Cyber as a transformative element in the Critical Infrastructure Protection framework

Alexandru GEORGESCU, Adrian-Victor VEVERA, Carmen CÎRNU
National institute for Research and Development in Informatics - ICI Bucharest
alexandru.georgescu@ici.ro, victor.vevera@ici.ro, carmen.cirnu@ici.ro

Abstract: Critical Infrastructure Protection represents a comprehensive conceptual framework for the management of risks, vulnerabilities and threats arising from interconnected socio-technical systems termed infrastructures. Their criticality stems from the impact which disruption or destruction would have on a society or a region, whether through human and material losses, or of prestige and trust. Cyber has become an important factor in CIP, a crosscutting issue whose ascent has resulted in significant changes. This article argues that the penetration of cyber into almost every facet of human activity has resulted in fundamental structural changes, describes those changes in a systematized manner and theorizes what may happen to security governance under the new status quo.
Keywords: critical infrastructure protection, resilience, cyberspace, system-of-systems

INTRODUCTION

Critical Infrastructure Protection (CIP) was developed as a framework for explaining an increasingly complex world and managing the allocation of scarce resources towards security needs in an all-hazards approach that maximizes the ability of our societies to withstand harmful impacts and revert to normality (or an acceptable level of functioning) as quickly as possible *[Mureșan et al, 2016]*.

Infrastructure are socio-technical systems which are also critical if their disruption or destruction would cause significant loss of life, material damage and loss of prestige/ trust. They include pipelines, power plants, highways, financial markets and hospitals. CIP is also concerned with the development of methodologies to identify and designate critical infrastructure and the toolbox necessary to protect them from a complex security environment in which a large proportion of harmful effects stem from interconnections with other critical infrastructure systems. These systems-of-systems are extraordinarily complex and interdependent, and CIP offers the conceptual framework required to understand and describe, though not completely predict, the phenomena affecting these systems.

This article concerns itself with the systematization of the impact of cyber on critical infrastructures. Usually, terms such as the digitalization of services and other such formulas are used, but we shall introduce the term "cyberization" to describe a complex process wherein important elements of CI functioning are taken over by cyber capabilities relying on a physical and software substrate, resulting in fundamental changes to risk transmission, governance or normal, day-to-day functioning. We accept that the future may already have arrived in certain domains and countries, but not others, but contend that this process is inevitable under the impetus of mainly economic factors. The impact should be studied in depth through the lens of the latest developments in CIP theory, especially as they pertain to complexity and governance.

A NEW INFRASTRUCTURE DOMAIN

With the CIP framework appearing late on the scene of modernity (1997), when globalization and digitalization were already in full swing, we consider that an important shift in the theoretical demarcation of critical infrastructure domains was overlooked, which indicated important systemic shifts. One of the most important among these was the appearance of ITC infrastructure as a domain of its own in the CIP taxonomy, though its lines are blurring much faster than those of other domains due to factors which will also be explored in this paper.

In our estimation, the ICT infrastructure is formed, primarily, of the physical substrate of cyberspace (servers, routers and processing nodes), of the physical communication links (copper landlines, fiber optics, satellite uplinks and downlinks), of the software, operating systems, communication protocols and other intangible assets/resources which ensure system functionality and, finally, the governance structure which gives the system its coherence, such as the creators of new standards. The latter component is the most difficult to define since, through the haphazard and organic development of the cyber field, it has come to encompass not only traditional

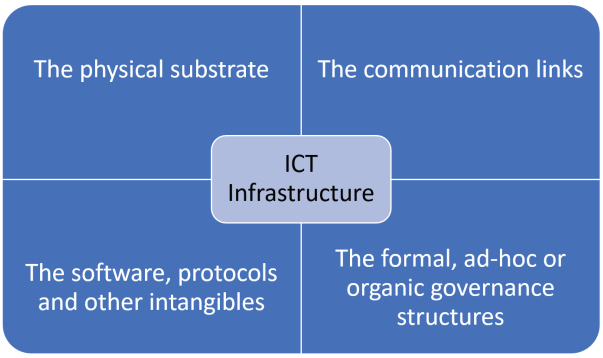

Fig. 1: *The ICT infrastructure main components [source: authors]*

regulatory entities, but also open-source software collectives, standardization groups, international institutions like the Internet Engineering Task Force and so on.

The borderless nature of cyber is an often remarked characteristic, but the mushrooming of cyber in the computing sense, followed by the establishment of networked communication, was done within the framework of states as territorial-administrative units and so the development of ICT infrastructure followed along similar lines that conform to the need for security and regulation. The advancement of globalization in business has led to an erosion in the relevance of borders both in the physical sense and in the cyber one, as data can be stored anywhere and accessed from anywhere. Dominant states like China try to maintain a form of "digital-territorial sovereignty" by using industrial policy to create national alternatives of major services and equipment providers to attain nominal ICT autonomy, and by using physical chokepoints in conjunction with organizational efforts to establish information control, but it is a continuous struggle to maintain this regime, and only China, by virtue of its size and resources, and the US (de facto, but not as intended policy), by virtue of its preexisting dominance, size and resources, can hope to achieve this

CYBER AS THE UPPER LAYER

Cyberization has had an impact in every critical infrastructure domain, in addition to developing its own. Whether we are discussing energy,

finance, industry or water supply, the process of cyberization has led to significant changes in the make-up of these critical infrastructures, how their components interact with each other, how they interact with the larger environment and the wider system-of-systems, but also what their governance processes look like.

In general, cyberization has resulted in a wholly digital command, coordination and integration function which ensures the harmonious\optimal functioning of systems and components. The process of data gathering, processing, secure transmission, visualization, response formulation, transmission and feedback loops for improvement have been cyberized. Cyber has become an upper control layer in every critical infrastructure system in advanced nations, and this has prompted the reorganization of operators and regulators, as well as the transformation of governance procedures *[Georgescu and Cirnu, 2019]*. Nowhere is this more obvious than in Supervisory Control and Data Acquisition (SCADA) and other industrial control systems, which utilize sensors, communication links, computer systems and control software applications to ensure the functioning, integrity and availability of a critical infrastructure *[Mehta and Reddy, 2015]*.

If we refer to Keating and Katina (2016) and their complex system governance theory, we may consider that the cyberization of critical infrastructures has resulted in a profound transformation of the critical infrastructure meta-system, which is the framework in which we may understand the CI being analyzed in terms of identity, system development, environmental surveillance and other critical meta-system functions on which system viability depends. Katina et al (2016) specifically analyze the application of complex system governance theories to cyber-physical systems which are exactly what most critical infrastructures have evolved towards being.

SYSTEMIC CHANGES

Drawing on Gheorghe and Schläpfer (2006), we find that there are a variety of types of interdependencies which define relationships between critical infrastructures. An interdependency is a bidirectional relationship in which changes in the status of one infrastructure will result in changes to another and vice versa. These interdependencies ranges from physical and geographical to logical and social/political. There are also the informational and cyber dependencies. The flow of information is necessary to any coordinated critical infrastructure system-of-systems. Before the advent of cyber, critical infrastructures (though not having a framework to be designated as such) would be dependent on information passed in a written medium or orally, through messengers. The digital era brought with it a coexistence between information and cyber, since pre-cyber transmission channels remained valid and were only sidelined slowly. However, we find that the rapid penetration of cyber in all walks of life under the three priorities of speed, efficiency and reliability have led, in advanced societies, to an almost complete replacement of informational interdependencies with cyber interdependencies, which have subsumed them. Information regarding events, prices, and intermediary readouts for equipment are now collected, processed, transmitted, received and interpreted digitally. The systemic consequences of this transformation, and the underlying cyberization of infrastructure command and control systems has led to interesting developments. Since resilience is a desired end state of CIP efforts, we break down these developments to detail them by using several of the seven attributes of resilience developed by Johnsen (2010) in reverse.

Firstly, we find that we have increased complexity. The advent of cyber and of networking through integrated webs rather than separate ones has led to an increase in the area of contact between a given system and the rest of the system-of-systems and of the environment. Linear increases in the number of agents lead to exponential increases in the number of connections and interactions. This complexity is also compounded by the growth of sources of data (especially through the Internet of Things), of data production and a corresponding need

to analyze it to support decision making processes. Complexity increased because the capabilities afforded by cyberization allowed systems to gain in complexity without a reduction in efficiency or a too great increase in "normal accidents" *[Perrow, 1999]*. Systems settle, *catteries paribus*, at a level of complexity which represents a stable equilibrium between performance and disruption risk, through an evolutionary process. In an environment of technological stagnation, the complexity level remains essentially unchanged for long periods of time, only to shift abruptly overnight in a period of technological ferment. However, the new levels may not represent equilibrium levels; rather, we are still undergoing a systemic transformation whose end state has yet to be reached in the absence of significant disruption whose only answer would be a reduction in complexity. So far, the cybercrime, hybrid warfare in the cyber realm, the accidents of complexity and the disruption in established economic and social patterns have not reached the level where growth in cyberization (and, therefore, in complexity) would be inhibited. The most optimistic among us view the process as essentially self-correcting and continuing indefinitely, albeit with periods of government-led and risk-induced slowdown.

Secondly, in our appreciation, cyber has become a key adjunct of the economic drive towards higher efficiency in the use of all resources. The result of this is not only economic efficiency and therefore growth, but also a corresponding reduction in the (frequently unintentional) margins of available capacity which systemic inefficiencies allow infrastructures to accumulate, with the positive effect of providing a buffer between systems in the propagation of disruptions and risks. Cyber became a new instrument of efficiency, which had a negative effect on resilience. For instance, just-in-time inventory management is only possible at global levels through cyber-mediated coordination mechanisms involving communications, satellite positioning and navigation, database harmonization and digital procurement and logistics tools. With the advent of this capability, logistical reliability increased and the added efficiency was spent on two things – greater decentralization of supply and production chains chasing after lower labor and input costs and lower requirement of costly on-hand stocks of intermediary products and raw materials to maintain optimal functioning of an infrastructure (whether a factory, a power plant or any other node in such a chain). However, this added efficiency reduced redundancies and heightened the impact of disruptions, when they did take place.

To this, we add the inherent potential of cyber as the medium of transmission for risks, vulnerabilities and threats. From a perspective derived from Johnsen (2010), this had the effect of tightening system couplings, which is the degree of delay between a system or system component shifting in state and the consequence being felt in another component of the system-of-systems. More tightly coupled systems fail faster and to a greater degree, with later warnings and less time to implement countermeasures and perform adaptations. The impact of cyberization on couplings can be mitigated through other methods to process delays, to generate flexible sequencing of processes, to employ flexible operating methods, have redundant capabilities, be flexible in the utilization of resources and be able to substitute for resources and systems should the need arise *[Perrow, 1999]*.

Some of the systemic developments mediated by cyberization have both positive and negative consequences from a security standpoint. For instance, system flexibility and adaptability may increase, as a system controller may have more than one mechanism or avenue to perform a system function, leading to diversity and an opportunity for improvisation and incremental improvement. New suppliers and supplies can be quickly identified and routed to the needed areas, meaning that local and regional crises are cushioned by the capabilities of the wider area, when coordinated through cyber.

Of course, this is not true for all systems. Rather, the most complex and important ones, like nuclear power plants and other high-level infrastructures governed by SCADA and industrial control systems are also the most rigid, because of the importance of maintaining system availability and integrity, which significantly limits what may be done for fear of disruption.

The changes we theorized above also lead to the conclusion that graceful and controlled decline of infrastructure functioning becomes much less likely in a cyber-mediated system-of-systems, thought this may be ameliorated through organizational competencies and other capabilities which can arrest the speed with which a cascading disruption is propagated within a system-of-systems. The most extreme example of a non-graceful decline is a disastrous disruption, involving not only an interruption in the provisioning of critical goods and services, but also a substantial degradation (explosion, meltdown, wipeout) of the underlying assets.

Quite possibly, the most positive overall example of systemic transformation which cyberization has brought with regards to governance is the steady development of common security cultures, mental modes and the diffusion of best practices, which have a positive impact on the security equation. This is due to the shrinking world of security professionals, the recurring concentration and consolidation of cyber-specific industries and a purposeful drive for regulatory coordination and harmonization. On the other hand, the risks associated with global infrastructure networks and globally networked infrastructures enabled by cyberization also created a corresponding need for this development which cyberization then facilitated.

Lastly, the rise in complexity which was fostered by cyberization results in the five consequences presented in ***Figure 2***, which are the attributes of complex systems that governance processes must be configured to handle.

In the context of ***Figure 2***, the properties may be defined as follows *[Keating et al, 2014]*:

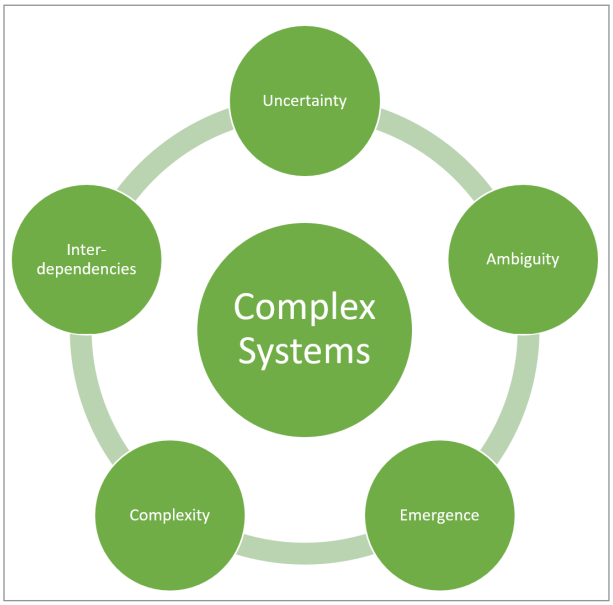

Fig. 2*: Attributes of complex systems [Keating et al, 2014]*

• Uncertainty – incomplete knowledge results in doubts regarding decisions, actions and consequences;

• Ambiguity – a lack of clarity in the overall systems;

• Emergence represents the unexpected and unanticipated properties and phenomena emerging from the interaction between system components and system components and their environment;

• Complexity – the system-of-systems and its interdependencies have become so vast that knowing them, understanding them, predicting them and explaining them becomes next to impossible;

• Reciprocal influences across major vectors where the state of one component influences that of another.

TRANSFORMATIONS IN THE SECURITY ENVIRONMENT

The prior sections have, inadvertently, detailed transformations of a security nature which we will not restate, resulting from systemic transformations within the systems.

If we return to complex systems theory, as defined by Keating et al (2015), we may extract two categories of challenges to the governance of these systems and link them directly to cyber.

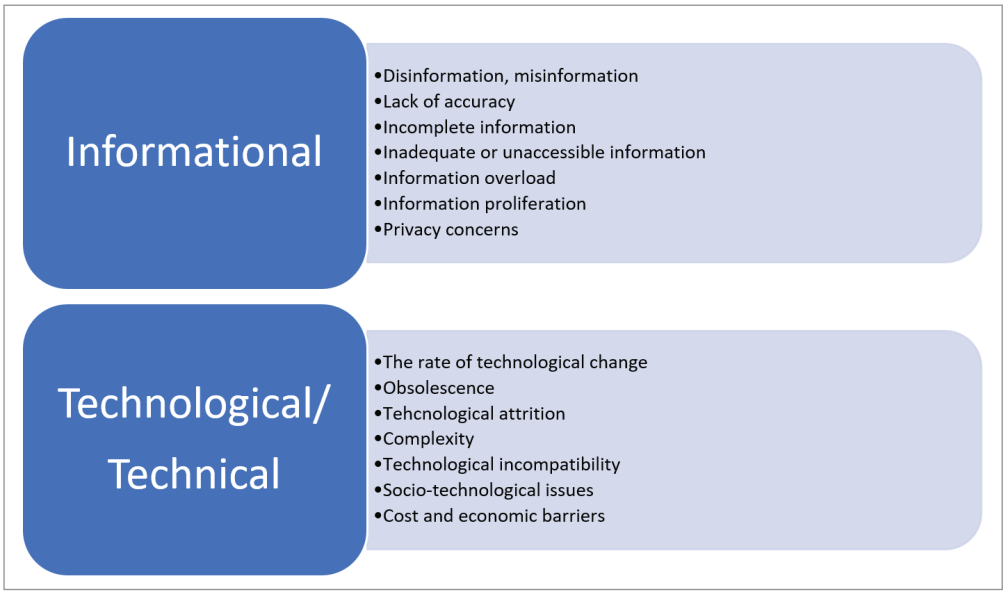

***Fig.3**: Challenges to complex system governance from a technological and informational perspective [Keating et al, 2015]*

However, the security environment has been systematically transformed by the penetration of cyber into every facet of activity, from physical production to transport and safety and security processes. In this context, cyberspace has become the ultimate (and preferred) medium for the transmission of risks, vulnerabilities and threats. In addition to the possibility of cascading disruptions triggered by "normal accidents" *[Perrow, 1999]*, that is phenomena triggered by complexity and component interactions, we have also the advent of deliberate threats. Georgescu (2018) detailed the aspect of cybercrime, and the main aspects that accompany the extraction of value:

- The subversion of institutions and organizations;
- The disruption of activity;
- The deterritorialization of crime;
- The confounding of jurisdictions.

In addition, since the cyber environment is continuously changing, we are witnessing also transformative trends in cybercrime *[Cyber security Ventures, 2020]:*

- The commoditization of malware;
- The professionalization of cybercrime;
- New forms of cybercrime such as ransom ware;
- The turn towards mobile devices and the devices associated with the Internet of Things;
- The vulnerabilities stemming from commercial-off-the-shelf hardware and software;
- The ubiquity of cybercrime.

Some cyber attackers are not pursuing profit. They are agents seeking to utilize coercion through deniable attacks in order to achieve a strategic or political goal. Cyberspace has become a battleground for states seeking to utilize hybrid warfare techniques, tactics and procedures to pursue goals in a way which leaves them with plausible deniability, avoids the use of regular forces and relies on actions below the threshold of armed response or the trigger for collective defense. As Gherasimov (2013) states, the lines between war and peace are being blurred and wars are no longer being declared or even fought in accordance with established models. At the same time, "the very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness" *[Gherasimov, 2013]*. Reichborn-Kjennerud and Cullen (2016) describe hybrid warfare as a conflict which „is characterized by the appropriate use of all power tools on the vulnerabilities of the opponent". Cyber is increasingly part of the toolbox of the novel forms of war, as they deliver not only the advantages mentioned above, but also the prospect of a good cost\benefit ratio, a low barrier to entry in such activities and synergies with other activities, such as cybercrime, terrorism, data theft and others, which may support a wider strategy of confrontation.

In addition to these issues, another one stems from the CIP perspective – the fact that private companies own and operate 70-80% of critical infrastructures in the West. More and more, as they become acceptable targets of hybrid cyber-attacks, they will have to defend themselves first, before other actors become involved to ameliorate the security situation, investigate and compose a plan of action. Therefore, in the security environment that cyber is helping to create, a whole new form of security culture is being developed and instilled in organizations faced with significant losses or even worse consequences from the manifestation of the cyber threat *[Carpenter and Wyman, 2018]*. This security culture is not only for employees, but also for leadership and how they interact with other stakeholders, including the critical infrastructure protection coordination authorities.

CONCLUSION

Our societies rely for their prosperity, capability and security on the proper functioning of critical infrastructures. The advent of cyber and of the process we termed as "cyberization" has led to a remodeling of the critical infrastructure system-of-systems and of the security environment, through effects on command, coordination, integration, data gathering and decision making, as well as on the incentives of possible attackers.

These transformations have had a tremendous impact on the governance process of critical infrastructures, since they have created both new tools and efficiencies, as well as larger contact surfaces with hostile actors and new vectors for the transmission of risks, vulnerabilities and threats. On this basis, we can say that future governance, as it related to the cyber aspects of CIP theory, will be a more and more hierarchical process, in which traditional regulators will be caught between the operational level of the owners\operators of critical infrastructure and the international level, where diplomacy and "collaborative competition" will create a framework of standards and practices which will become the norm in the domain. More and more, the growth of our dependence on cyber will outstrip our capacity to resolve security issues stemming both from exposure and from dependence. At the same time, while resilience to locally disruptive phenomena may be increased through greater interconnectivity with other regions which provide redundancies and flexibility, it is quite possible that a global systemic issue will cause significant cascading disruptions and incalculable consequences. We consider that, more and more, as we approach a period of temporary maximum in awareness of the security environment, we will see companies, governments and individuals trying to manage exposure to cyber risk through simplification and complexity reduction in pursuit of resilience, even if it means foregoing some of the momentary efficiencies of open networks, transparent system architectures, avoiding proprietary hardware and software and so on.

REFERENCE LIST

Carpenter, G., Wyman, O. (2017), MMC CYBER HANDBOOK 2018 – Perspectives on the next wave of cyber, Marsh & McLennan,https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf

Cyber security Ventures (2020). 2020 Cybercrime Report. Herjavec Group, https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

Georgescu, A. (2018) Pandora's Botnet – Cybercrime as a Persistent Systemic Threat. Future of Europe: Security and Privacy in Cyberspace, Visio Journal No. 3, Dec. 2018, Visio Institut, ISBN: 2536-1481-3

Georgescu, A., Cirnu, C.E. (2019). Blockchain and critical infrastructures – challenges and opportunities, in Romanian Cyber Security Journal, ISSN 2668-1730, ISSN-L 2668-1730, vol. 1 (1), 93-100

Gheorghe, A., Schläpfer, M. (2006) Critical Infrastructures: Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures, Systems Man and Cybernetics 2006. SMC '06. IEEE International Conference, vol. 1, p. 580-584

Gherasimov, V. (2013) The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations (Ţennost nauki v predvidenii), Military-Industrial Kurier, (Voenno-Promîşlennîi Kurier), nr.8 (476), p. 3, February 27, 2013, https://jmc.msu.edu/50th/download/21-conflict.pdf

Johnsen, S. (2010) Resilience in risk analysis and risk assessment. In Moore, T., Shenoi, S. (eds). Critical Infrastructure Protection IV - Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. IFIP Advances in Information and Communication Technology series (311), p. 215-227. Washington DC, USA: Springer, ISBN 978-3-642-16806-2

Katina, P.F., Keating, C.B., Gheorghe, A.V. (2016) Cyber-Physical Systems: Complex System Governance as an Integrating Construct. Proceedings of the 2016 Industrial and Systems Engineering Research Conference. Anaheim, California, US, https://www.researchgate.net/publication/307539626_Cyber-Physical_Systems_Complex_System_Governance_as_an_Integrating_Construct

Keating, C. B., & Katina, P. F. (2016) Complex system governance development: A first generation methodology. International Journal of System of Systems Engineering, 7(1/2/3),43-74

Keating, C. B., Katina, P. F., & Bradley, J. M. (2014). Complex system governance: concept, challenges, and emerging research. International Journal of System of Systems Engineering, 5(3), 263–288

Keating, C., Katina, P. and Bradley, J. (2015) Challenges for Developing Complex System Governance. Proceeding of IIE Annual Conference. p. 2943-2952

Mehta, B., Reddy, Y. (2015) SCADA systems, in Industrial Process Automation Systems, Elsevier, pp. 237–300. doi: 10.1016/B978-0-12-800939-0.00007-3

Mureşan, L., Georgescu, A., Jivănescu, I., Popa, Ş, Arseni, Ş.C. (2016) Charting Critical Energy Infrastructure Dependencies on Space Systems – New Frontiers in Risks, Vulnerabilities and Threats. In Caşın, M. H.

Gluschke, G. (eds.) (2016) Critical Energy Infrastructure Protection and Cyber Security Policies", Hazar Strateji Enstitüsü, ISBN 978-605-83541-4-2, Istanbul, Turkey, 2016

Perrow, C. (1999) Normal Accidents: Living with High-Risk Technologies. Princeton University Press, ISBN: 9781400828494

Reichborn-Kjennerud, E., Cullen, P. (2016) What is Hybrid Warfare? Norwegian Institute for International Affairs, Policy Brief 1/2016, p.3