrates on the fact that critical infrastructures typically imply various interdependencies. Consequently, effects of a partial failure of a critical infrastructure provider are hard to predict unless strict assumptions are made in advance. This complexity between different critical infrastructure networks raises new challenges for a professional risk management of critical infrastructures. For instance, the damage depends on the availability of substitutes but also on external influences such as weather, temporary demand or load peaks, etc. König and Rass propose a stochastic model where the state of an infrastructure is a random variable. Each infrastructure changes its state depending on how the other CIs react, based on a probabilistic change transition regime. This allows to model complex interdependencies, which underlying dynamics may be stochastic or deterministic yet partly unknown. The model of the entire CI thus consists of several Markov chains which retain simplicity for implementation in software such as R, and flexibility to capture various forms of mutual influence between CIs.

III. CONCLUSION

The CIP-NCT special session includes a broad range of topics related to critical infrastructure protection, covering different stages in the risk management life cycle. It emphasizes the beginning by setting up appropriate environment conditions – estimation of risk factors, preparing the scoping – and concludes with discussing the complexity of interdependency handling.

ACKNOWLEDGMENT

We would like to thank the organizers of SECURWARE 2017, Petre Dini, Steve McGuire and especially the whole logistics team behind for their tireless efforts and for accepting CIP-NCT as a special track. We also thank the members of the program committee for their hard work with the reviews and feedback. Last, but not least, we are very thankful to the authors for their very interesting contributions.

The organization of this special track as well as the contributions presented therein were financially supported by the project "Cross Sectoral Risk Management for Object Protection of Critical Infrastructures (CERBERUS)", funded by the Austrian Research Promotion Agency under grant no. 854766.

REFERENCES

[1] European Union Agency for network and information security(ENISA), "Overview of current and emerging cyber-threats," *Threat Landsc.*, 2013.

[2] E. Kovacs, *Researchers Hack Infrastructure of Iran-Linked CyberSpies http:// www. securityweek. com/ researchers-hack-iran-linked-spy-groups-infrastructure*. Accessed, 2016.

[3] ICS-CERT, "Indicators Associated With WannaCry Ransomware," 2017. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01I. [Accessed: 19-Jul-2017]

[4] B. Bill, "WannaCry: the ransomware worm that didn't arrive on a phishing hook," Sophos Ltd, 2017 [Online]. Available: https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/. [Accessed: 08-Jun-2017]

[5] ICS-CERT, “Petya Malware Variant,” 2017. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-181-01C. [Accessed: 19-Jul-2017]

[6] C. Cimpanu, “Petya Ransomware Outbreak Originated in Ukraine via Tainted Accounting Software,” *BleepingComputer*, 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/petya-ransomware-outbreak-originated-in-ukraine-via-tainted-accounting-software/. [Accessed: 06-Jul-2017]

[7] T. Fox-Brewster, “Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry,” *Forbes*, 2017. [Online]. Available: http://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/. [Accessed: 06-Jul-2017]

[8] K. Zetter, “Everything We Know About Ukraine’s Power Plant Hack | WIRED,” 20-Jan-2016. [Online]. Available: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/. [Accessed: 03-Feb-2017]

[9] ICS-CERT, “Cyber-Attack Against Ukrainian Critical Infrastructure,” 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. [Accessed: 03-Feb-2017]

[10] E-ISAC, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” Washington, USA, 2016 [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. [Accessed: 26-Jul-2017]

[11] J. Condliffe, “Ukraine’s Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks,” 22-Dec-2016. [Online]. Available: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/. [Accessed: 26-Jul-2017]

[12] P. Paganini, “Operation Dust Storm, Hackers Target Japanese Critical Infrastructure,” *Security Affairs*, 2016. [Online]. Available: http://securityaffairs.co/wordpress/44749/cyber-crime/operation-dust-storm.html. [Accessed: 19-Jul-2017]

[13] J. Gross and Cylance SPEAR Team, “Operation Dust Storm.” 2016 [Online]. Available: https://www.cylance.com/content/dam/cylance/pdfs/other/Op_Dust_Storm_Report.pdf

[14] European Union, *Council Directive 2008/114/EC on the Identification and Designation of European Critical infrastructures and the Assessment of the Need to Improve their Protection*, vol. L 345. 2008, pp. 75–82 [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[15] A. R. Berkeley III, M. Wallace, and C. COO, “A framework for establishing critical infrastructure resilience goals,” *Final Rep. Recomm. Counc. Natl. Infrastruct. Advis. Counc.*, 2010.

[16] U.S. Departmernt of Homeland Security, “NIPP 2013: Partnering for Critical Infrastructure Security and Resilience | Homeland Security,” 2013. [Online]. Available: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience. [Accessed: 22-Aug-2017]

[17] European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, vol. L194. 2016 [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=EN. [Accessed: 22-Aug-2017]

[18] J. Wachter, T. Grafenauer, and S. Rass, “Visual Risk Specification and Aggregation,” presented at the SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Special track CIP-NCT: Critical Infrastructure Protection - Novel Concepts and Technologies, Rome, 2017 [Online]. Available: www.thinkmind.org

[19] T. Schaberreiter, J. Röning, C. Wills, and G. Quirchmayr, “Addressing Complex Problem Situations in Critical Infrastructures using Soft Systems Analysis: The CS-AWARE Approach,” presented at the SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Special track CIP-NCT: Critical Infrastructure Protection - Novel Concepts and Technologies, Rome, 2017 [Online]. Available: www.thinkmind.org

[20] S. König and S. Rass, “Stochastic Dependencies Between Critical Infrastructures,” presented at the SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Special track CIP-NCT: Critical Infrastructure Protection - Novel Concepts and Technologies, Rome, 2017 [Online]. Available: www.thinkmind.org