THE DIGITALIZATION OF CRITICAL INFRASTRUCTURES – SYSTEMIC CONSIDERATIONS, EVOLUTIONS OF GOVERNANCE AND ELEMENTS OF A NATIONAL RESEARCH AGENDA –

Adrian Victor VEVERA, BEng, PhD
General Director, National Institute for Research and Development in Informatics-ICI, Bucharest

10.55535/RMT.2024.3.6

The rapid digitalization of all aspects of economic, social, and political life in advanced societies has produced new risks, vulnerabilities, and threats. Rapid technological change is generating new systemic trends related to digitalization. This article presents the main arguments in favour of this view and attempts to delineate the main transformations that will take place, while emphasizing their impact on societal security, including at the level of defence. It does so through the critical infrastructure protection framework, which provides a system-of-systems perspective uniquely suited to the analysis of complex systems and processes.

Keywords: digitalization; resilience; critical infrastructures; emerging technologies; system-of-systems;

INTRODUCTION

Digitalization is a quantitative and qualitative process through which digital technology becomes embedded into key social, economic, and political processes[1]. Based on the revolution in connectivity and computing power, whereby more data transfer capacity and more computing power are made available at lower prices to greater numbers of users, digitalization has changed the face of all societies, including developing ones. This article presents a transversal analysis of the cyber domain using the framework of Critical Infrastructure Protection (CIP). Utilizing this framework provides us with key concepts and terminologies to use a system-of-systems approach in analysing the systemic impact of digitalization, the changes in the cybersecurity environment, and the changes in governance processes. The article ends with a non-exhaustive list of recommendations for priority research and development areas for Romania.

DIGITALIZATION AND CIP THEORY

CIP theory relies on the concept of Critical Infrastructures (CI), which are socio-technical systems made up of assets, resources, components, and organizations working together to produce critical goods and services. Their criticality stems from the fact that, according to legislated methodologies for identification and designation of CIs, their disruption or destruction would cause significant loss of human life, material damage and loss of confidence on the part of citizens, investors, partners and allies, among other effects. CIP enables us to develop a systemic view of the functioning of advanced societies, both internally and cross-border, or even at global levels, in order to manage the risks, vulnerabilities and threats that global infrastructure connectivity,

CIs criticality stems from the fact that, according to legislated methodologies for identification and designation of CIs, their disruption or destruction would cause significant loss of human life, material damage and loss of confidence on the part of citizens, investors, partners and allies, among other effects.

[1] Note: This article summarizes the main theoretical conclusions of the book *A Transversal Analysis of the Cyber Domain in Critical Infrastructure Protection*, Vevera, A-V (2022). București: Editura Militară.

natural disasters and deliberate actions on the part of malignant or criminal actors have generated. CIs are often interdependent, whereby changes in one infrastructure generate changes in another, based on a geographical, logical, physical, or informational relationship. Thus, they are often affected by disruptions stemming from common causes, which lead to aggravated and prolonged crises, and they can even experience cascading disruptions, where a chain of interdependent infrastructures is disrupted in sequence. (Bucovețchi, Simion, 2015).

Digitalization is a leading factor in the greater coordination and integration of critical infrastructure, beyond national borders and even at global level. Digital systems provide command, control, coordination, and data gathering capabilities that enable the safe and predictable operation of critical infrastructures across vast geographic distances, requiring various components, which are sometimes infrastructures in themselves, to work in unison to achieve productivity, reliability, affordability and safety.

Digitalization is a leading factor in the greater coordination and integration of critical infrastructure, beyond national borders and even at global level. Digital systems provide command, control, coordination, and data gathering capabilities that enable the safe and predictable operation of critical infrastructures across vast geographic distances, requiring various components, which are sometimes infrastructures in themselves, to work in unison to achieve productivity, reliability, affordability and safety. For CIs, digitalization does not mean just communication and databases, as it does for most users, but also the emergence of cyber-physical systems that rely on digital mechanisms to interpret signals from the physical world and to give commands to systems, which create an effect in the physical world. The industrial control systems (ICS) as well as supervisory control and data acquisition systems (SCADA), which have become central to the operation of many CIs across different sectors, are all the result of digitalization and networking.

Thus, critical infrastructures are exposed to various risks and threats, such as those posed by hackers. At the same time, decision-makers and policymakers in the field of security governance have to protect these systems and increase their resilience, which is their capacity to prevent an accident or thwart attacks and, if they happen anyway, to minimize damage and disruption times and to resume as soon as possible a minimum acceptable level of functioning, while extracting lessons learned. However, the rapid advances in digital technology and the continuing rise of digitalization are changing key paradigms, and stakeholders must rapidly adapt to the new security environment and the new evolution of the critical infrastructures.

SYSTEMIC TRANSFORMATIONS IN THE CYBER FIELD

The phenomenon of digitalization has led to obvious changes in how we work, shop, educate ourselves or interact. For better or worse, they are reshaping human relationships and societies. This is a systemic effect. When seen from a Critical Infrastructure Protection framework, digitalization also has a systemic effect and it, too, has both positive and negative effects.

We are undergoing a process of acceding to a new paradigm of digitalization, characterized by the following features:

- It is based on ubiquitous computing and connectivity between system components;
- There will be no more dumb or non-networked systems, except by intentional design and at the cost of efficiency and usability;
- It is integrating new technologies, especially emerging technologies such as AI, blockchain, quantum computing;
- It is generating new risks, vulnerabilities and threats, as well as accentuating the lack of predictability of the resulting system and the mismatch between the systems whose security needs to be governed and the governance system, which is based on territorialized understandings of jurisdiction and action.

The negative consequences of new technologies and the patterns of interaction and activity they generate can be profound. The most visible examples are those resulting from deliberate human action, for manipulative, disruptive or destructive purposes, both for profit (organized crime) and for political, social, and ideological purposes (cyber terrorism, hacktivism etc.).

The negative consequences of new technologies and the patterns of interaction and activity they generate can be profound. The most visible examples are those resulting from deliberate human action, for manipulative, disruptive or destructive purposes, both for profit (organized crime) and for political, social, and ideological purposes (cyber terrorism, hacktivism etc.).

There are significant categories of consequences that do not come from human deliberation or decision, but result from the interaction between various systems, sub-systems, and their environment, which generates unpredictable, emergent, and uncertain effects, phenomena and behaviours. The intersection of natural phenomena and deliberate threats produces new patterns of disruption or degradation of CI. It affects not just cyber infrastructure, but every CI that relies on digital systems for command, control, and coordination.

We can identify four main systemic transformations.

The Revolution of Scope and Scale

Digitalization revolutionizes the scope and the scale of critical infrastructures acting within a wider system-of-systems by enabling better control and coordination among large or dispersed assets or within production and supply chains. This phenomenon has been taking place ever since the revolution in communications represented by the telegraph. The digital and connectivity era has enabled higher volumes of information and greater automation in systems, which has made CI systems-of-systems truly global not just in their impact, but also in their degree of control and coordination. *Figure 1* shows the degree to which EU Member States have digitalized, expressed through the *Digital Economy and Society Index.*

Digitalization revolutionizes the scope and the scale of critical infrastructures acting within a wider system-of-systems by enabling better control and coordination among large or dispersed assets or within production and supply chains.

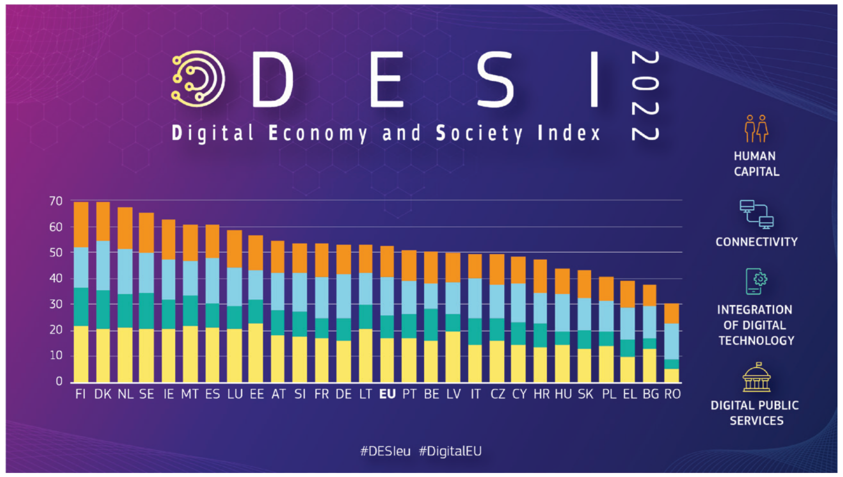


Figure 1: Digital Economy and Society Index 2022
(European Commission, 2023, https://digital-strategy.ec.europa.eu/en/policies/desi)

The Transition from Proprietary Systems to Commercial-Off-The-Shelf (COTS) Systems

Many of the most sensitive and function specific critical infrastructures require specific assets, hardware and software, in order to operate. Their initial digitalization in the form of industrial control systems was done through bespoke hardware and software, developed internally or tailor-made by an external contractor, often working in obscure programming languages. Gradually, the growth of digitalization created a digital mass of services and other capabilities which could be adaptable to various needs in order to provide the scale required for economic efficiency and high investment in research and development. Concentration effects in technological ecosystems, where a series of solutions and standards could win over others, also took place. What that means is that Critical Entities or Critical Infrastructure Operators no longer need bespoke systems and are actually better off not trying to develop them. They can buy hardware and software from the mass market, at better prices, with better performance, with better lifetime cost and upgrades and with better security in other ways, including time for repairs and maintenance, vulnerability to various hazards and so on. Even if an entity develops a bespoke system, that system will likely still use some components, such as sensors, coming from specialized producers, which supply the rest of the market, or software that uses open-source libraries or a particular operating system. Their own vendors are also dependent on commercial supply chains and are themselves suppliers for a wider array of actors. (Nazir et al., 2017; Mehta, Reddy, 2015). It translates into a reduction in security through obscurity, the quality of being harder to hack or disrupt because most potential attackers lack specific knowledge about your systems, your programming language, your software etc. Most attackers of such systems are either highly specialized entities with state backing or internal threat actors. On the other end of the scale, the emerging paradigm sees CI operators relying on complex systems made up of commercial-off-the-shelf hardware, software, public communication links (the Internet) and other generic solutions. We are not just discussing Enterprise Resource Management solutions such as SAP or office software suites for organizations, but also the industrial control systems themselves. It means that a hacker can use the same set of general knowledge to effectively attack (though maybe not with ideal performance as that given by specific knowledge) any system, whether it is a thermal power plant, a data centre, a waste treatment facility, a logistics company, or a large retailer.

The growth of digitalization created a digital mass of services and other capabilities which could be adaptable to various needs in order to provide the scale required for economic efficiency and high investment in research and development. Concentration effects in technological ecosystems, where a series of solutions and standards could win over others, also took place.

The process is still ongoing, with new horizons for COTS paradigms, such as satellites running on Android mobile operating software, or facilities retooled under an Internet-of-Things paradigm, full of wireless sensors and access nodes, including for non-essential functions such as office lights, centralized heating-ventilation-air-conditioning systems and other systems that are unpatched or unpatchable across the product lifetime and can provide access points into company networks for enterprising hackers. That is is also why supply chain attacks have grown so much in recent years, as well as attacks through unreported backdoors, vulnerabilities and zero-day exploits.

Infrastructure Reorganization

Digitalization is enabling the reorganization of critical infrastructures to take advantage of the new possibilities offered by connectivity, computing, high levels of data transfers and automation. This reorganization can take place at physical level, at cyber level, at economic level and at organizational level, and can result in new infrastructure typologies that generate new risks, vulnerabilities and threats. The process is ongoing, because of the gradual nature of digitalization and the adoption of new technologies, which depend not just on technological levels, but also on economic incentives such as competition, on capital expenditure requirements, on appetite for risk and on general market evolution.

Digitalization is enabling the reorganization of critical infrastructures to take advantage of the new possibilities offered by connectivity, computing, high levels of data transfers and automation. This reorganization can take place at physical level, at cyber level, at economic level and at organizational level, and can result in new infrastructure typologies that generate new risks, vulnerabilities and threats.

The best example of a strong reorganization effect has been the trend in recent decades for production offshoring and outsourcing, which has led to globally fragmented production and supply chains kept functioning by just-in-time logistical systems first pioneered by Japanese companies. It enabled entities to move production where labour and other input costs were lower. It resulted in decentralized production chains, even within the same company, requiring global coordination mechanisms that were managed digitally. The security costs of that model were seen in the growing exposure to cyber attacks, but also in supply issues when events like conflicts or the 2020 pandemic interrupted cross-border transport.

A more recent example of reorganization is the rise of cloud computing, whereby distributed computing systems (each worker with own desktop, laptop, with processor, memory, or each company with its own servers) were replaced by work stations that depended on centralized computing and memory. It enabled lower costs, more rapid scaling of services for growth, more flexible allocation of resources (you pay for the computing power used without capital expenditure in your own systems), easier upgrade and replacement and better security (since systems could be professionally run, administered or replaced). However, it is creating a single point of failure for the entire enterprise (in the case of a dedicated company cloud) or for an entire ecosystem of entities relying on a very big cloud services provider (the marketing being concentrated among three great actors – Microsoft, Google, Amazon). Even when trying to avoid this development, many services that are used by an entity might have cloud processes running in the background, so there is an indirect risk.

Extreme examples of reorganization have led industrial aerospace giants like Boeing or tech giants like Apple to become technology integrators, performing research and handling marketing, finance and other functions, while outsourcing and offshoring most the actual production chain to other actors.

Infrastructure Virtualization

One particular form of reorganization of CI is the virtualization of the CI, in which critical elements of differentiation between specific CI processes are moved from the physical space into the virtual one, where it becomes very difficult to delineate between one process or another and between one infrastructure or another, especially when it comes to cyber infrastructures or their components. We can no longer pinpoint a particular physical asset involved in a process. It has numerous implications for various aspects of CI functioning, such as single point failures, common cause failures, escalating failures, cascading failures and more. The consequences are profound, from a security governance perspective, since it makes CI much more malleable and therefore harder to adequately map, interpret, explain and predict. Key processes are transformed into specific software running on generic hardware which is delocalized. The previously mentioned cloud infrastructure is one such example, but we may also include here various elements of the 5G communications infrastructure,

One particular form of reorganization of CI is the virtualization of the CI, in which critical elements of differentiation between specific CI processes are moved from the physical space into the virtual one, where it becomes very difficult to delineate between one process or another and between one infrastructure or another, especially when it comes to cyber infrastructures or their components.

which is what raised the spectrum of security issues related to the Chinese vendor ecosystem for 5G solutions, since core and periphery elements of the 5G infrastructure could no longer be separated to reduce security risks. A simple example is a company or a department inside a company providing critical coordination services for industrial manufacturing processes, for market operations or for logistics. Once, it would have had its own data centre with physicalized infrastructure that it could shut off, physically disconnect, replace or segment. Then, it started leasing this infrastructure from a particular company, which provided it with its own dedicated facility or sector of a facility. Afterwards, the solution vendor moved the company's processes onto much larger and more efficient servers, which it segmented virtually into dedicated space or *"devices"* for that company's operation. Lastly, the infrastructure became completely virtualized, running on a virtual infrastructure made up of hundreds of data centres, being everywhere and nowhere all at once so that no amount of maintenance or power outages would require planning the continuity of service, given that the infrastructure reorients itself automatically around non-functioning elements. It has great advantages from a cost and safety perspective, but also increases the risks associated with a successful cyber attack or another phenomenon (electromagnetic pulse) targeting the infrastructure itself.

The virtualization of infrastructure leads to new paradigm shifts, such as: IaaS – Infrastructure as a Service; SaaS – Software as a Service; PaaS – Platform as a Service.

The client has very little say over the day-to-day management of that infrastructure – its maintenance cycles, its communication technology, its upgrades, its cybersecurity measures etc.

The virtualization of infrastructure leads to new paradigm shifts, such as:

- IaaS – Infrastructure as a Service – in which a competing cloud provider offers distributed computing services;
- SaaS – Software as a Service – in which cloud computing is used for software distribution;
- PaaS – Platform as a Service – where the cloud computing provider provides the platform for building new applications by developers, who then find customers for a specific service running on a generic platform.

Blockchain technology enables an even greater decentralization and unbundling of critical organizational functions for critical infrastructures. The ability to have smart contracts run automatically rather than depend on a third party such as a bank or a dedicated department for assurance will lead to even more virtualized infrastructures.

EVOLUTION OF THE CYBERSECURITY ENVIRONMENT

The cybersecurity environment is undergoing rapid change due to technological development and a greater permeation of economic, social and political life, especially after the smartphone revolution. While certain aspects of this change are unknowable, given the uncertainties regarding rates of technological adoption and the speed of new breakthroughs, we can safely assume that the cybersecurity environment is dynamic, multifaceted and challenging. A thorough analysis of the scientific literature and especially the industry reports that keep track of the changing security priorities can let us aggregate various information into a series of key trends, summarized in *table 1.*

Blockchain technology enables an even greater decentralization and unbundling of critical organizational functions for critical infrastructures.

Table 1: Trends in the cybersecurity environment (Vevera, 2022)

Trend	Explanation
Increased surface area for contact	Various technological and economic trends have increased the contact surface between the real world and the cyber world, as well as between the systems that need to be secured and a chaotic and dangerous cyber security environment. The contact surface metaphor expresses the increase in deliberate as well as accidental interactions, and the proliferation of attack opportunities, especially through the exploitation of unknown vulnerabilities and access paths by defenders.

Trend	Explanation
The variety of actors involved	The actors who deliberately attack critical infrastructures are varied and changing. Among them, we list: • Cross-border criminal organizations; • Lone wolves; • Non-state groups driven by ideology; • Rebellious states (rogue); • Groups sponsored by states; • The enemy within the organization; • Combinations of them.
The complexity of motivations	Some actors seek profit, others wish to apply coercive measures to change the behaviour of the state or targeted actors, and others act out of ideology. Frozen conflicts between states are another contributor to such motivations. It should be noted, however, that many actors have mixed motivations, and a trend noted by O'Gorman et al. (2019) refers to the increasing profit motivations of state-supported actors.
The commodification of malware	The traditional model is one where the attacker develops its own means of attack and the skills to use them, which naturally limits the number of attackers and attacks. Today, however, especially through the anonymity promoted by cryptocurrencies, malware has been commodified so that malware production and even its use can be outsourced. An aspiring attacker can buy a particular application and use it to accomplish their goals with a tool that is likely much better than what they could have developed on their own. The proliferation of cyber weapons following their loss by intelligence agencies contributes to this phenomenon.

The cybersecurity environment is undergoing rapid change due to technological development and a greater permeation of economic, social and political life, especially after the smartphone revolution.

Trend	Explanation
Cyber criminals are mirroring legitimate business practices	The trend was noted by Fortinet (2013), being a development of the phenomenon detailed before. Developed markets are emerging to facilitate the division of labour in cyber attacks. Bidders adopt legitimate business techniques and compete with each other to attract customers. A customer may purchase specific malware or information related to vulnerabilities; can rent virtual machines and computers with pre-existing malware infections for a DDoS attack; can acquire passwords and bank data in large quantities, hoping to be able to embezzle funds and so on.
Unequal rates of advancement	The cyberspace is advancing faster than the security culture of users or the governance capacity of authorities and large companies, which increases the opportunities for enterprising criminals.
The link between cybercrime and cyberterrorism	Terrorism and cross-border organized crime are closely linked. First, the terrorist is often a cybercriminal himself in order to finance himself, obtain information about the target, and coordinate with other entities. Second, organized crime provides a market for goods and services for terrorists – cyber weapons and the ability to purchase specific services, including information and vulnerabilities, but also the destructive effect that organized crime and corruption have on targeted organizations.
Technological evolution	The emergence of blockchain-based ransomware and, more recently, the replacement of Trojan worms with ransomware as contagious malware. The field is dynamic and innovative, where new ideas spread quickly and are reflected in the level of new threats.

The cyberspace is advancing faster than the security culture of users or the governance capacity of authorities and large companies, which increases the opportunities for enterprising criminals.

Trend	Explanation
Systemic fragility	Field-wide technological developments have encouraged systemic changes, some detailed in the previous section, that have increased the vulnerability of critical infrastructures to accidental and deliberate threats. There are many more opportunities to disrupt the good functioning of a system, and systemic transformations have reduced system-wide resilience, robustness, adaptability, redundancy and other attributes of resilience.

The cybersecurity environment is registering an increase in malignant activities due to a lack of a proper global cybersecurity architecture and framework, coupled with the high potential gains, both financial and strategic, from engaging in such activities.

We can be quite certain that the cybersecurity environment is registering an increase in malignant activities due to a lack of a proper global cybersecurity architecture and framework, coupled with the high potential gains, both financial and strategic, from engaging in such activities. In line with the increase in the surface contact area between critical infrastructures, the Internet and networked systems in general, we can assert that the frequency and severity of attacks and infiltrations are growing. Because of the cyber-physical system paradigm, the cyber attacks are also having more and more impact in the physical world, especially when it comes to critical goods and services or the critical coordination necessary for avoiding disastrous effects in the physical world from disturbances in the functioning parameters of critical infrastructures.

TRANSVERSAL APPROACHES

We have picked two transversal approaches to the issue of digitalization seen through a CIP lens. The first is the analysis of the European framework for cyber issues, seen in a wider sense, encompassing both legislation and institutions. The second is sketching a national agenda for targeted developments in cyber issues in order to deal with the impact of digitalization.

The European Framework for Handling Systemic Digitalization

Starting with the first Green Book on Critical Infrastructure Protection in 2004 and reaching fruition with Directive 114/2008 on the Identification and Designation of Critical Infrastructures, the European Union has developed a comprehensive framework for CIP under the European Programme for Critical Infrastructure Protection (EPCIP). The Programme differs from the US version through the politically necessary distinction between the EU and Member States, entailing a distinction between national CIs and European CIs. Member States are responsible for both, but EPCIP has a special role in administering European CIs, whose disruption or destruction would affect two or more Member States. Under the latest EU Critical Infrastructure Blueprint, a new category of ECIs has been defined, affecting six or more Member States. This stronger form of subsidiarity is a political necessity and creates important challenges, which the multilateral framework strives to overcome.

Starting with the first Green Book on Critical Infrastructure Protection in 2004 and reaching fruition with Directive 114/2008 on the Identification and Designation of Critical Infrastructures, the European Union has developed a comprehensive framework for CIP under the European Programme for Critical Infrastructure Protection.

Cyber is an important part of EPCIP and associated efforts, and the European governance regime for systemic issues has been enhanced over time with a *European Cybersecurity Strategy*, the *Network and Information Security Directive (NIS)* and a host of other documents of reference. The governance regime has both legislative and institutional components. *Figure 2* represents an attempt to map the institutionalized European framework for cybersecurity, both legislatively, strategically, operationally, and from a research and innovation perspective.

From a legislative perspective, we have chosen to highlight a particularly important recent development – the 2023 political approval of the *Critical Entities Resilience Directive (CER)* and the *NIS 2 Directive*, with planned transposal into Member State legislation by October 2024, though it seems optimistic, given the breadth of changes they introduce.

The two Directives maintain continuity with EPCIP, but introduce major systemic changes that are the result of the lessons learned from the pandemic and from the war in Ukraine, in terms of the true interconnectivity between the CIs of Member States at European level, both within sectors and across different sectors. The most important feature from the perspective of our analysis is that the cyber

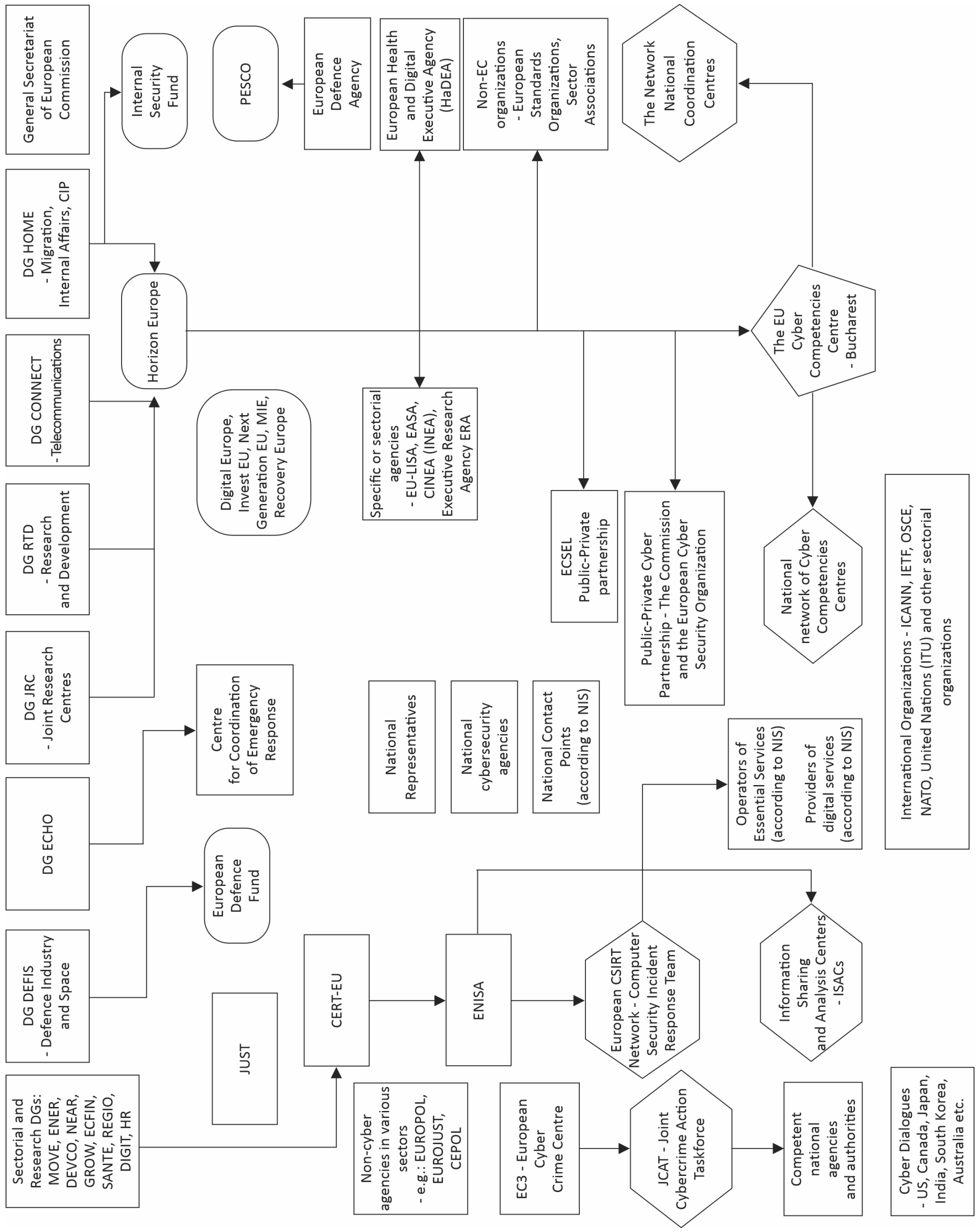
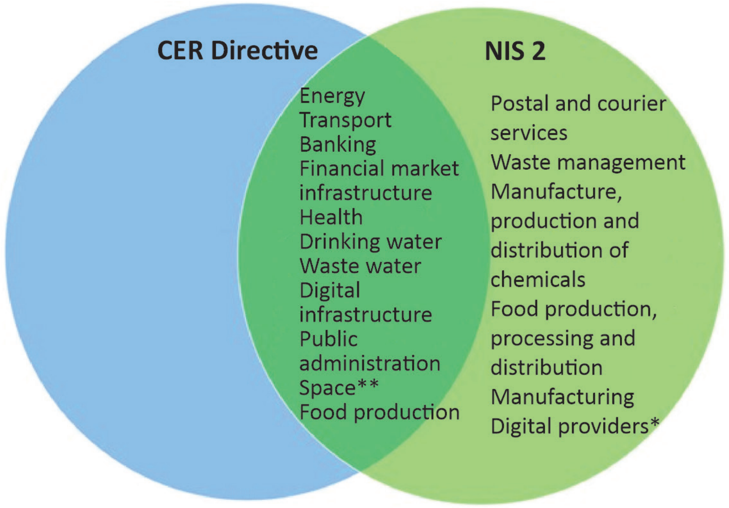

General Secretariat of European Commission
DG HOME - Migration, Internal Affairs, CIP
DG CONNECT - Telecommunications
DG RTD - Research and Development
DG JRC - Joint Research Centres
DG ECHO
DG DEFIS - Defence Industry and Space
Sectorial and Research DGs: MOVE, ENER, DEVCO, NEAR, GROW, ECFIN, SANTE, REGIO, DIGIT, HR
Internal Security Fund
Horizon Europe
PESCO
Digital Europe, Invest EU, Next Generation EU, MIE, Recovery Europe
Centre for Coordination of Emergency Response
European Defence Fund
JUST
European Defence Agency
European Health and Digital Executive Agency (HaDEA)
Specific or sectorial agencies - EU-LISA, EASA, CINEA (INEA), Executive Research Agency ERA
Non-EC organizations - European Standards Organizations, Sector Associations
The Network National Coordination Centres
The EU Cyber Competencies Centre - Bucharest
ECSEL Public-Private partnership
Public-Private Cyber Partnership - The Commission and the European Cyber Security Organization
National network of Cyber Competencies Centres
International Organizations - ICANN, IETF, OSCE, NATO, United Nations (ITU) and other sectorial organizations
National Representatives
National cybersecurity agencies
National Contact Points (according to NIS)
Operators of Essential Services (according to NIS)
Providers of digital services (according to NIS)
CERT-EU
ENISA
European CSIRT Network - Computer Security Incident Response Team
Information Sharing and Analysis Centers - ISACs
Non-cyber agencies in various sectors - e.g.: EUROPOL, EUROJUST, CEPOL
EC3 - European Cyber Crime Centre
JCAT - Joint Cybercrime Action Taskforce
Competent national agencies and authorities
Cyber Dialogues - US, Canada, Japan, India, South Korea, Australia etc.

Figure 2: Map of European cybersecurity governance (Ib.)

dimension now permeates all the CIP governance framework, through the fact that the taxonomies of essential/critical/important systems identified by the two Directives now overlap almost completely. Every CI in the CER Directive is also present in the NIS 2 Directive, while the NIS 2 Directive also creates an additional category for less than critical systems such as postal services. *Figure 3* presents this overlap.

The cyber dimension now permeates all the CIP governance framework, through the fact that the taxonomies of essential/ critical/ important systems identified by the two Directives now overlap almost completely.



* 'Important entities' under NIS2
** 'Essential enitities' under NIS2 and 'critical entities' upon identification under the CER Directive

Figure 3: Overlap between CER Directive and NIS 2
(Georgescu, Bucovețchi, 2023)

We see the following main changes:

- The adoption of the term *"entity"* from the NIS methodology as the building block of EPCIP efforts, replacing almost entirely the concept of critical infrastructure *owner/operator/administrator*. It leads to a more expansive definition of CIs, which also encompasses aspects related to the organization that owns and runs it, including also financial and ownership dimensions;
- The addition of nine new European CI sectors, after energy and transport, which were already in EPCIP. The new 11 sectors are energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, food, digital infrastructure,

public administration, and space. It was mainly the result of the recorded impact of the pandemic, but a tendency towards expansion had already been noted through European framework developments on cyber and through European projects on critical space infrastructures supplying critical services requiring dedicated European agencies to manage;

- A more developed European methodology to assist in the identification and designation of critical entities;
- Lower thresholds for criticality, meaning that more critical entities will be identified and designated compared to the previous models, which underestimated the required size and scope for a critical infrastructure to have systemic effects in case of its disruption;
- The development of a new category of critical entity (the critical entity of special importance), which affects a third or more Member States and which requires special coordination and resources to protect, increase its resilience and recover from disruptions. They also require stronger mechanisms for identification and designation through a collective approach;
- The development of a Critical Entities Resilience Group, made up of Commission experts who assist Member States and national authorities in the various EPCIP processes;
- The development of new networks and institutions/agencies, such as Cyber Competencies Centres and Information Sharing and Analysis Centres (ISACs) at European and national levels, constituting important networks for multilateral governance.

The national security and defence of Romania in the context of rapid digitalization of its own infrastructures and systems, as well as those of commercial partners, security partners and allies, require a proactive approach to the development of a cyber-resilient society.

Towards a New Agenda for Romanian Responses to Systemic Digitalization

The national security and defence of Romania in the context of rapid digitalization of its own infrastructures and systems, as well as those of commercial partners, security partners and allies, require a proactive approach to the development of a cyber-resilient society.

Table 2 identifies key priorities for research and development for Romanian private and public actors. This is not an exhaustive list, but one that covers a large spectrum of systemic cyber threats, including emerging technologies, new architectures and strategic priorities. (Vevera, Cârnu, Rădulescu, 2022). It is not feasible for the Romanian technological ecosystem to develop all of them on its own to adequate levels. Therefore, Romanian security consumers need to be aware of the threats to identify supply chains and vendors that can provide solutions when they are needed, whether they come from Romanian entities, Romanian subsidiaries of foreign companies or foreign companies headquartered in allied states with secure supply chains.

Deepfakes are a type of synthetic media content where the behaviour of a person in an existing video is intentionally altered.

Table 2: Priorities for cyber research to address systemic issues (Vevera, 2022)

Priority	Explanation
Integrating AI technology into remote authentication systems	AI technology can be used to introduce an additional level of security against the backdrop of the increase in remote working, through digital means, encouraged by the Covid-19 pandemic.
Researching digital forensic methods on Deepfake media content	Deepfakes are a type of synthetic media content where the behaviour of a person in an existing video is intentionally altered. It is used in disinformation and other hybrid operations. The emergence of these new digital means of manipulation generates the need and the opportunity to create innovative products to address the problem.
Analysis of the security and integrity of smart contracts used in Blockchain technology	Smart contracts allow the execution of credible transactions without the involvement of third parties to validate them. These transactions are public and irreversible in blockchain technology. The integration of blockchain applications not only in the area of cryptocurrencies, but as part of the background processes in the functioning of financial, logistical and administrative operations generates opportunities to create new products with security impact, but also the need to ensure security against terrorism, money laundering and attempts to manipulate and interrupt these processes.
Design and analysis of the architecture of self-sovereign digital identity systems (SSI)	SSI deals with the problem of establishing trust in an interaction. To be trusted, one party to an interaction will present its credentials to the other parties, and those parties can verify that the credentials come from an issuer they trust. In this way, the trust of the verifier in the issuer is transferred to the holder of the accreditation. These systems require new system architectures and innovative encryption solutions.

Quantum computing promises, once it becomes commercially available, to render existing encryption technologies obsolete.

Priority	Explanation
Research of adaptive networks based on analytical and business data	Adaptive networking is a new approach that expands on autonomous networking concepts to transform the static network into a dynamic, programmable environment driven by data analytics and intelligence. There are also applications for AI, going as far as autonomous decision-making systems, with security impact, as well as generation of new capabilities, including in the field of security.
Researching cyber threat detection methods using supercomputing (HPC) technology	HPC generally refers to the practice of aggregating computing power in a way that provides much higher performance than could be obtained from a desktop or workstation computer to solve problems of high complexity. The use of these applications, in conjunction with AI and other tools and capabilities, will respond to the need to ensure resilience in the face of a challenging security environment, with diverse and ubiquitous threats that require increased reaction capacity and new capabilities to analyse, attribute, limit effects and prevent intrusions.
Researching post-quantum cryptography methods	Quantum computing promises, once it becomes commercially available, to render existing encryption technologies obsolete. Therefore, there is a race to explore quantum-secure encryption methods, which can theoretically provide data security, and quantum-safe encryption methods, which can provide absolute certainty that they cannot be decrypted. Many research institutes are working on it, with the NIST in the US having already proposed 60+ quantum-secure methods of encryption, but some of them have already been broken. Therefore, this is an ongoing concern.
The transition of traditional network infrastructures to Zero-Trust architecture	A zero-trust security model requires that every device in a network undergoes a strict identity check every time it authenticates to the network, regardless of its location (whether it is inside the network or outside the network perimeter).
Cyber security research and the use of AI in addressing the problems of aggression and warfare in the electromagnetic spectrum	The anticipated revolution in the field of 5G, the ubiquity of mobile communications by various means (including Wi-Fi networks) and the implementation of wireless communication systems between the components of critical infrastructure systems such as sensors (even between the components of compact systems such as satellites), or in the framework of some distributed weapons systems generates a new security environment, exposed to attempts at jamming, signal hacking and data theft. As part of the hybrid war, we anticipate the evolution of electronic warfare as a means of diminishing the military capabilities as well as the civil infrastructures functioning. At the same time, we can anticipate the use of means of electronic warfare supported by AI decision-making systems related, for example, to signal modulation, as a means of equalizing military capabilities in the face of stronger and better equipped adversaries.
Using AI technology for new weapon systems	AI technology can be used for autonomous weapon systems, the coordination of drone swarms or *"loyal wingman"* systems already under development (UAVs that accompany piloted fighter jets) and the integration of classic military units with robotic systems logistic support or fire concentration.
Development of modelling and simulation capabilities, including in the *"digital twins"* field	These capabilities allow the detailed analysis of multifactorial security, including in the cyber domain, of complex systems or systems-of-systems, including at the level of cities or at the level of widely distributed critical infrastructures, such as electricity networks.

AI technology can be used for autonomous weapon systems, the coordination of drone swarms or "loyal wingman" systems already under development and the integration of classic military units with robotic systems logistic support or fire concentration.

In addition to the research priorities, the authorities, along with other stakeholders, should act to develop a resilient cyber solution ecosystem that provides supply chain security for critical infrastructure operators. With this in mind, we recommend fostering a dynamic private sector, not just through university-based hubs that encourage new start-ups (supply side), but also through demand side policies that generate more demand for cybersecurity related products and services in an expanding array of domains, including those undergoing late digitalization such as the construction industry (there is even a paradigm called Construction 4.0, based on the automation of the architecture, engineering, construction and facilities operation sector) (de Soto et al., 2022).

CONCLUSIONS

Omnipresent digitalization is generating a systemic impact on the functioning of critical infrastructures and, consequently, on the production of critical goods and services. On the one hand, it creates new efficiencies and new capabilities, allowing tighter integration of complex infrastructure systems-of-systems across geographic areas, domains, and value chains. On the other hand, it generates new risks, vulnerabilities and threats. Decision-makers, legislators and policymakers are trying to advance the framework for security governance to respond to the new circumstances, but technological change and the implementation happen faster than our capacity to adapt our awareness of the problem and improve our security culture.

We recommend fostering a dynamic private sector, not just through university-based hubs that encourage new start-ups (supply side), but also through demand side policies that generate more demand for cybersecurity related products and services in an expanding array of domains, including those undergoing late digitalization such as the construction industry .

The CIP framework provides a useful way to gauge the overall impact of digitalization. We have underscored the systemic transformations in the cyber field, the evolution of the cybersecurity and environment. Moreover, we have defined transversal approaches including the impact of new legislative developments at EU level and a possible national agenda for cyber development.

Future research will require new capabilities in modelling and simulation, their integration into business and governance processes, as well as adequate strategies and plans for dealing with the introduction of new technologies such as AI, quantum computing and blockchain.

BIBLIOGRAPHY:

1. Bucoveţchi, O., Simion, P.C. (2015). *Importance of interdependencies in critical infrastructures' protection.* UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science, 77 (1), pp. 301-309.
2. Chen, J., Lu, Y., Zhang, Y., Huang, F., Qin, J. (2023). *A management knowledge graph approach for critical infrastructure protection: Ontology design, information extraction and relation prediction*. International Journal of Critical Infrastructure Protection, 43, art. no. 100634, doi: 10.1016/j.ijcip.2023.100634.

3. *Cybercriminals Today Mirror Legitimate Business Processes*. *Fortinet Cybercrime Report 2013*. Fortinet, https://cybersafetyunit.com/download/pdf/Cybercrime_Report.pdf, retrieved on 12 January 2024.
4. De Soto, B.G., Georgescu, Al., Mantha, B., Turk, Ž., Maciel, A.&Sonkor, M.S. (2022). *Construction cybersecurity and critical infrastructure protection: new horizons for Construction 4.0*. ITcon, vol. 27, pp. 571-594, https://doi.org/10.36680/j.itcon.2022.028, retrieved on 22 January 2024.
5. European Commission (2023). Digital Economy and Society Index 2022, https://digital-strategy.ec.europa.eu/en/policies/desi, retrieved on 12 January 2024.
6. Georgescu, Al., Bucovețchi, O. (2023). *Protecția Infrastructurilor Critice – abordări conceptuale.* Craiova: Editura SITECH, ISBN 978-606-11-8547-4.
7. Gheorghe, A. V., Georgescu, A., Bucovețchi, O., Lazăr, M., & Scarlat, C. (2018). *New dimensions for a challenging security environment: Growing exposure to critical space infrastructure disruption risk*. International Journal of Disaster Risk Science, 9, 555-560.
8. Katina, P.F., Keating, C.B. (2015). *Critical infrastructures: a perspective from systems of systems*. International Journal of Critical Infrastructures, no. 11:4, pp. 316-344.
9. 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.
10. Nazir, S., Patel, S., Patel, D. (2017). *Assessing and augmenting SCADA cyber security: A survey of techniques*. Computers&Security, 70, pp. 436-454, doi: 10.1016/j.cose.2017.06.010.
11. O'Gorman, B., Wueest, C., O'Brien, D., Cleary, G., Lau, H.&Power, J.P., Corpin, M., Cox, O., Wood, P., Wallace, S. (2019). *Internet Security Threat Report.* Vol 24, Symantec, https://docs.broadcom.com/doc/istr-24-2019-en, retrieved on 22 January 2024.
12. Vevera, A.-V. (2022). *A transversal analysis of the cyber domain in critical infrastructure protection (Abordarea transversală a domeniului cyber în protecția infrastructurilor critice).* București: Editura Militară, ISBN 978-973-32-1275-1.
13. Vevera, A.V., Cîrnu, C.E., Rădulescu, C.Z. (2022). *A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection*. Studies in Informatics and Control, 31 (1), pp. 13-23. Doi: 10.24846/v31i1y202202.