MAKING SENSE OF THE MANY UNDERSTANDINGS OF CYBER RESILIENCE

Stine Skaufel Kilskar, Matthieu Branlat, Tor Olav Grøtan, Jannicke Fiskvik
SINTEF Digital[1]
[stine.s.kilskar ; matthieu.branlat ; tor.o.grotan ; jannicke.fiskvik] @sintef.no

Abstract

This paper reports on a survey of scientific literature which aim has been to describe how the concept of *cyber resilience* is used in the literature. It discusses the method of systematic mapping study, presents the results from the conducted study, provides the first insights from the findings, and outlines the future work based on the results. Literature was obtained through searches in Scopus and mapped according to the following dimensions: 1) domain of application, 2) focus, 3) scope of cyber resilience, and 4) main contribution to cyber resilience. The study shows a distinct rise in research on cyber resilience. The results demonstrate that existing literature is predominantly generic rather than domain-specific and that focus is mainly on cyber security. It also shows an overwhelmingly technical concern, highlighting the need to develop approaches including other components of the management of critical infrastructures, such as organizational processes and human decision-making. Finally, only a small fraction of this literature contributes to the discussion of the nature of cyber resilience, whereas most of the contribution is related to ways of analysing cyber resilience. The survey is part of the project Theoretical Advances on Cyber Resilience (TECNOCRACI), and the motivation is to establish an initial overview of the landscape of scientific publications on the field. According to the abductive research approach the project is founded on, the findings will be compared with the project's pre-understanding of cyber resilience. The observed differences as well as the vacancies in the literature will be used to carefully devise direction for more in-depth literature studies and empirical case studies that will be the foundation for further theory building on cyber resilience on three areas; energy supply, water supply and offshore oil and gas industry.

Keywords: cyber resilience, mapping study, cyber security, critical infrastructure

Introduction: Digitalization and the need for a theoretical grasp of cyber resilience

This paper is written as a part of the research project *Theoretical Advances of Cyber Resilience – Practice, Governance and Culture of Digitalization (TECNOCRACI)*.

Digitalization is a transformation process involving the introduction of information technology (IT) in already existing technological systems. In critical infrastructures such as power or water management installations, industrial control systems are key elements of existing technology commonly labelled 'Operational Technologies' (OT). Digital technologies provide unprecedented capabilities for supporting more distributed and efficient operations in many ways. However, the development of and increased reliance on digital capabilities have also exposed these systems to new, sometimes increased, risks. For instance, technical malfunctions might perturb the proper delivery of valuable services at larger scales due to increased connections between previously separated parts of the systems. In addition, these industrial and critical infrastructure systems are increasingly exposed to hostile activities and attacks due to external connections (i.e. Internet) mercilessly demonstrating a

[1] Strindvegen 4, 7034 Trondheim, Norway

security gap that is very difficult to close, and even increasing in the near future. Larger and more complex systems also mean that anticipating all possible failures is even less feasible than it used to be. Adding to the burden, stakeholders acknowledge that the solution is not purely technological, but also a matter of organizational capability to deal with this complexity.

In the face of these risks and of the need to adopt a more systemic perspective on critical infrastructures, more and more practitioners and researchers have turned to alternatives to traditional risk- or vulnerability-based approaches. To these researchers and practitioners, it is critical that, in addition to experiencing limited numbers of disruptions, systems such as critical infrastructures have the capacity to maintain some level of operationality even when disruptions do occur: unanticipated, sometimes surprising, adverse events are seen as unavoidable and need to be managed in ways that avoid larger disruptions or even catastrophes. The notion of *resilience* has shown increased popularity in the past decade, also in scientific literature. It appears to capture the fundamental issues and objectives described above, but this corpus of scientific literature originates from many and diverse contexts. Increased popularity has also generated a wide diversity in how the notion is used (what it means, why it is necessary) and in what types of solutions or approaches it refers to – and a potentially confusing landscape of understandings.

The aim of TECNOCRACI is to investigate how the key ideas of resilience (engineering) can be conveyed to the digital arena and articulated as theoretical positions with practical relevance, mainly for critical infrastructures. A central line in this way of thinking is how to deal with surprise and complexity through leveraging an adaptive, sociotechnical capacity in an organizational context typical for critical infrastructures. Thus, the point of departure for TECNOCRACI is that the notion of *cyber resilience* conveys a potential for substantially larger scope than just slightly enhancing, or relabelling, existing cyber security practices, or "cyber hygiene". *Relabelling* is identified as a trap that emerges from the massive attention towards resilience. There is a real temptation that such a "demand side" is served by a "supply side" that to a large extent merely relabels existing (good) practices, in good faith. In contrast, TECNOCRACI aims for a theoretical encircling of cyber resilience as an emergent property of an organization, driven by human initiative, rather than as an instrumental result of technical or organizational measures.

At the same time, TECNOCRACI also acknowledge – as an implication of understanding resilience as an emergent property – that important keys to understanding cyber resilience also may reside in current sociotechnical practices, although they may not be appreciated as part of the formal organizational repertoire, nor acknowledged as resilient practice. Hence, TECNOCRACI employs a strategy of being particularly sensitive to sociotechnical, situated practice, distinguishing between "work as done" and "work as imagined". Moreover, as the principles of resilience may also work as an invitation to fallible practices, performativity, management, and governance issues are also at central stage. Finally, as IT and OT already represent different cultural approaches and presumptions around similar technical building blocks, and the telecom actors are arriving on the scene with 5G and IoT, technologies that challenge existing architectures, also "technocultural" aspects are part of the overall organizational research interest.

The TECNOCRACI project's objective is thus to develop a comprehensive theory of cyber resilience, aiming for relevance for current and future challenges of digitalized critical infrastructures, grounded on insight from situated practice both at the operational and managerial level, and moving beyond the confines of a classical technocratic approach.

This paper is part of initial efforts which aim to provide a preliminary clarification of key terms and concepts related to the field of study based on a systematic search in relevant academic literature; the results reported in this paper being a first step.

The research issue is to clarify if there is a similar rise in research on cyber resilience as is observed on resilience in general, and how this literature frames the concept of cyber resilience. The methodology chosen for investigating this is a mapping study, as described in the next chapter.

Research Methodology: Systematic mapping study

This paper reports on a survey of scientific literature which aim has been to describe how the concept of *cyber resilience* is used in the literature. The survey has been organized as a systematic mapping study (SMS). According to Kitchenhand and Charters (2007), systematic mapping studies "are designed to provide a wide overview of a research area, to establish if research evidence exists on a topic and provide an indication of the quantity of the evidence" (p. 44). They differ from systematic literature reviews, which focus on gathering and synthesizing evidence. The main difference lies in terms of goals and approaches to data analysis (Petersen et al., 2015). Mapping studies are mostly concerned with structuring a research area. The aim is to identify and categorize the available research on a given topic. As such, mapping studies are a useful point of departure to get a broad overview of a research field, but also to identify gaps and areas for future research.

First step: Search for potentially relevant papers

Literature was obtained through Boolean searches in the interdisciplinary database Scopus. With 'cyber resilience' being the single concept of interest, the study is based on publications covering this term in either its title, abstract or keywords; that is, literature resulting from the following search string:

TITLE-ABS-KEY ("cyber resilien" OR cyberresilien*)*

The asterisk, representing any number of characters, was included so that the search not only returns resilience, but also resiliency, resilient, etc. The search returned 282 search results.

Second step: Sorting of papers

This step aimed primarily at excluding papers that should not or could not be included in the following analyses. Exclusion criteria were defined:

- Formal exclusion criteria: missing content (esp. absence of abstract); not individual papers (e.g., collection of proceedings); non-English language (only one in our results)
- Relevance-based exclusion criteria: papers that appeared to only cite “cyber resilience”, but be focused on another topic (e.g., a paper really about blockchain, which only mentions cyber resilience as an interesting outcome of using this technology)

As mentioned before, the purpose of a mapping study is to analyse and describe broadly the literature about a concept of interest, to show the landscape of research interested in this concept. The exclusion criteria above aimed at selecting for further analysis the papers that contribute to such landscape. Such papers discuss components of or approaches to cyber resilience, sometimes define the concept and describe its nature. We therefore included papers that belong to domains other than our own domains of research because they contribute to such landscape (e.g., technical papers focused on very specific components of cyber resilience).

While formal exclusion criteria are non-controversial, the use of relevance-based criteria can be more problematic due to the reliance on reviewers’ judgment. This task is further complicated by the fact that the review process is only based on partial information (essentially titles, abstracts and keywords). To limit the impact of subjective judgement, all 282 items were reviewed at least twice independently. Papers judged twice similarly were included or excluded accordingly. When judgments differed, they were individually reassessed and potentially discussed by the reviewers.

At the end of this sorting process, 147 publications were excluded due to the reasons outlines above; thus, 135 of the 282 search results were included for further research, i.e. the mapping study.

Third step: Mapping of papers

The literature obtained was then mapped according to the following dimensions of interest:

- domain of application, i.e. which domains of activity, if any, were primarily targeted
- focus, i.e. which research topic or field was providing the contribution
- scope of cyber resilience, i.e. which system of interest or scope was considered to analyse or improve cyber resilience
- main contribution to cyber resilience, i.e. which type of contribution to cyber resilience was made

Within each dimension, categories were identified, in part based on prior knowledge, but to a large degree based on the topics emerging from the literature analysed. Such iterative process implies that the categorization process required reviewers to reconsider papers to a significant degree when new categories were proposed or clarified.

The mapping was based the information gained from the title, abstract, author keywords, and indexed keywords only. As with the sorting step above, the mapping of papers is a judgment-based process, complicated by the limitations of available information. Again, the use of multiple reviewers (3) and a similar consensus-seeking process was the approach implemented to limit the impact of judgments.

Results from the mapping

The mapping study included 135 publications, including 84 conference papers, 38 journal articles, 10 book chapters, and 3 review articles. Figure 1 illustrates this distribution in terms of percentages.

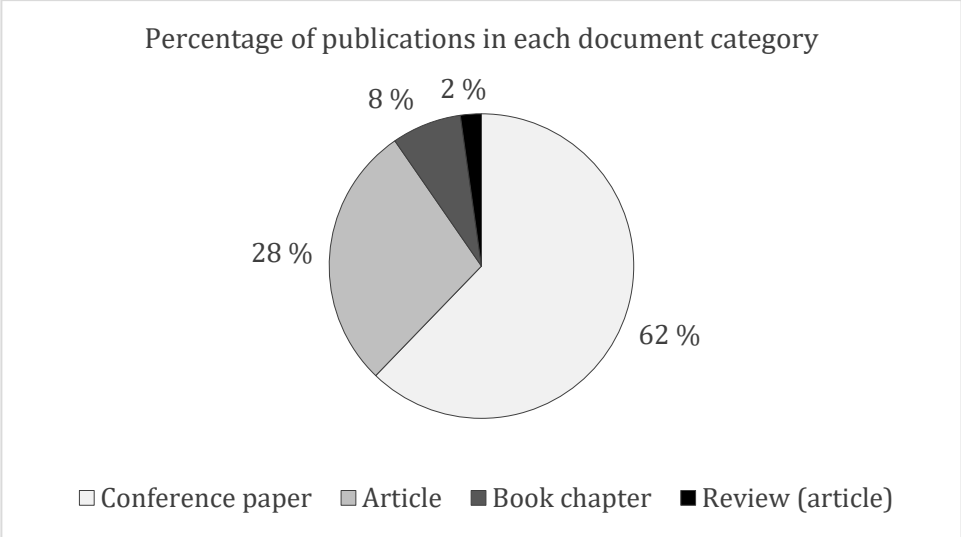

Figure 1: Distribution of publications with respect document type

Figure 2 illustrates the distribution of the publications with respect to year of publication. This shows a distinct increase approximately three years ago, implying a is a similar rise in research on cyber resilience as is observed on resilience in general.

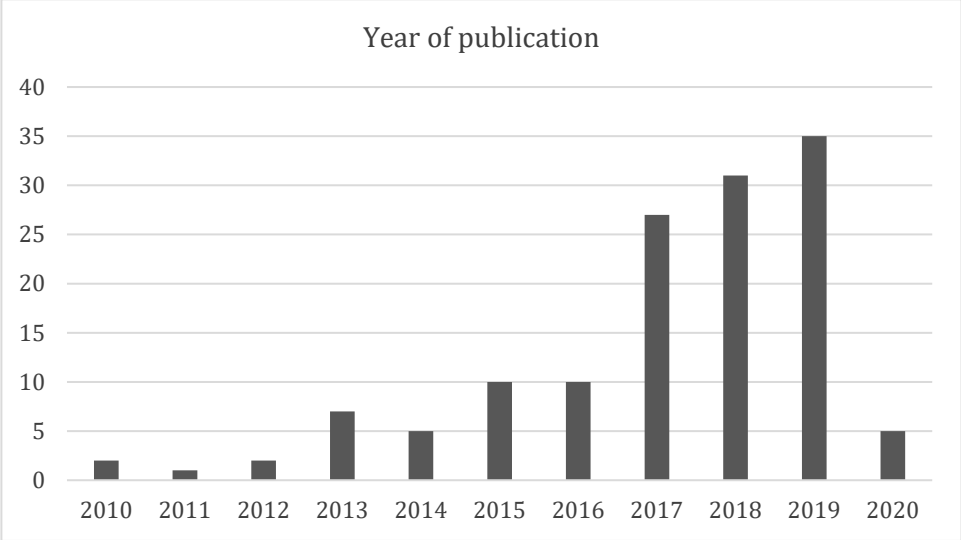

Figure 2: Distribution of publications with respect to year of publication

In the following subchapters, results are presented for each of the dimensions of the mapping study, respectively, i.e. domain of application, focus, scope of cyber resilience, and main contribution to cyber resilience. Tables are included to show the distribution according to the categories within each dimension. Also, references to examples of publications are provided to illustrate the diversity in the literature and for highlighting some areas that are of particular interest for the TECNOCRACI project.

Domain of application

The distribution of the publications with respect to which domains of activity, if any, that were primarily targeted is listed in Table 1.

Table 1: Distribution according to domain

Domain of application	*No.*	*%*
Generic	64	47 %
Critical infrastructure	16	12 %
Energy	16	12 %
Military	13	10 %
Industry	11	8 %
Healthcare	5	4 %
Transportation	4	3 %
Finance	3	2 %
Space	3	2 %
Other	0	0 %

Nearly half of the included literature (i.e. 47 percent) is mapped as being generic; hence, most of the literature on cyber resilience is not domain dependent. However, as TECNOCRACI focuses on critical infrastructure, it is interesting noticing that 16 of the publications explicitly address cyber resilience in the context of critical infrastructure (protection). Some of these are mentioned in the following sub-chapters. Including the papers which domain of application is either energy, healthcare, transportation, or finance, a total of 44 publications address the protection of critical infrastructure in some way.

Focus

Table 2 shows the distribution of the publications with respect to research topic or field in focus.

Table 2: Distribution according to focus

Focus	*No.*	*%*
Cyber security	79	59 %
Cyber-physical systems	15	11 %
Strategy/policy	10	7 %
Management processes	6	4 %
Software defined networking	5	4 %
IoT/Edge computing	4	3 %
Block chain	3	2 %
Cloud computing	3	2 %
Culture	3	2 %
Other	7	5 %

A majority (i.e. 59 percent) of the mapped literature discusses cyber resilience in a context of cyber security, and a substantial part (11 percent) is related to cyber-physical systems. Examples of papers focusing on cyber security include a paper addressing the fundamentals for a definition of cyber resilience, contrasting cyber resilience against cybersecurity (Björk et al, 2015); a study that measures individual resilience to cyberterrorist attacks on financial systems and explores the antecedents of resilience (Hua et al, 2018); and the description of a framework for developing and delivering a multilateral educational and training scheme based on a proactive approach to cybersecurity (Rajamaki et al, 2018).

Only 19 publications have a focus that is either on strategy/policy, management processes or culture. With his article, Stoddart (2016) intends to aid the UK government in protecting the UK from cyber-attacks on critical national infrastructure. He further argues that complete engagement and partnership with private sector owner-operators of critical national infrastructure are vital to the success of the government's National Cyber Security Strategy. One example of an article focusing on management processes is Kikuchi and Okubo (2020), in which the authors identifies critical factors of polycentric governance and propose how these factors should be applied to build resilience of cyberspace. Three publications address cyber resilience with a focus on culture, one of them proposing a conceptual model for promoting positive security behaviour in Internet of Things era (Kautsarina and Anggorojati, 2018).

Finally, it is worth mentioning that this dimension initially included the category "standards"; however, none of the included publications fit this category.

Scope of cyber-resilience

The third dimension concerns the system of interest or scope that is considered to address cyber resilience. The distribution of publications according to this dimension is listed in Table 3.

Table 3: Distribution according to scope of cyber resilience

Cyber resilience scope	*No.*	*%*
Technical	47	35 %
Holistic	31	23 %
Organizational	18	13 %
National	13	10 %
System architecture	11	8 %
Human/individual	6	4 %
Industry	2	1 %
Other	7	5 %

More than one third of the publications mainly consider technical aspects, whereas approximately a quarter take on a holistic scope in addressing cyber resilience. Publications in the first category often have a narrow scope. One example is a paper by Mylrea and Gourisetti (2017), in which the authors explore the application of blockchain and smart contracts to improve smart grid cyber resiliency and secure transactive energy applications. Another example is an article that presents a software-defined networking-based communication network architecture for microgrid operations and claims to demonstrate that it can significantly enhance the resilience and security of microgrid operations against the realization of various cyber threats (Jin et al, 2017).

Examples of publications with a more holistic scope of cyber resilience include an article on the future of cyber resilience in an age of global complexity (Herrington and Aldrich, 2013); a book chapter that describes a hybrid infrastructure resilience assessment approach combining qualitative analysis techniques with performance-based metrics (Vugrin and Turgeon, 2014); and a paper on building cyber resilience through a discursive approach to what the author refers to as "big cyber" threat landscapes (Grøtan, 2018).

A smaller fraction of the publications (i.e. 18 percent) address cyber resilience from an organizational or human/individual perspective. Mailloux and Grimaila (2018) are among the authors that employ a more explicit emphasis on organizational aspects of cyber resilience. In their article, they argue that as the world becomes more dependent on connected cyber-physical systems, the cybersecurity workforce must adapt to meet these growing needs. Another article is based on observations that the authors conducted in a full-scale adversarial cyber security training for critical infrastructure (Aoyama et al, 2015a). Based on the observations, the authors found some tendencies in the defensive team's negative social behaviours and the management issues that lead to malfunction of the team, and they present these as possible challenges in real-world cyber incident management. A human-factor based study by Aoyama et al (2015b) discussed the methodology to achieve high resiliency of the organization by better management. Other examples of organization- or human-oriented publications include Björk et al (2015), Hua et al (2018), Rajamaki et al (2018), and Kikuchi and Okubo (2020) that were all briefly mentioned in the previous subchapter.

Main contribution to cyber resilience

Table 4 shows the distribution of publications with respect to which type of contribution to cyber resilience was made.

Table 4: Distribution according to main contribution to cyber resilience

Contribution to cyber resilience	*No.*	*%*
Analysis	72	53 %
Solution	44	33 %
Nature	9	7 %
Training	2	1 %
Other	8	6 %

Approximately half of the mapped literature proposes ways of assessing, measuring, or in other ways analysing cyber-resilience. Examples of such publications have been mentioned in the previous two subchapters, including Stoddart (2016), Hua et al (2018), Mailloux and Grimaila (2018), Aoyama et al (2015a), Aoyama et al (2015b), and Kikuchi and Okubo (2020).

One third of the remaining publications present solutions for achieving or increasing cyber-resilience. One of these are Jin et al (2017), which was mentioned in the previous subchapter. Another is Tran et al (2016), presenting the implementation of an epidemiological model to combat a zero-day outbreak within a closed network. These are both quite narrow in their contributions. Others presents general resilience requirements, a resilience management process, resilience levels, and an overview of methods to different resilience management steps for each resilience level (Häring et al, 2017).

Only 9 publications provide discussions of the nature of cyber-resilience as their main contribution. Already mentioned is the paper by Björk et al (2015) that provides fundamentals for definition of cyber resilience. Authors providing a more recent publication included in this category are Conklin and Kohnke (2018), who present the justification and underlying principles for implementing cyber resilience as well as a standard process for designing and deploying a cyber resilient architecture. Stafford and Bouwens (2018) argues that resilience involves cognitive, behavioural, and contextual features, and use these features to highlight design considerations across the constituent systems of the cyber ecosystem landscape using complex system methods.

A comparison of the mapping done within the two last dimensions, i.e. scope of cyber resilience and main contribution to cyber resilience was carried out. This revealed a couple interesting, but perhaps not surprising, findings. Firstly, more than 60 percent of the publications with solution as main contribution have a technical scope (as opposed to 35 percent when counting all included literature). Secondly, none of the papers addressing the nature of cyber resilience are technical.

Discussion and implications for further research

The main results from the current mapping study related to the TECNOCRACI-derived objective can be summarized as follows: 1) Most of the literature on cyber-resilience is generic in terms of domain of application. 2) The majority discusses cyber resilience with a focus on cyber security. 3) There is an overwhelmingly technical concern, highlighting the need to develop approaches including other components of the management of critical infrastructures, such as organizational processes and human decision-making. 4) In terms of contribution to cyber resilience, most provide ways of assessing, measuring, or in other ways analysing cyber-resilience and few discuss the nature of cyber resilience.

Concerning the focus (Table 2), it should be noticed that the three dominant categories represent a wide diversity. The term cyber resilience may be used (e.g., WEF, 2012) to raise a business-level awareness of systemics risk that also stem from the cyber domain, to which businesses, organizations and societies need to prepare for disturbances from the cyber domain, in a broad manner. It is likely that such understanding may be reflected in the category strategy/policy. The dominant case (cyber security) is however that resilience principles are applied in a narrower sense for strengthening or enhancing cyber security per se, e.g. of critical infrastructures, to deal with new, complex, and systemic threats. The cyber-physical category may be seen as overlapping, referring to cyber security in cases where insufficient cyber security may have physical consequences, e.g. in industrial control systems. For the latter, the NIST Special Publication on "Developing Cyber Resilient Systems" points at "cyber resiliency engineering" as "an emerging *speciality systems engineering* discipline" (Ross et al, 2019). The implication for TECNOCRACI is that there may be theoretical substance to build on across a wide range of foci, but it may be necessary to make distinctions related to the context of cyber resilience, and the intended audience for the theoretical advances.

The results from this mapping study will be used to identify priorities for design of empirical case studies for advancing on building a theory on cyber resilience. The empirical studies will be within energy supply, water supply and offshore oil and gas exploration/production. The actual priorities for case design will reflect the contrasts between the preunderstanding sketched out in the Introduction, and the findings in this mapping study.

The following findings are of special interest for our further research process:

- the existing literature is predominantly generic rather than domain-specific
- the perspective is primarily about technical and holistic aspects, while a substantially smaller fraction is explicitly on organizational and human aspects

It is not surprising that the main bulk of the literature is generic and technology centric. The high occurrence of "holistic" orientation also signifies that many authors recognize that there is a need for going beyond the technical. However, a holistic approach is informative and valuable but hardly a guidance for action, and the literature hardly address organizational and human aspects explicitly. TECNOCRACI therefore needs to advance on how an adaptive capacity in face of surprise and complexity, driven by human initiative in specific organizational contexts, may be framed theoretically. Moreover, this must be done in a manner that avoids a rather common weakness of resilience concepts, namely that they are formulated so generically or holistically that they lose sensitivity to context.

Also, the predominant focus in the literature on cyber security and orientation towards analysis and solutions, confirms the presumption that cyber security is the most intuitive area for application of cyber resilience. This is not surprising, as the field of cyber security is constantly lagging behind in relation to a persistent flow of new and unprecedented vulnerabilities, threats and attacks. The situation is so grave that strong voices argue for hesitance in the introduction of newer technologies into, e.g., the energy grids (Bochman, 2018). There is therefore an instant demand for novel solutions and measures, and this prepares the ground for a resilience orientation in addition to best practices derived from past experiences.

For TECNOCRACI however, it is paramount that the theoretical advances also are sensitive to purpose, beyond the immediate and intuitive coupling to cyber security. It must be assumed that no critical infrastructure operator will seek to be "resilient" in a purely generic manner. While enhanced

cyber security appears as a "natural" purpose of resilience due to the shortcomings of traditional cyber security approaches, the interest of a critical infrastructure operator may be both wider and narrower. One example of the latter is securing the integrity of networked Safety Instrumented Systems (SIS), which are traditionally built and operated as OT, but remotely accessed through IT. This may be framed as "SecureSafety", in which the potential for resilience approaches are apparent (Grøtan et al, 2020). At other end, an example of the former is to maintain a similar narrow purpose in a broader context of a digital transformation process that is conceived as a constant mix of old and new technologies, and a more profound integration of IT and OT, for which security of energy supply must be ensured throughout (Antonsen et al, 2020).

The prevalence of cyber security, analysis and solutions in the existing literature is thus a strong reminder for the forthcoming theoretical advances to be sensitive to context, both for conditions of implementation of, and for purpose of being resilient in terms of a managed adaptive capability driven by human initiative and organizational accountability.

A deeper look into one of the papers categorized as "organizational" in this mapping study (based on the abstract) indicates the profoundness of the challenge ahead. Here (Björck et al, 2014), terms and concepts from organizational science are strikingly absent. Instead, apparently from a computer and system sciences perspective, the argument is made that while the scope of cyber security should be "atomistic", that is, related to one organization and "applied from the outside", the scope of cyber resilience should be "holistic", related to a network of organizations, and "built-in". While the validity of the first part of the argument is disputable, the latter part is interesting in the sense that the paper also claims that the objective of cyber resilience is to ensure business delivery rather than protect the IT systems per se. Hence, what appeared to be a contribution with an organizational scope to cyber security, actually is about cyber resilience as advocated by WEF (2012).

For further work in TECNOCRACI, this is a reminder of the urgency to contextualize resilience both in terms of purpose/objective and operational conditions for maintaining an adaptive capacity, founded on organizational science, and to pay attention to the polycentric nature of resilience.

Acknowledgment

This paper is written as a part of the project *Theoretical Advances of Cyber Resilience – Practice, Governance and Culture of Digitalization (TECNOCRACI)*, which is founded by The Research Council of Norway, grant nr 303489.

References

Antonsen, S., Grøtan, T.O., Gjerde, O., and M. Istad. (2020). Security of electricity supply in the transition toward smarter grids. Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. Research Publishing, Singapore.

Aoyama T., Naruoka H., Koshijima I., and Watanabe K. (2015a). How Management Goes Wrong? – The Human Factor Lessons Learned from a Cyber Incident Handling Exercise. Procedia Manufacturing, Vol.3, pp. 1082-1087.

Aoyama T., Naruoka H., Koshijima I., Machii W., and Seki K. (2015b). Studying resilient cyber incident management from large-scale cyber security training. 10th Asian Control Conference (ASCC), Kota Kinabalu, 2015, pp. 1-4.

Björck F., Henkel M., Stirna J., and Zdravkovic J. (2015). Cyber Resilience – Fundamentals for a Definition. In: A. Rocha, A. Correia, S. Costanzo, & L. Reis (eds.) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, Vol 353, pp. 311-316. Springer, Cham.

Bochman, A. (2018). The End of Cybersecurity. Harvard Business Review. The Big Idea. May 2018.

Conklin W.A. and Kohnke A. (2018). Cyber resilience: An essential new paradigm for ensuring national survival. In Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018, National Defence University, Washington D.C., USA.

Grøtan, T. O. (2018). Building cyber resilience through a discursive approach to “big cyber” threat landscapes. In: Haugen, S et al (eds.) Safety and Reliability – Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway, pp. 3115-3126.

Grøtan, T.O., Petersen, S., Myklebust, T and G.K. Hanssen. (2020). SecureSafety; state-of-the-art and remaining challenges. Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. Research Publishing, Singapore.

Häring I., Sansavini G., Bellini E., Martyn N., Kovalenko T., Kitsak M., Vogelbacher G., Ross K., Bergerhausen U., Barker K., and Linkov I. Towards a generic resilience management, quantification and development process: General definitions, requirements, methods, techniques and measures, and case studies. In: I. Linkov & J. Palma-Oliveira (eds.) Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht.

Herrington L. and Aldrich R. (2013). The future of cyber-resilience in an age of global complexity. Politics, Vol. 33, No. 4, pp. 299-310.

Hua, J., Chen, Y., Luo, X. (2018). Are we ready for cyberterrorist attacks? – Examining the role of individual resilience. Information & Management, Volume 55, No. 7, pp. 928-938.

Jin D., Li Z., Hannon C., Chen C., Wang J., Shahidehpour M., and Lee C.W. (2017). Toward a Cyber Resilient and Secure Microgrid Using Software-Defined Networking. IEEE Transactions on Smart Grid, Vol. 8, No. 5, pp. 2494-2504.

Kikuchi M. and Okubo T. (2020). Building cyber resilience through polycentric governance. Journal of Communications Vol. 15, No. 5, pp. 390-397.

Kitchenham. B. and Charters, S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering. Tech. rep., Technical report, EBSE Technical Report EBSE-2007-01, 2007.

Mailloux, L. O. and Grimaila, M. (2018). Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce. IT Professional, Vol. 20, No. 3, pp. 23-30.

Mylrea, M. and Gourisetti, S. N. G. (2017). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. 2017 Resilience Week (RWS), Wilmington, DE, 2017, pp. 18-23.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2019). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Volume 2. Derived from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

Stafford R.B. and Bouwens C.L. (2018). Designing systems for cyber resilience. In E-H. Ng, B. Nepal, E. Schott, & H. Keathley (eds.) Proceedings of the American Society for Engineering Management 2018 International Annual Conference.

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. International Affairs, Vol. 92, No. 5, pp. 1079-1105.

Petersen, K., Vakkalanka, S., and Kuznairzm L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, Vol. 64, pp.1-18.

Rajamaki J., Nevmerzhitskaya J., and Virag C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). 2018 IEEE Global Engineering Education Conference (EDUCON), Tenerife, 2018, pp. 2042-2046.

Vugrin E.D. and Turgeon J. (2014). Advancing cyber resilience analysis with performance-based metrics from infrastructure assessments. In: Management Association, I. (eds.). Cyber Behavior: Concepts, Methodologies, Tools, and Applications, Vol. 4-4, IGI Global, pp. 2033-2055.

World Economic Forum (WEF). (2012) Partnering for cyber resilience. Derived from: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf