CRITICAL INFRASTRUCTURE DIPLOMACY – TRACING THE CONTOURS OF A NEW PRACTICE

Adrian Victor VEVERA
National Institute for Research and Development in Informatics – ICI Bucharest
victor.vevera@ici.ro

Abstract: The security environment, as evidenced by the hybrid warfare methods applied during the Ukrainian conflict starting in 2014, and by the global pandemic and its after-effects, is complex, dynamic and challenging. This article describes the challenges we are facing in terms of critical infrastructure protection, articulates some of the systemic trends, and proposes a new perspective on managing international cooperation to address critical infrastructure issues. Critical Infrastructure Protection Diplomacy is an emerging field that mixes diplomacy with technical expertise related to systemic issues in order to effect systemic governance.
Keywords: Critical infrastructures, Diplomacy, Systemic governance, Resilience, Risk.

INTRODUCTION

The functioning of our advanced and complex societies has been repeatedly disrupted by localized crises whose effects expanded beyond their initial borders and regions, and beyond the initially affected sector of human activity. Both the pandemic and the recently resumed war in Ukraine have had complex effects on a variety of systems and in widely spaced places. The conceptual framework of Critical Infrastructure Protection (CIP) explains these cascading disruptions and contagion effects and provides tools and methodologies to address them. This article argues that, similarly to cyber diplomacy, we can define a subdomain of international relations we title Critical Infrastructure Protection Diplomacy (CIPD) whose practitioners deploy specialized knowledge and engage in specific activities to counter the risks, vulnerabilities and threats generated by the complexity and emergent behaviors of the critical infrastructure (CI) system-of-systems (Sousa-Poza et al., 2008) in a dynamic and challenging security environment. This article sketches these issues and presents trends which indicate an amplification of the aforementioned factors of disruption. Finally, we sketch a sectoral perspective for CIPD on energy.

CRITICAL INFRASTRUCTURE PROTECTION

Infrastructures are socio-technical systems composed of facilities, distributed technical assets, organizations and legislative and administrative frameworks for governance which produce goods and services, as well as facilitating the economic, social and political activities of our societies (Moteff et al., 2002). These range from power plants and pipelines to roads, ports and railways, as well as financial markets, banking, education, health and public administration. They are critical if their destruction and disruption would generate significant human losses, material damage and loss of prestige and confidence in authorities on the part of citizens, partners, allies, investors and other stakeholders. Critical infrastructures are identified and designated on the basis of critical thresholds defined by the competent authorities to ensure

the concentration of scarce security resources where they are most necessary, on the basis of the reality that we cannot protect all infrastructures all the time (Gheorghe et al., 2018).

The globalization trend has led to critical infrastructures aggregating into conglomerations that go beyond national borders and function at regional and global levels (Helbing, 2013). The digitalization of critical infrastructures contributed to this trend, by facilitating coordination and control at higher levels, with the consequences of introducing new risks related to exposure to an increasingly dangerous cyber environment (Georgescu et al., 2020).

The CIP framework offers two useful concepts for understanding how disruptions occur and are transmitted through geographical space and sectoral boundaries. The first is the concept of interdependencies, where CIs features (bi)directional interrelationships which facilitate the transmission of a change in the state of one infrastructure to another. These can be geographical, logical, physical, informational, cybernetic and social/political (Gheorghe & Schlapfer, 2006). This is a key explanation for economies of scale, growing productivity and economic efficiency, but also the origin of common cause failures, escalating failures (where infrastructures influence each other in a feedback loop) and cascading disruptions. The latter represents the second concept, explaining that the fortuitous alignment of breakages can ensure the rapid transmission of disruptions throughout an entire system-of-systems, prolonging a crisis and amplifying damages beyond what could be predicted by decisionmakers (Pescaroli & Alexander, 2016). The complexity of infrastructure systems leads to emergent behaviors through the interaction of numerous components, as well as uncertainty and ambiguity in ascertaining system reactions to decisions and events (Keating & Katina, 2016).

KEY TRENDS

CIPD is also justified by the likely future evolution of the critical infrastructure system-of-systems (Sousa-Poza et al., 2008), whose trends suggest a process which will lead not only to greater economic efficiency and greater capabilities, but also greater risks, vulnerabilities and threats.

Figure 1 highlights some key systemic trends.

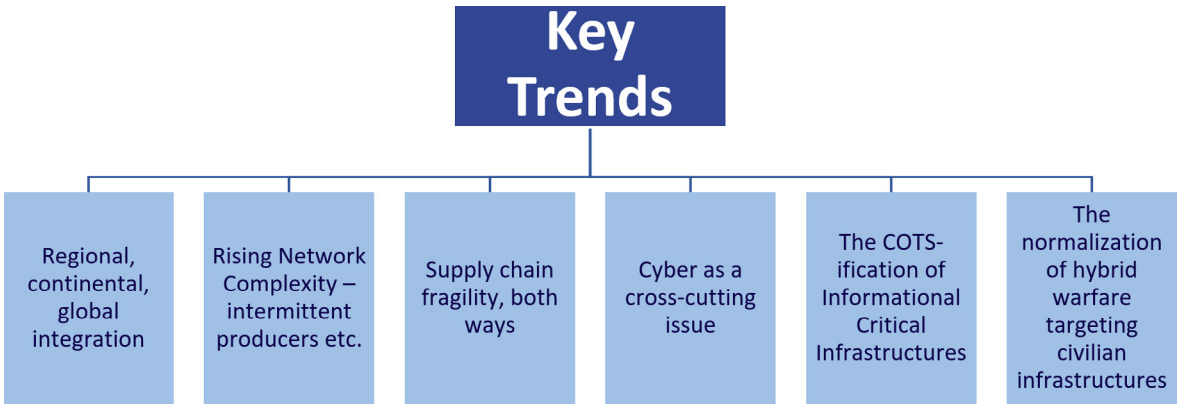

Figure 1. *Key trends in the evolution of the CI system-of-systems (source: authors)*

These trends are explained as follows:

- Regional, continental and global integration are an ongoing process of transborder interconnection of critical infrastructures under the impulse of efficiency and value creation (Helbing, 2013). The first transborder infrastructures appeared as a result of global divisions of labor and differences in endowment with natural factors – ex: producers of basic foodstuff and of energy sending these critical products elsewhere. Now, they area appearing as the result of a drive towards greater efficiency from economies of scale and larger markets – ex: the EU Energy Union. Not all infrastructures are as interconnected or are interconnecting at the same level and the same rate.

- Rising network complexity refers to the qualitative transformation of infrastructure networks, as opposed to just the quantitative one described above. They are becoming more complex because the linear rise in infrastructure components is accompanied by an exponential rise in the number of possible interactions, generating emerging behaviors, system ambiguity and uncertainty as to the consequences (Keating & Katina, 2016);

- Supply chain fragility – the pandemic and the recent upsurge in the Ukraine crisis have underscored the fragility of supply chains, and how easy it is to destabilize them through demand and supply shocks leading to the overburdening or the atrophy of logistical systems;

- Cyber has become a cross-cutting issue through the ongoing digitalization of critical infrastructures, which has become interconnected across sectors and geographical regions by the cyber domain, either through direct links related to their functioning, or through their general exposure to the global cyber environment (Georgescu et al., 2020);

- The COTS-ification of critical information infrastructures refers to the trend for "commercial off the shelf" hardware and software to be used in critical infrastructure systems (especially their cyber command and control components) as a way of reducing costs and enhancing capabilities (Georgescu et al., 2019). Before, critical infrastructures used bespoke hardware, operating systems and applications, along with separate communication channels, which created a "security by obscurity" effect. The more recent trend is to go in the opposite direction, which is also enhancing the surface contact with the challenging and threatening cyber environment. The Internet-of-Things paradigm is also supercharging the COTS-ification rate of critical infrastructures, as trillions of unpatched and unpatchable sensors, LED lights and other components get integrated into facilities, providing entry points for knowledgeable hackers (Georgescu, 2018). On the software end, the use of open-source libraries and operating systems in systems such as satellites will also result in the same thing;

- The normalization of hybrid warfare targeting civilian infrastructures – while we can trace this trend to the cyber-attacks on Estonian banks and public administration in 2007, the invasion of Ukraine by Russia was accompanied by attacks not just on Ukrainian civilian infrastructure, but also on those of partner or supporting countries. The very good cost/benefit ratio of cyber attacks, coupled with attribution issues and with the centrality of

critical infrastructures to the functioning of our societies has led to the normalization of hybrid attacks against them, with multiple possible purposes – economic damage, data theft, physical sabotage, data manipulation, demoralization, deterrence, humiliation etc.

At the cyber level, we also have a series of interesting trends that signify a greater increase in the exposure to various deliberate risks:

- Cyber as a permeating and penetrating factor in every critical infrastructure system. It is so important, that the European regulatory frameworks are converging, with the Critical Entities Resilience Directive's critical infrastructure taxonomy being identical to that of the NIS 2 Directive (Figure 2);

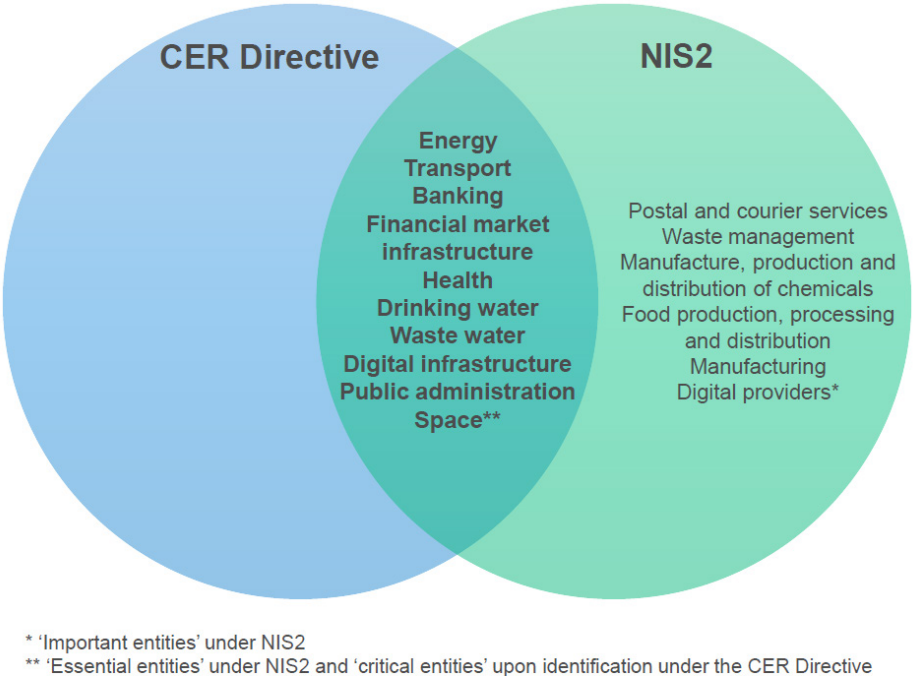

Figure 2. *The overlap between the proposed CER Directive and the NIS 2 Directive (source: DG ENER presentation, 2021)*

- The rise of hybrid warfare and advantages of cyber-attacks;
- The effects of transborder organized crime, which are undermining public institutions, turning states more fragile and providing support (through specific services) to terrorist groups (identity, data, resources for cyber-attacks), to state proxies or to state actors themselves (Georgescu, 2018);
- The commodification of malware, where even non-expert attackers can employ purchasable tools to generate significant damage in an unprepared victim organization (Georgescu, 2018);
- The innovative and dangerous rise of commercial-off-the-shelf systems and system components (Georgescu et al., 2019);
- The blurring of the lines between physical and virtual infrastructure;

- The threat proliferation and diversification outpacing improvements in security culture and in the regulatory frameworks governing these issues;
- The "proliferation" of cyber weapons and the competence of non-state actors in employing them to great effect for strategic, financial or ideological reasons;
- Initial application of new technologies – blockchain and AI – creating new advantages but also risks;
- The mismatch between territorialized state agencies and institutions and cyberspace, which do not have borders per se, except in the physical infrastructure supporting them.

CRITICAL INFRASTRUCTURE PROTECTION DIPLOMACY

Critical Infrastructure Protection Diplomacy is the use of diplomatic means, tools and organizational modes to address issues related to the secure design, construction, operation and decommissioning of transborder critical infrastructures. It entails a wide variety of actors, bringing together government, the private sector, academia, civil society and international organizations.

We envision this subdomain of international relations study and practice as a pragmatic, risk oriented form of diplomacy, which aims to be realistic about the underlying security environment which it must address and whose goals are oriented specifically towards achieving greater security and resilience, as opposed to secondary roles unrelated to that.

One constant of the significant changes that the critical infrastructure system-of-systems has undergone is that the internationalization of critical infrastructure networks means that countries are "condemned to cooperate" to protect critical infrastructures on which they are mutually reliant, regardless of underlying tensions or geopolitical confrontations. Therefore, the current tensions between China and the West should also contain a dimension of CIPD in two directions. The first is the use of CIPD to mobilize partners and allies for comprehensive action in the field of critical infrastructures, as dictated by geopolitical considerations, whether it means excluding Chinese equipment providers from Western 5G networks or securing infrastructures against geopolitically motivated cyber attacks attempting to sabotage or steal information. The second is the use of CIPD to handle the non-reducible risk of existing critical infrastructure ties between countries, regardless of momentary or long-term disagreements and tensions. The trade between China and the West is persistently at a very high level, and the pandemic has proven that disruptions in this trade can affect both sides, with limited political and economic scope for amelioration through a reduction in economic exchanges. Since global networks are only as strong as their weakest links and there is a significant risk of cascading disruptions across economic sectors and geographical boundaries, it follows that cooperation in CIP must be achieved. CIPD offers a set of tools to enable this, while also making it possible to regard it as a source of cooperation, trust building and amelioration of tensions.

Figure 3 indicates the main avenues for CIPD that we have identified on the basis of the practice of inter-state CIP cooperation.

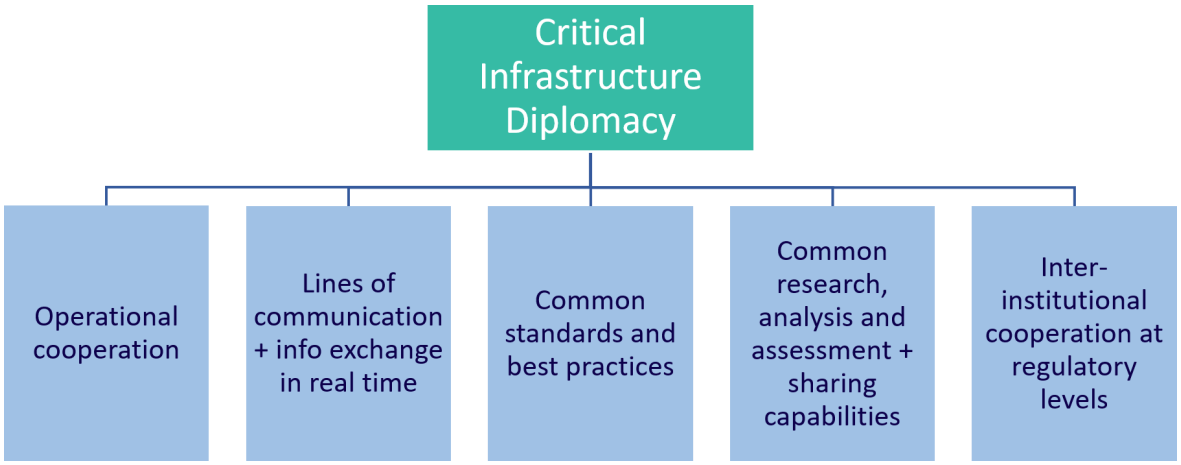

Figure 3. *Elements of Critical Infrastructure Protection Diplomacy (source: authors)*

The domains are as follows:

- Operational cooperation is related to the exploitation of existing critical infrastructure or the implementation of new critical infrastructure projects;
- Lines of communication and information exchanges in real time – the operational cooperation requires lines of communication, preferably between counterpart positions rather than going through to the highest level to be approved on a case-by-case basis;
- Real-time information exchanges are the result of very high trust between countries, which decide to share information on important issues, such as cyber-attacks and other alerts, as they come in, rather than subject to review to expunge sensitive information. Information exchanges are required because of the fragmentary nature of transborder critical infrastructures, which limits the information that is accessible to any one group of competent state authorities in a particular country. However, CIP processes and increasing resilience require high levels of information regarding the security environment, including upstream, downstream and laterally in the supply and production chain for critical goods and services. Only through real time exchanges between countries, whether through government entities or as a service permitted to private entities, can decision makers aspire to having a picture that is as complete as possible;
- Common standards and best practices – the states or other stakeholders can share best practices and develop common standards to enable a growth in the minimum level of CIP provisioning and to enable better cooperation;
- Common research, analysis and assessment, as well as sharing capabilities – states can aid each other in achieving a higher level of CIP as a precondition for increasing resilience, involving cooperation beyond the sharing of best practices and moving into the operational domain and the pooling of important resources, such as back-ups and modelling and simulation capabilities;
- Inter-institutional cooperation at regulatory levels – last, but not least, these desiderata are achieved through inter-institutional cooperation, including at regulatory levels,

where the various competent authorities cultivate converging perspectives and practices and cooperate to reduce asymmetries and uncertainties in regulating CIP, which, among others, also simplifies the regulatory processes for companies operating transborder critical infrastructures.

The previous enumeration indicates a significant compatibility with cyber diplomacy. In fact, there is a significant overlap, because of the role of cyber in critical infrastructure control, coordination and data gathering, and because of the future ubiquity of cyber-physical systems (Georgescu et al., 2020). The difference stems from the much more in-depth treatment of the cyber issues that cyber diplomacy affords, including in emerging technologies, while CIPD has, by necessity, a much wider net of interests, including an all-hazards approach.

Regarding practical approaches for CIPD, there are numerous approaches that we envision and we enumerate a few of them:

- Technical assistance for developing and implementing a CIP roadmap, in countries without one, from legislative issues to personnel training and administrative development;
- Common security planning sessions for future infrastructure projects, pursuing resilience by design and having cooperation in place when the project is complete;
- Fostering research on cross-border infrastructure risks, which is an important information gap for state authorities;
- Organizing exercises to anticipate the results of the materialization of these risks and to formulate response options;
- The sharing of capabilities between states, whenever possible, such as access to cyber ranges, to data libraries and other facilities;
- The implementation of data transmission measures, both digital and automatic, but also through Security Liaison Office mechanisms (within state authorities and critical infrastructure operators) for the transmission of early warnings and other information;
- A reduction in asymmetry of information regarding local infrastructure security environment between states, through various mechanisms of exchange, including at the level of professional education programs;
- Decide, plan and implement measures for more transparency and predictability of the functioning of transborder critical infrastructures;
- Decide, plan and implement measures for the minimization of damages and the rapid resumption of an acceptable level of functioning for critical infrastructures.

TOWARDS A SYSTEMIC ENERGY DIPLOMACY

We can theorize an example of CIPD, based on a sectorial division of the issue. For instance, we may take Systemic Energy Diplomacy, which encompasses energy diplomacy as we

consider it, related to the price, demand and supply for energy, but also adds the issue of critical infrastructure provisioning and protection for extraction, transmission, conversion (to electricity or heat) and consumption in an international relations and transborder context.

Such an approach makes sense in many different ways, which are beyond the scope of this paper, but it suffices to state some background realities. Firstly, the energy context is changing rapidly and strongly – we saw the energy independence of the US after decades of reliance on imports from the Middle Eastern region and from places such as Venezuela; we saw the US becoming the world's top producer of energy and then losing the title; we have seen extraordinary variations of price, more than 100% in either direction; we have seen attacks against energy infrastructure of all types, both in the context of conflict but also as a backdrop to non-violent struggle for geopolitical power; and energy is one domain which is not amenable to "slowbalization" or autarchy in the context of the requirements of an advanced society (affordable, accessible and sustainable energy), so it will remain an important component of international dialogue, competition and cooperation, mediated by expensive and vulnerable critical infrastructure assets.

Secondly, we are undergoing a politically motivated green transition and decarbonization which implies the management of deliberate shifts in critical energy infrastructure topology – the phasing out of certain energy sources (coal), the rapid build-up of other types of energy (renewables), the need to balance grids by having back-up power (mostly based on natural gas) or energy storage requiring vast industries to implement and service, the interconnection of energy grids, including by using the electricity trade to balance supply and demand fluctuations, as well as new economic arrangements to sustain societies prioritizing intermittent sources of energy. These issues also include the prospect of the rapid adoption of new technologies with systemic impact on global energy infrastructure, including through advances in accessing reserves that will shift the geographic centers of energy extraction or production.

Thirdly, the permanent presence of geopolitical considerations also has a significant effect on critical infrastructures, since projects are planned and implemented or hindered also in accordance with geopolitics.

A Systemic Energy Diplomacy helps partners to coordinate the design, implementation, operation, protection, security, response and policies for the affordability, sustainability and accessibility of energy.

CONCLUSION

The challenges of the modern world can be analyzed through a CIP perspective, revealing how the functioning of interdependent and interconnected CIs affects the security of our societies. Following on the development of Cyber Diplomacy as a discrete field of study and practice in international relations, we propose Critical Infrastructure Protection Diplomacy as a response to the aforementioned challenges, opening a rich field of inquiry in a domain that includes, by necessity, an all-hazards and multidisciplinary approach, with an important variety of stakeholders, and great sectoral variability. It also features an important overlap with cyber diplomacy, since critical information infrastructures are a recognized CI sector and critical components of other CIs.

REFERENCE LIST

Georgescu, A. (2018). Pandora's Botnet – Cybercrime as a Persistent Systemic Threat. Future of Europe: Security and Privacy in Cyberspace. *The VISIO Journal*, *3*, 1-8.

Georgescu, A., Gheorghe, A. V., Piso, M.-I. & Katina, P. F. (2019). *Critical Space Infrastructures: Risk, Resilience and Complexity, Topics in Safety, Risk, Reliability and Quality*. Springer International Publishing. DOI: 10.1007/978-3-030-12604-9

Georgescu, A., Vevera, V. & Cirnu, C. E. (2020). The Diplomacy of Systemic Governance in Cyberspace. *International Journal of Cyber Diplomacy*, *1*(1), 79-88.

Gheorghe, A., Vamanu, D. V., Katina, P. & Pulfer, R. (2018). *Critical Infrastructures, Key Resources, Key Assets: Risk, Vulnerability, Resilience, Fragility, and Perception Governance, Topics in Safety, Risk, Reliability and Quality*. Springer International Publishing. DOI: 10.1007/978-3-319-69224-1

Gheorghe, A. V. & Schlapfer, M. (2006). Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures. In *2006 IEEE International Conference on Systems, Man and Cybernetics* (pp. 580–584). DOI: 10.1109/ICSMC.2006.384447

Helbing, D. (2013). Globally networked risks and how to respond. Nature, 497, 51–59. DOI: 10.1038/nature12047

Keating, C. B. & Katina, P. F. (2016). Complex system governance development: a first generation methodology. *International Journal of System of Systems Engineering*, 7, 43–74.

Moteff, J. D., Copeland, C. & Fischer, J. W. (2002). *Critical Infrastructures: What Makes an Infrastructure Critical?*. UNT Digital Library. Retrieved from: https://digital.library.unt.edu/ark:/67531/metacrs3176/

Pescaroli, G. & Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards*, *82*, 175–192. DOI: 10.1007/s11069-016-2186-3

Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*, 11–25. DOI: 10.1109/37.969131

Sousa-Poza, A. A., Kovacic, S. & Keating, C. B. (2008). System of systems engineering: An emerging multidiscipline. *International Journal of System-of-Systems Engineering*, *1*(1/2), 1–17.

Adrian Victor VEVERA

Is a Senior Researcher II, the General Director and a member of the Scientific Council of the National Institute for Research and Development in Informatics. Mr. Vevera holds a Ph.D. in military and information sciences, being both a lawyer and a nuclear physics engineer. He has extensive experience in the field of national security, fulfilling various positions, over time, in numerous managerial and counseling positions in different staterun organisations. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.