SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Introduction to the Special Issue: Critical infrastructure protection—the challenge of resilience

Aleksandra Gasztold[1], Gordan Akrap[2]

[1]a.gasztold@uw.edu.pl

[1]https://orcid.org/0000-0002-9114-1604

[1]Faculty of Political Science and International Studies, University of Warsaw, Poland

[2]https://orcid.org/0000-0003-2666-596X

[2]Hybrid Warfare Research Institute, Teslina 9, 10000 Zagreb, Croatia
University North, Trg Žarka Dolinara 1, 48000 Koprivnica, Croatia

Citation: Gasztold, A. and Akrap, G. (2022) 'Introduction to the Special Issue: Critical infrastructure protection—the challenge of resilience', Security and Defence Quarterly, 39(3), pp. 1–5. doi: 10.35467/sdq/154046.

Published: 28 September 2022

The idea to invite scholars and experts for this SDQ Special Issue came after the 6th Zagreb Security Forum in 2020, where it was clear that sufficient development of critical infrastructure protection (CIP) needs private-public partnership based on academic results (ZSF, 2020). As editors, we believe that this volume traces an intellectual debate over the course of actions toward an approach to strengthening resilience and ensuring sustainable development. The presented articles may contribute to the introduction of new solutions in the face of contemporary challenges and threats. In our opinion, studies and comparative analysis are not only investments in the protection of facilities, information and communication technology (ICT) systems, resource and data protection, but also investments in human capital, including the vetting of employees' knowledge of security.

Critical Infrastructure (CI) refers to systems and their functionally interconnected objects, equipment, installations, and services essential for the state's security and its citizens. Critical in this sense means crucial to ensure the efficient functioning of public administration, institutions, and businesses. Each EU member state specifically defines the sectors of national critical infrastructure (CI). European, supranational, critical infrastructure is also defined based on agreed criteria. Sectors where critical infrastructures is located should be connected both at national and international levels. However, the goal of rapid

exchange of experiences and information about security threats is limited by the security culture in various entities such as public institutions, private operators, stakeholders, and society (Newbeel, 2019). Security management it is not only investment in the protection of facilities and ICT systems, but also investment in human capital, including vetting employees' knowledge of security and risk-informed end-users.

Effective protection at the national and regional level is also limited by law, budget, and time. This rapid and complete sectoral exchange of information is essential in the process of preventing the appearance of the same threats in other places within the same sector. Given that CIs are strongly interconnected and interdependent to a considerable extent, it is necessary to establish intersectoral communication channels to prevent the occurrence of negative cascading effects and the spill over of a crisis from one CI to another. In such a way, one can very effectively try to prevent the creation of unwanted malicious actions against the economy and society. This protects democracy and the entire system of values, beliefs, and principles on which the EU is based. Advanced liberal societies are vulnerable. Therefore, physical protection cannot be separated from the process of increasing risk awareness.

We argue that CIP needs a proactive approach based on intertwined elements: the comprehensive perception of threats, minimising CI vulnerability by identifying systemic dependencies and interdependencies of critical infrastructure, and preparing societies for a possible crisis situation. The result of such an approach, based on resilience, is more flexible and allows one to adapt to a current, unforeseen situation. This Special Issue aims to provide an understanding of our perspective.

The sectors in which the CIs are located can be organised and/or divided according to several different criteria. One of the criteria can be the physical appearance of CI. Namely, numerous CIs exist in the physical domain. These are objects that have their own physical appearance. One of the key sectors where CI appears is of a non-material nature: vision, beliefs, and principles.[1] The content of this CI sector is most often the primary target of numerous attacks by contemporary attackers. By (re)shaping the identity values of the target audience (TA), the attacker is trying to (re)shape the TA so that under the influence of influence operations, the TA accepts new standards and acts according to the wishes of the attacker; and that TA may not even be aware of it. Identity CI is, in the context of emerging security challenges, very important because its resistance/resilience to modern security threats and risks is of key importance for the establishment of the entire defence system at the national and international level against contemporary and future security challenges.

[1] *In Croatia, this is "National Monuments and Values" sector of CI; https://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html*

In addition to identity CI, energy, water-food, cyber, and information and communication CI are key targets where the hybrid aggressor tries to achieve its dominance or supremacy. Therefore, it seems necessary, following the example of countries that have come a long way in designing and organising a preventive defence system (NCTV 2022), to organise the existing CI sectors into different but interrelated categories: Key Critical Infrastructure and Important Critical Infrastructure. The key critical infrastructure would include those CI sectors that have a strong malicious cascading effect on other CIs if they are hit by some of the threats. Energy, water-food, cyber, information-communication and identity infrastructure can (and should) find their place in it, because they are the primary targets of contemporary attackers.

The previously expressed views are justified if one analyses the conflicts and wars of the last few decades. Most of them started with attacks on one or more sectors of critical infrastructure. It is worth mentioning: (1) the process of changing existing regimes in North Africa, known as the Arab Spring, when different actors tried to change existing knowledge

and shape new ones in order to bring social and political changes in the affected states; (2) the war in Syria, when numerous activities in the information and media space tried to disintegrate Syrian society and encourage it to make internal political and social changes; when that didn't work, an armed conflict ensued that continues to this day. Analogical tendencies can be seen in contemporary Russian-Ukrainian relations. Russia has been using its own, Ukrainian, and international cyberspace for malicious activities (influence operations, cyber-attacks), its energy policy, and has developed capabilities in the information and communication space in order to influence operations that might lead to overthrowing the pro-Western government and the installation of a pro-Russian one in Kyiv. Influence operations are organised worldwide and have a considerable impact on modern liberal societies, as was seen during the presidential elections in the USA in 2016, the BREXIT referendum in 2016, and in attempts to alter voting behaviour in France, Germany, and Italy. Hostile multifaced activities are cleverly designed to remain below certain legal, detection-related, or response-related thresholds (Gasztold & Gasztold, 2022).

It is quite certain that due to the increasingly strong development of cyberspace and its importance as a fast and mostly uncensored communication channel which guarantees a high level of anonymity, future security will come from cyberspace. Almost every CI has a strong and thorough dependence on the safe and secure work of cyber space. It is both a front line and a tool used for other offensive malicious operations. Offensive actions will be hybrid in nature. This means that with the help of cyberspace, CI can be attacked with the means of a tactical level of importance, which can achieve results in the strategic domain. CIs will be attacked from one or more sectors in which CIs exist to obtain the maximum expected results. Attacks on different sectors of CI can be simultaneous, gradual, or in stages depending on the planning of operations and on the ratio of expected and achieved results of the first and later actions. The goal is to cause a cascading effect with negative consequences for society and the state in reducing its ability to detect risk, not recognising the threat, the absence of defensive measures and imposing the attackers will on the TA. The use of kinetic combat assets comes into consideration only if the influence operation does not achieve the expected results (such as the Russian aggression against Ukraine, because the influence operations did not achieve the desired results).

The papers published in this volume of the SDQ show that the challenges faced by different societies and countries are very similar. Especially in the protection of critical infrastructure and attempts to preserve and recover its normal, safe, and reliable functionality after its exposure to threat. If there are CI threats that exist within one sector in country A that the same sector in country B has not yet felt or noticed, this does not mean that this type of threat will not happen there too. The works we are publishing along these lines are therefore of value.

It is no longer a question of whether a risk will turn into a threat and endanger the functioning of one or more CIs. The question is when, with what intensity, with what intention (intentionally or accidentally), for how long and with what consequences will a particular (or several) sector(s) of CI be exposed to malicious activity. Given that jeopardising the functioning of CI, which is largely privately owned, also endangers the normal functioning of the entire society and the state, the strong and responsible cooperation of all stakeholders is necessary. Owners and managers of CI must invest in making critical infrastructure more resilient. States should encourage these investments because it is of great benefit to them and their societies. Justified investments in the resiliency of CI should be supported and recognised as an investment in the defence of the state and treated in the same way as tax relief. On the other hand, these justified investments recognised by the state can, and should, be recognised as defence budget expenditures.

Events have been reported when a large number of CI sectors[2] were directly endangered by the appearance of two powerful threat generators: the simultaneous negative impact of the COVID-19 pandemic and connected reduction of the functionality of society at almost all levels, and the powerful and devastating earthquakes that hit Croatia in 2020 (Akrap, 2021). The integrating effects of these two crises in the city of Zagreb (March 22, 2020) did not have a major negative impact on society due to the preparedness of Zagreb's crisis management and protective system. This was in contrast to a similar case in the city of Petrinja (December 28-29, 2020), when there was a complete collapse of the protection and crisis management system at the level of the affected county for almost 7 days.

Furthermore, it is necessary to develop the abilities of crisis management and crisis and strategic communication at different governance levels, especially in cooperation with all parts of society: private, state, public, academic, and non-governmental. That is the concept of homeland security or whole-of-state approach. All interested stakeholders should actively work to identify and later recognise the signals that may indicate the appearance of a certain threat early enough for the system to be able to defend itself effectively. It is also necessary to work on developing the ability to oppose threats through a policy of prevention by deterrence. This should include the ability to safely, reliably, and unequivocally identify a possible attacker so that the system can react and transfer the crisis to the "attacker's territory," applying the analogy of the reciprocal level of response (differentiating the processes of defence and retaliation). Given that future risks will increasingly be carried out in cyberspace, it is necessary to work on the development of one's own digital sovereignty in the wake of the Berlin Declaration (Berlin Declaration 2020).

How well and safely we will live in the future depends on the reliability and resiliency of critical infrastructure. Will some still be able to dream of a different, utopian, world like John Lennon in his song *Imagine* (1971), or will we face the scenario described by Marc Elsberg in his book *Black Out* (Elsberg, 2012) every day? It is expected that the EU directives NIS2 (NIS2 Directive, 2020) and CER (CER Directive, 2022) will create the foundations of the contemporary framework of CIP. However, the key factor, human behaviour, remains an unpredictable variable.

We owe thanks to many people involved in the publishing process and not least to our contributors. We appreciate their responses (and patience) to our pressures, and we have learned a great deal from them. Selected articles remain a useful starting point not only to understand current trends and dynamics in crisis management and risk assessment but also to gain recognition among decision-makers. This Special Issue is an introduction to the diverse ways in which CIP can be examined by security scientists.

[2] *Such as transport, energy, health protection, communication and information technology, food, public sector, and science and education (seven from eleven CI sectors defined in Croatia, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html).*

References

Akrap G. (2021) *The role of STRATCOM in crisis from the defence systems' perspective*, Central European Defence Cooperation, The STRATCOM Expert Workshop: Combating fake news and disinformation campaigns", Zagreb, VTC, October 13. Available at: https://cedc.info/mors_event/cedc-stratcom-expert-workshop-combating-fake-news-and-disinformation-campaigns/; https://www.morh.hr/en/cedc-and-western-balkans-stratcom-expert-workshop-combatting-fake-news-and-disinformation-campaigns/ (Accessed: 30 August 2022).

Berlin Declaration (2020) *Berlin Declaration on Digital Society and Value-based Digital Government*, December 8. Available at: https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government (Accessed: 30 August 2022).

CER Directive (2022) *Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities*. Brussels, December 12 (COM/2020/829 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829 (Accessed: 30 August 2022).

Elsberg M. (2012) *Blackout: Morgen ist es zu spät*. München: Blanvalet Verlag.

Gasztold A. and Gasztold P. (2022) 'The Polish Counterterrorism System and Hybrid Warfare Threats', *Terrorism & Political Violence*, 34(6), pp. 1259–1276. doi: 10.1080/09546553.2020.1777110.

NCTV (2022) *Critical Infrastructure Protection.* National Coordinator for Security |& Counterterrorism, The Netherlands. Available at: https://english.nctv.nl/topics/critical-infrastructure-protection (Accessed: 1. September 2022).

Newbeel C. M. (2019) 'Defining Critical Infrastructure for Global Application', *Indiana Journal of Global Legal Studies* 26(2), pp. 761–780.

NIS 2 Directive (2020) *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, December 16, (COM/2020/823 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN (Accessed: 30 August 2022).

ZSF (2020) *Grand Strategy, Foresight and Hybrid Threats 21st Century - Making Society and Critical Infrastructure Resilient*. Zagreb Security Forum organized by Hybrid Warfare Research Institute & St. George Association, Zagreb September 3–4, 2021. Available at: https://zagrebsecurityforum.com (Accessed: 1 September 2022).