ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY
A MAGYAR TUDOMÁNY ÜNNEPE
Az MTA programsorozata
Engineering Symposium at Bánki
(ESB 2024)

Cyber threat of social critical infrastructure

[1]Péter Balogh

[1] *University of Szeged Department of Sociology. Szeged, Hungary, baloghp@socio.u-szeged.hu*

Abstract

In this article, we introduce some results concerning certain characteristics of cyber-attacks against social critical infrastructure. The investigation applies a quantitative approach based on statistical analysis of relevant data sources and a secondary dataset for the purpose of network analysis. From an operational perspective, a model of network asymmetry is introduced and utilized while exploring patterns of structural advantages. Based on the results, cyber-attacks against social critical infrastructure show an increasing trend in the last decade and have caused significant damages dominantly private targets, with some key actors in the network of the countries concerned.

Keywords: Cyber Operations, Critical Infrastructure, Data Analysis, Network Advantage

1. Introduction and research problem

Cyberspace – with its physical and cognitive elements – can be considered a crucial sphere of the increasingly complex societies of the new millennium, but it is an area that deserves special attention when examined in terms of the challenges, risks, and threats associated with various critical infrastructure elements. Based on the sectoral security concept by Buzan and his co-authors [1], we can distinguish segments of complex social systems. Among these, the informational sector of security is typically associated with the IT tools of various organizations and users. In this research, however, we approach this dimension of security related to cyberspace as having significant relevance for all aspects of the given society as a complexity, i.e., it affects the state and functioning of other sectors of security. In accordance, in the multi-domain approach of conflicts [2], the multi-actor [3] and multidimensional [4] cyberspace is one of the five areas in which threats can unfold [2, 5, 6]. The complex nature of cybersecurity is particularly important with regard to critical infrastructure [7], and as a kind of circular process, cyberspace itself currently also constitutes a kind of critical infrastructure [8].

This article introduces some of the research results concerning the trends, patterns, and characteristics of cyber attacks by state actors [9] in a specific area: social critical infrastructure in the new millennium. Our particular interest concerns the structural characteristics of the network evolving from the cyber operations.

2. Methodological background

The investigation is based on a quantitative approach applying the method of secondary data analysis. In order to explore the patterns and characteristics of cyber operations targeting social assets of critical infrastructure, the DCID dataset has been utilized [10], which contains several different aspects of interstate cyber operations with a total sum of 429 cases regarding the time period between 2000 and 2020. In the course of data analysis, we applied statistical description and

comparisons, furthermore, some elements of network analysis methods. In each case, if not indicated otherwise, Chi-square tests were used to statistically investigate the significance of the differences measured in the comparisons, considering an alpha of 0.05.

2.1 Conceptual and operational considerations

In the examination the following sectors of critical infrastructure were considered to be relevant as social ones: Commercial Facilities; Communications; Emergency Services; Financial Services; Food and Agriculture; Healthcare and Public Health; Transportation Systems; Water and Wastewater Systems; Other (Election Infrastructure, Academia); and all the other sectors (Chemical; Critical Manufacturing; Dams; Defense Industrial Base; Energy; Government Facilities; Information Technology; Nuclear Reactors, Materials, and Waste) were grouped in the other category.

As for the operationalization of the network characteristics we introduced [11] and applied in this analysis, the concept of network asymmetry or structural advantage is based on two different aspects. On the one hand, it is worth distinguishing between relational – i.e., link or edge-based – and node-based – i.e., actor-based – forms from the [1] formal aspect. On the other hand, a [2] character-based breakdown can be applied, which refers to whether a single link or possibly multiple or multi-dimensional relationships are characteristic between the parties involved. By combining the two aspects, more complex patterns of network benefits can also be interpreted or examined through practical examples of various possible cases.

Table 1. Dimensions and forms of network advantages (own edition)

		Nature of ties	
		simplex	**multiplex**
formal aspect	relational	1	3
	node-based	2	4

3. Research results

3.1 Trends of the cyber incidents

Critical infrastructure elements classified as social critical infrastructure and other categories appear in approximately one-third to two-thirds of the cyber-attacks examined here (31.2% and 68.8%), and clear differences can be seen in the temporal trends of the operations. Cyber-attacks against social critical infrastructure typically occur at a lower rate, but the data shows a continuous increase (Figure 1.A). Apart from some minor declines, a stable positive trend can be revealed (this is particularly clearly visible in the data series containing cumulative values), while the pattern can be considered much more varied for operations against other targets, and from 2015 onwards, a fundamentally decreasing trend prevails – to the point that by the end of the investigated period, attacks against socially relevant critical infrastructure exceed the number of operations against other systems. So, a generally different pattern can be observed since the mid-2010s, with an increase in attacks against social critical infrastructure elements and a decrease in operations against other targets, which may indicate the increasing importance of the former.

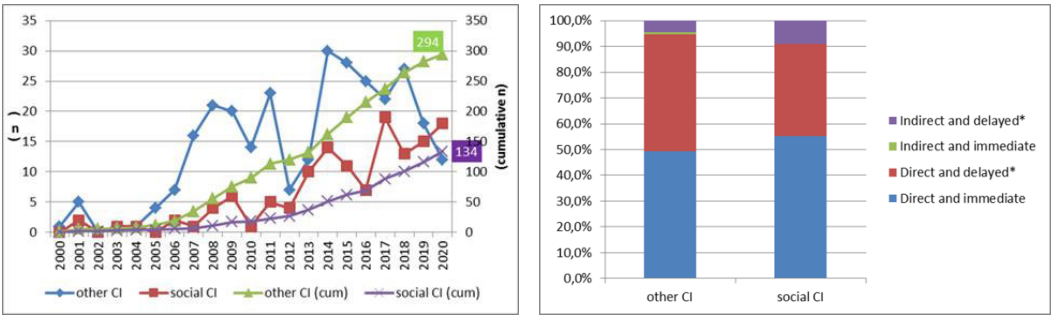

Figure 1. A, B. Tendencies and damage type of cyber attacks (own calculations)

3.2 Composition and characteristics

In the case of attacks against critical social infrastructure, civilian non-state targets represent a dominant proportion (71.6%), followed by government non-military targets at a relatively higher rate (23.9%). While in the case of other operations, this latter category appears at the highest rate (49.2%), and civilian and government military targets occur at a similar rate (p=0.000). Although the nature of the damage caused by the attacks cannot be considered statistically significant (p=0.063), based on the relevant statistical indicators, a notable difference emerges in terms of delayed damage (Figure 1.B). The residual values indicate that direct and delayed attacks occur in a slightly higher proportion (45.4%) in the case of operations against social critical infrastructure, while in the other group of attacks, indirect and delayed damage forms can be observed in a somewhat higher proportion. That is, the role of delayed effects in attacks against socially relevant critical infrastructure can be considered remarkable, which can also be interpreted as a kind of peculiarity in terms of the complexity of social systems and their potential level of resilience. An interesting difference can be measured regarding information operations (p=0.046). Actions against other types of critical infrastructure are coupled with information operations in a proportion of about one quarter (25.1%), while in the case of socially relevant critical infrastructure, this share does not reach one-fifth (16.4%), which implies a less complex picture. Similar results appear in terms of the additional actors possibly present in the composition of cyber operations – a presence of a possible third party (additional state actor, rebel group, corporation). Based on the data, these actors are present with greater frequency (9.2%) in attacks against other types of critical infrastructures, while in the field of operations against social critical infrastructure, their proportion is lower (p=0.048), at only 3.7%. This also implies a less complex pattern of cyber operations against social critical infrastructure[1].

Table 2. Some characteristics of cyber-attacks (own calculations)

	information operation	**third-party initiator**
other critical infrastructure	25.1%	9.2%
social critical infrastructure	16.4%	3.7%

[1] No statistically significant difference can be measured regarding the objectives (p=0.128), attack methods (p=0.412), objective achievement (p=0.239), the presence of supply chain attack (p=0.698), concessionary behavioural change (p=0.269), and ransomware attacks (p=0.091).

3.3 Network structure and characteristics

The investigated cyber-attacks against social critical infrastructure evolve into a network of the countries concerned, with a total sum of 24 nodes and 244 ties (Figure 2). The network proves to be an integrated one, since all of the nodes can be reached by any of them at least indirectly through paths of different lengths. However, the structure could also be considered fragmented, as different clusters can be explored in the network. These clusters prove to evolve around the main actors of the cyber sphere: China, Russia, Iran, and North Korea are the countries that seem to dominate the network structure of the countries involved in attacks against social critical infrastructure. The seizure of the hubs around Russia and China is approximately similar to 8-9 other countries, and in this sense, North Korea and Iran could also be considered identical, as their sub-network consists of a similar number [4,5] of adversaries. The activities in the cyber sphere of these four major countries overlap in different ways – this can be demonstrated most clearly with the United States, which is part of all of the clusters. That is why the United States can be found in the most central position of the network, and a partially similar position can be seen in the case of the United Kingdom, which has been attacked by China, North Korea, and Russia as well. From this perspective, Turkey, France, and Japan also have a similar position around the borders of more network segments of the four main actors.

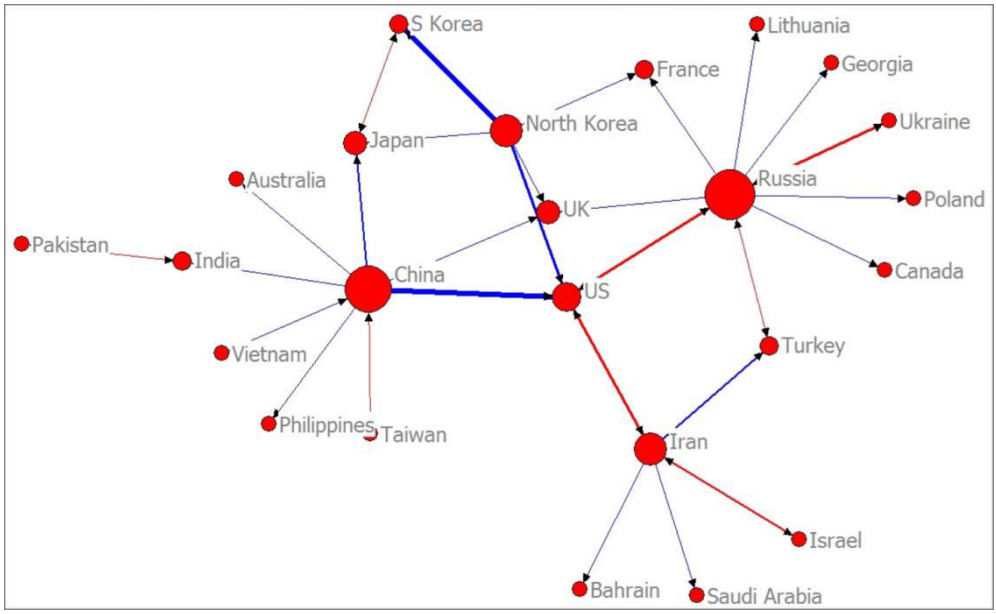

Figure 2. Network of the countries involved in the cyber-attacks

The network – at least partially – also reflects some of the traditional opposing relations and even the actual conflicts implied by the mutual links (highlighted with red coloured tie) between certain nodes. India and Pakistan have a longer-term regional competitive relationship, which seems to be present in the cyber dimension as well. In the case of Israel and Iran, the situation is also similar. The Russo-Ukrainian conflict and the confrontation between China and Taiwan are reflected in the cyber network as well. The United States is also related to Russia and Iran with reciprocal ties, that is their generally competitive relation in the international sphere can also be illustrated in this section of the cyber activities.

The positions of the countries in the network can be characterised with different measures and

figures. From an overall perspective the distribution of the ties can be considered rather concentrated as the share of three ones from the four main actors with the relative frequency of the United States covers more than half (59,8%) of the total ties with a dominant value of the United States (19,3%), and similar shares of China, North Korea and Russia (13,9%, 13,5% and 13,1% respectively). However, if we distinguish between the values of the directed links, it can be said that the United States has dominantly inward relations – that is, in most of the operations, it is the attacked party – while the other key actors have higher shares in the outward relations. The differences based on the distinction of the roles in the investigated cyber-attacks imply a slightly negative relation (Figure 3.A) where the countries with a higher level of attacking activities tend to have lower values of becoming victims (and vice versa). However, there is a great variance among the countries.

When investigating the different dimensions of network asymmetry, an opposite pattern can be explored – in accordance with our essential presumption. In our initial model introduced above we distinguished between two aspects of structural advantage – as for the perspective of the formal dimension we refer to the node-based aspect with the size of the network of the countries in the network, and as for the other dimension we quantify the aspect of simplex-multiplex nature of the relations by calculating the average number of ties. Comparing these values of the countries[2] in this case involved in the cyber operations against social critical infrastructure a pattern with positive relation emerges (Figure 3.B). That is, the countries that have a higher position in one of the network advantage dimensions tend to be in a more favourable position from the perspective of the other dimension as well. The pattern of the values also implies that all the countries with values higher than the average in one dimension prove to have above-average values in the other aspect; furthermore, most of the countries with size values lower than the average can be found in the below-average value range in the average tie dimension.

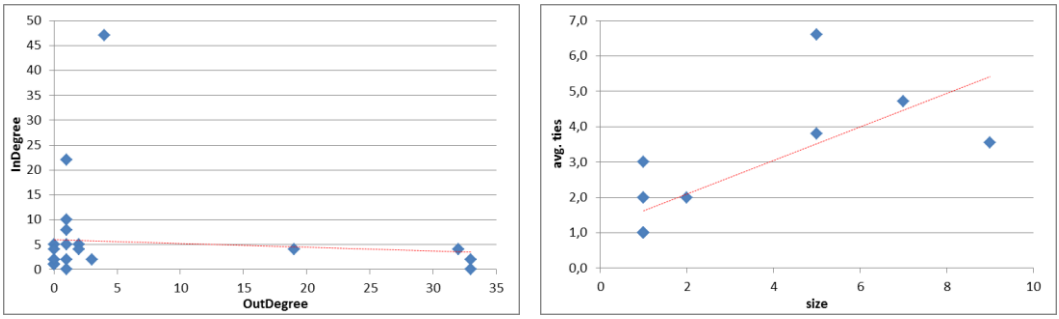

Figure 3. A, B. Network Characteristics of countries in the network (own calculation)

4. Concluding remarks

Based on the results of the data analyses [1], social critical infrastructure as a target of cyber operations proves to cover approximately one-third of the attacks investigated, characterized by an increasing trend in the last decade. This category of critical infrastructure cyber-attacks [2] proves to have dominantly delayed damages on private targets with [3] methods, objectives, and success similar to the other group of critical infrastructure. As a kind of specific characteristic [4], the less frequent presence of information operations and other actor involvement could be explored in the case of the actions against social assets of critical infrastructure. The cyber operations investigated from a network perspective evolve into [5] structure built around some key actors which – on the one hand – seem to be gravitation points with particular network segments, and – on the other hand

[2] In this case the data analysis needs to be narrowed down to the relevant part of the countries in the network that have attacking relations, that is the following considerations apply to the 14 states which have outdegree values.

– these nodes are in certain cases [6] interlinked by mutual relations thus also enhancing the embeddedness of the network. Both from the perspective of the distribution of the [7] in- and outward ties among the countries and the values measuring the different aspects of network advantage, specific patterns could be explored, which, in the latter case, imply a kind of convergence of the characteristics or advantages in the network.

Among some further possible directions of the investigation, a more complex, multi-variable statistical analysis of the cyber operations, a more profound study of the evolution of the network characteristics, and a comparative approach utilizing other relevant data sources can be considered in order to better evaluate the validity of the present outcomes.

5. References

[1] Buzan, B., Wæver, O., de Wilde, J. (1998). Security: A New Framework for Analysis. Boulder, London: Lynne Rienner Publisher

[2] Fazekas F. (2022). A multitér (multi-domain) műveletek kialakulása és szükségessége. Hadtudomány 2022/2. 59-73.

[3] Kovács L. (2018). A kibertér védelme. Budapest: Dialóg Campus Kiadó.

[4] Haig Zs. (2018). Információs műveletek a kibertérben. Budapest: Dialóg Campus Kiadó.

[5] Chwe, H. (2016). The Rise of Cyber Warfare: The Digital Age and American Decline. Swarthmore International Relations Journal 2016/1. 43-49.

[6] Robinson, M., Jones, K., Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & Security 49 (2015) 70–94.

[7] Amin, H. E., Samhat, A. E., Chamoun, M., Oueidat, L., Feghali, A. (2024). An integrated approach to cyber risk management with cyber threat intelligence framework to secure critical infrastructure. Journal of Cybersecurity and Privacy, 4(2), 357-381. https://doi.org/10.3390/jcp4020018

[8] Amir Djenna, A., Harous, S., Saidouni, D. E. (2021). Internet of things meet internet of threats: new concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580. https://doi.org/10.3390/app11104580

[9] Balogh P. (2024). „Túlélhetjük-e…?" - … avagy a számítógép nem játék" In: Csizmadia N., Kasznár A., Hágen Á., (eds.): Neumann János élete és munkássága. Lakitelek, Antológia Kiadó, 13-28.

[10] Maness, R. C., Valeriano, B., Hedgecock, K., Jensen, B. M., Macias, S. M. (2022). The Dyadic Cyber Incident and Campaign Dataset, version 2.0.

[11] Balogh P. (2025.) Hálózati aszimmetria az új évezred konfliktusaiban – bevezetés, értelmezés, alkalmazás, értékelés. Hadtudományi Szemle, 2025. különszám (megjelenés alatt)