ACIG
APPLIED CYBERSECURITY
& INTERNET GOVERNANCE

NASK

Cybersecurity is more than a Technological Matter – Towards Considering Critical Infrastructures as Socio-Technical Systems

Veronika Nowak University of Vienna, SBA Research, Austria, ORCID: 0000-0003-4229-4134

Johanna Ullrich University of Vienna, SBA Research, Austria, ORCID: 0000-0003-0297-9614

Edgar Weippl University of Vienna, SBA Research, Austria, ORCID: 0000-0003-0665-6126

Abstract

Cybersecurity is still considered a purely technological challenge; however, despite all technological progress, this challenge remains unsolved – as emphasized by many high-impact attacks against public administration and industry worldwide. We postulate that the mere focus on technology fogs the bigger picture, since people generate, operate, and interact with all technological systems, thus making them socio-technical systems. Hence, in this commentary we argue for a change of perspective towards a holistic, interdisciplinary view on our technological infrastructure. By example of the European power grid – inarguably a critical infrastructure not only for daily life but also for the continuity of our polity – we show that through interpretation as a socio-technical system, systematic and interdisciplinary studies would allow to reveal how its (cyber)security is not only a technological matter. An interdisciplinary approach combining STEM disciplines and Social Sciences would additionally advance the understanding of stakeholders and their goals and mindsets as well as the manifold dependencies between technology and human actors. While interdisciplinary endeavours appear to be generally supported by funding agencies, reviewers, universities, and researchers, they rarely occur in practice. We discuss why this is the case and present ideas on how to facilitate more interdisciplinary research.

Keywords

critical infrastructure; cybersecurity; European power grid; socio-technical systems

Received: 14.11.2022
Accepted: 29.11.2022
Published: 03.12.2022

Cite this article as:
V. Nowak, J. Ullrich, E. Weippl, "Cybersecurity is more than a Technological Matter Towards Considering Critical Infrastructures as Socio-Technical Systems," ACIG, vol. 1, no. 1, 2022.
DOI: 10.5604/01.3001.0016.2055

Corresponding author:
Veronika Nowak, University of Vienna, SBA Research, Austria;
ORCID: 0000-0003-4229-4134;
E-mail: veronika.nowak@univie.ac.at

1. Introduction

Traditionally, researchers and practitioners in technological fields take a highly focused point of view on the systems they are working on. However, due to the now ubiquitous digitalization, everything becomes increasingly linked; therefore, isolated perspectives on individual infrastructures are no longer feasible. For instance, cyber-physical systems, i.e., legacy systems combined with digital infrastructure, are now prone to cyberattacks which threaten their reliable operation. This is also the case for power grids, a major critical infrastructure crucial for daily life as we know it.

Due to the many dependencies, today's energy supply faces additional challenges beyond ensuring cybersecurity: (I) The increased use of renewable energy makes power grids more volatile. Yet, the deployment of renewables is indispensable in responding to and fighting climate change; the drought of 2022, reducing power generation in Austrian hydroelectric stations [1] and French nuclear stations [2] alike, gave an impression of what to expect in the future. (II) Commodity markets influence producer structures and prices as the current gas shortage [3] – caused by Russia's full-scale invasion of Ukraine in February 2022 – shows. (III) Power supply does not only follow economic but also geopolitical rationales (see the emergency synchronization of Ukraine with the European grid in March 2022 [4] as well as the ongoing plans of the Baltics to become "electrically independent" from Russia [5]). (IV) Even a non-digitized power grid infrastructure would not be cyber-secure as more and more consumer devices become "smart", potentially causing high load fluctuations [6].

The secure operation of the power grid in presence of external factors like cyberthreats, climate change, economics and geopolitics requires multi-faceted expertise; therefore, we need specialists of diverse disciplines to work together. We argue that we do not only have to view critical infrastructures (like the power grid) as cyber-physical systems, but as socio-technical systems – thus considering the technological as well as the human factor and their mutual dependencies. To illustrate our point, we introduce a case study in which minor misfunctions and miscommunications cascaded and brought the European power grid on the verge of a blackout which would have left roughly 400 million people without electricity.

2. Critical Infrastructures as Socio-Technical Systems

In November 2006, the newly built cruise ship *Norwegian Pearl* was transported via the river Ems from its shipyard to the North Sea. As on similar occasions before, a 380 kV power line crossing the river had to be disconnected. However, the disconnection was preponed on short notice; thereby, the responsible Transmission Grid Operator (TSO) failed to inform its neighbour TSOs whose lines had to serve as replacement. Consequently, a power line connecting the TSO with one of its neighbours suffered from high power flows. In response, the TSO decided to couple busbars of a nearby substation; unfortunately, this action did not have the desired effect, but further increased the line's power flow. Eventually, the line tripped automatically and started a cascade involving 32 tripped lines. This caused the European power grid to split into three unconnected islands. Two of them suffered from a lack of power generation because smaller generation units like wind turbines had automatically disconnected, which further complicated the situation. The third island experienced a surplus of generation because many smaller generation units had initially disconnected to facilitate stabilization and later automatically reconnected; moreover, the threat of further disintegration remained due to high power flows on certain lines [7]. The incident was eventually solved, but for 38 minutes 24 European countries stood at the abyss of a continent-wide blackout – "a national catastrophe" in which "after a few days [...] the population cannot be provided with necessary goods and services anymore" [8].

Two characteristics of our power grid infrastructure can be observed here: (I) initially minor incidents in everyday operations can easily multiply into cascading failures, and (II) for these failures, neither technology nor people are solely responsible. This brings to the fore yet another layer of our cyber-physical and, thus, interdisciplinary power grid systems: the human factor. We therefore propose a perspective which views our power grid as a socio-technical system. This means to go beyond the existing STEM interdisciplinarity and cooperate with the Social Sciences. For instance, Science and Technology Studies (STS) – a Social Sciences branch founded in the late 1970s/early 1980s – provides research into among others the evolvement of large technological systems [9] and how in such systems economic, technical, and social actors and -factors form a "seamless web" [10]. Regarding our contemporary, highly complex technologies, sociologist Charles Perrow pointed out that incidents are by no means unexpected, but "normal accidents" [11]. Failures are not due to human error alone, but also have their causes in the design and operation of such technologies. Organisational issues were also identified as causing one of the defining disasters in 20th century space flight: the explosion of the *Challenger* Space Shuttle in 1986 due to a malfunctioning technical component. Sociologist Diane Vaughan revealed in a detailed study that differences between and particularities of the company- and engineering cultures at NASA and the respective contractor led to the fatal launch decision [12]. Methods based on such a socio-technical perspective would be beneficial when analysing the everyday workings and (cyber)security requirements of critical infrastructure. Considering the power grid, an interdisciplinary approach jointly developed by STEM and STS researchers would study the grid infrastructure, the people who maintain and operate it, the policy makers who regulate everyday operation and incident response, and the consumers who depend on electricity.

In this light, the incident from November 2006 might be interpreted as a malfunction of a socio-technical system: The TSOs relied on divergent maximum values for electric current of the initially tripping line. This was despite the actual values having been previously exchanged in an official program and being mentioned in the coordination calls during the incident. For grid stabilization, interventions on the energy market are (according to German law) only allowed as an ultimate measure and were therefore considered too late. The dis/reconnection behaviour of small generation units was irrelevant until the policy-driven extension of renewables made them a significant part of generation and, thus, even able to hamper stabilization efforts.

This is just one example of how, e.g., engineering decisions not only concern technical issues, but have economic, geopolitical, and societal reasons and consequences. Thus, we need to shift our perspective and look at our critical infrastructure as socio-technical systems. To do this properly, we will have to combine expertise and methodologies from STEM disciplines and engineering with Social Sciences and Humanities (SSH).

3. Interdisciplinary research and its challenges

In general, the need for alternative perspectives and interdisciplinary approaches has been acknowledged. In Austria, this is also visible in the funding landscape: the KIRAS [13] funding scheme, managed by the Austrian Research Promotion Agency (FFG) and covering security research, requires a consortium partner from SSH. The Austrian Science Fund (FWF) recently opened the funding call *Emerging Fields* [14] which aims at researchers who are "prepared to depart from established approaches" and specifically invites interdisciplinary teams to apply. In 2020, the Vienna Science and Technology Fund (WWTF) awarded roughly € 3.6 million to interdisciplinary projects [15] working within the framework of Digital Humanism [16]. Being grant applicants ourselves, we, however, experienced some difficulties with interdisciplinary proposals. Especially longer-term projects with ambitious approaches combining Computer- and Social Sciences did not succeed. Although the reviewers generally welcomed these interdisciplinary ideas, we got the impression that they did not know how to assess them or found them too risky for funding. As far as we can gather from such experiences and conversations with colleagues from various disciplines, almost everybody wants interdisciplinary research, but has little to no idea on how to do it.

Even to receive funding for projects combining STEM disciplines can be challenging, as the example of our *NurZu!* project shows. Its general idea is to combine the *Energiemosaik* – a model based on national statistics to infer power consumption of Austrian communities developed by the University of Natural Resources and Life Sciences (BOKU) – with an open data-based power grid model to analyse the power grid's resilience regarding climate change, cyberattacks, and diverging consumption/generation behaviour. The idea was well-received by the required industry partners: small stakeholders in the energy sector saw potential to accelerate the power grid's transition towards renewables; however, the project was not accepted upon first submission. Reviews considered the approach to be "standard"; in fact, we combine standard procedures which creates novel, interdisciplinary challenges. We explained this in more detail for the resubmission and eventually got funded. To what extent this acceptance might be due to Russia's invasion of Ukraine – emphasizing the need for changes in the energy sector – would be a question for a socio-technical study.

Our experience from 15+ years working on information security in science and practice has shown that purely technical solutions to security issues often do not (fully) work as intended. Digitalization, almost always marketed as the cure to technological and often also societal problems, has turned out to be a curse as well. Functionality, a fundamental tenet of engineering, is usually put before security. While this is already troubling in the context of web applications and business software, it becomes a huge societal issue with regards to critical infrastructures. We therefore postulate that a broader perspective will be crucial to better understand those socio-technical systems, securely operate them, and meet future challenges. Still, apart from the lack of adequate funding schemes, there are issues regarding interdisciplinarity:

1. Concepts, terminology, and methods: even between STEM disciplines, the differences can be huge; just finding a joint vocabulary usually requires considerable efforts.
2. Discipline-specific customs regarding publications: e.g., importance of conference papers in Computer Science vs publishing journal papers and books in Social Sciences and Humanities (SSH).
3. Career stage of the involved researchers: while early-stage researchers might have flexibility and be interested in an interdisciplinary path, mid-term researchers could be hindered in their career since they depend on publishing in specific venues.
4. Review system: apart from reviewers usually being specialised in one discipline, it has to be noted that the review system is overcapacity as it is.

A major consequence of these challenges is that interdisciplinary projects often happen in a "subordination/service mode" [17]; i.e., one of the disciplines is only playing a supporting role. The main question is how we create an academic environment conducive to equitable interdisciplinary research.

4. Conclusion

Although steps are taken towards interdisciplinary research, progress is slow and funding schemes bringing together STEM fields and Social Sciences are scarce. There is a lot of ideological support for such project ideas which does not translate into actual funding. This leaves very promising research potentials untapped, since there are SSH disciplines like Technology Assessment and STS which explicitly study technology, thus providing a link to STEM fields. Since large critical infrastructures like power grids should be considered socio-technical systems – i.e., technical and human factors playing equally important roles – joint work of STEM- and SSH researchers should be systematically promoted and funded.

To overcome the challenges of different terminologies, publication customs, and career requirements – thus arriving at the "integrative-synthesis mode" [17] of interdisciplinary research in which the understandings of different disciplines truly work together – some major systemic changes are necessary:

1. Funding should be available to give interdisciplinary teams enough time to find a joint vocabulary and understand each other's methods.
2. Coordination between reviewers of different disciplines should be facilitated for interdisciplinary proposals; alternative review structures such as juries may be feasible.
3. Established conferences and journals should be more open for interdisciplinary work to promote rather than hinder an interdisciplinary researcher's career.

We are aware that the current academic environment is not amenable to such drastic changes, especially not in the short run. Still, at this point the need for holistic perspectives on contemporary socio-technical issues is more than obvious. Since being well-versed in multiple disciplines like Gottfried Wilhelm Leibniz or Marie Skłodowska-Curie is virtually impossible in today's academia, we need the specialists to team up, and we need a funding- as well as publication environment which facilitates and rewards such efforts.

REFERENCES

[1] Austrian Power Grid (APG). (2022, Aug. 25). *Trockenheit reduziert Stromproduktion aus Wasserkraft um 31 Prozent*. [Online]. Available: https://www.apg.at/news-presse/austrian-power-grid-apg-trockenheit-reduziert-stromproduktion-aus-wasserkraft-um-31-prozent/. [Accessed: Oct. 27, 2022].

[2] S. Sijelmassi. (2022, Sep. 8). *Face au réchauffement climatique, l'avenir de l'énergie nucléaire est-il menacé?*, TV5 Monde. [Online]. Available: https://information.tv5monde.com/info/face-au-rechauffement-climatique-l-avenir-de-l-energie-nucleaire-est-il-menace-466906. [Accessed: Oct. 27, 2022].

[3] BBC. (2022, Sep. 29). *Nord Stream 1: How Russia is cutting gas supplies to Europe*. [Online]. Available: https://www.bbc.com/news/world-europe-60131520. [Accessed: Oct. 27, 2022].

[4] European Network of Transmission System Operators for Electricity (ENTSO-E). (2022, Mar. 16). *Continental Europe successful synchronisation with Ukraine and Moldova power systems*. [Online]. Available: https://www.entsoe.eu/news/2022/03/16/continental-europe-successful-synchronisation-with-ukraine-and-moldova-power-systems/. [Accessed: Oct. 27, 2022].

[5] European Climate Infrastructure and Environment Executive Agency. (2021, June 18). *Baltic Synchronisation Project: Works are on track*. [Online]. Available: https://cinea.ec.europa.eu/news-events/news/baltic-synchronisation-project-works-are-track-2021-06-18_en. [Accessed: Oct. 27, 2022].

[6] A. Dabrowski, J. Ullrich, E. R. Weippl, "Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well," in Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, Florida, USA, 2017, pp. 303–314, doi: 10.1145/3134600.3134639.

[7] UCTE. (2007). *Final Report - System Disturbance on 4 November 2006, Union for the Co-ordination of Transmission of Electricity*. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/otherreports/Final-Report-20070130.pdf. [Accessed: Oct. 27, 2022].

[8] T. Petermann, H. Bradke, A. Lüllmann, M. Poetzsch, U. Riehm, Eds., *Was bei einem Blackout geschieht: Folgen eines langandauernden und großflächigen Stromausfalls*. Berlin: Edition sigma, 2013.

[9] T. Hughes, "The evolution of large technological systems," in *The Social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, Mass: MIT Press, 1987, pp. 51–82.

[10] T. P. Hughes, "The seamless web: Technology, science, etcetera, etcetera," *Social Studies of Science*, vol. 16, no. 2, pp. 281–292, 1986, doi: 10.1177/0306312786016002004.

[11] C. Perrow, *Normal accidents: Living with high risk technologies*. Princeton: Princeton University Press, 2011.

[12] D. Vaughan, *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago: University of Chicago Press, 2007.

[13] KIRAS Sicherheitsforschung, *Sicherheitsklammer*. [Online]. Available: https://www.kiras.at/. [Accessed: Oct. 27, 2022].

[14] FWF Programmes, *Emerging Fields*. [Online]. Available: https://www.fwf.ac.at/en/research-funding/fwf-programmes/emerging-fields. [Accessed: Oct. 27, 2022].

[15] WWTF, *Digital Humanism 2020*. [Online]. Available: https://www.wwtf.at/funding/programmes/ict/index.php?lang=EN#ICT20. [Accessed: Oct. 27, 2022].

[16] Dighum, *Vienna Manifesto on Digital Humanism*. [Online]. Available: https://dighum.ec.tuwien.ac.at/dighum-manifesto/. [Accessed: Oct. 27, 2022].

[17] A. Barry, G. Born, Eds., *Interdisciplinarity: Reconfigurations of the social and natural sciences*. London, New York: Routledge, 2013.