University POLITEHNICA of Bucharest
Doctoral School of Entrepreneurship, Engineering and Business Management

The summary of the doctoral thesis titled:

New trends in the transversal analysis of the cyber domain in critical infrastructure protection. A system-of-systems perspective.

Scientific Advisor:
Prof. Dr. Eng. Adrian V. GHEORGHE

PhD Student:
Adrian Victor VEVERA

Bucharest
2022

Table of Content

Keywords: cybersecurity, critical infrastructure, system-of-systems, agent-based modelling, blockchain, resilience

Introduction

The purpose of the PhD thesis "New trends in the transversal analysis of the cyber domain in critical infrastructure protection. A system-of-systems perspective." Is to develop a systemic perspective on the cyber domain, making original contribution to our understanding of the evolution of the domain in the context of technological transformations which have made the digital ubiquitous within critical infrastructure networks at national, European and global levels. Information and communication technology (ITC) permeates every domain and facilitates important functions like command, control, coordination and information gathering for critical infrastructures to function at the efficiency and productivity frontier. At the same time, digitalization is generating new risks, vulnerabilities and threats, both as a result of the evolution of the technological substrate and as a result of the cybernetic interactions between the components of the infrastructure system-of-systems. The thesis proposes to describe these evolutions, to place them in an appropriate context and to make original contributions to our understanding of them from the perspective of the theoretical framework of critical infrastructure protection (CIP), anticipating major security trends. Practical contributions to the process of CIP governance will also be presented, whose usefulness will be validated through agent-based modelling,

The thesis features the following general objectives:

1. The transversal analysis of the cyber domain;
2. The identification of a specific need in the current security context, which can then guide the rest of the research process;
3. The development of an application, in a demonstration version, that can respond to that specific need.

The thesis features the following specific objectives:

1. The analysis of the cyber domain, including cybercrime, and generating conclusions regarding future systemic developments;
2. The analysis of the CIP domain and of its link to the cyber domain;
3. The analysis of national and international governance in the cyber domain and connected domains;
4. The development of a Netlogo model reliant on agent-based modelling to validate the application proposal's usefulness;
5. The designing of the application and of its systems architecture;
6. The building of the application and its validation on a virtual machine;
7. The drafting of an analysis on future avenues of development for the simulated model and for the application.

Figure 1 shows the research process through a logical schematic.

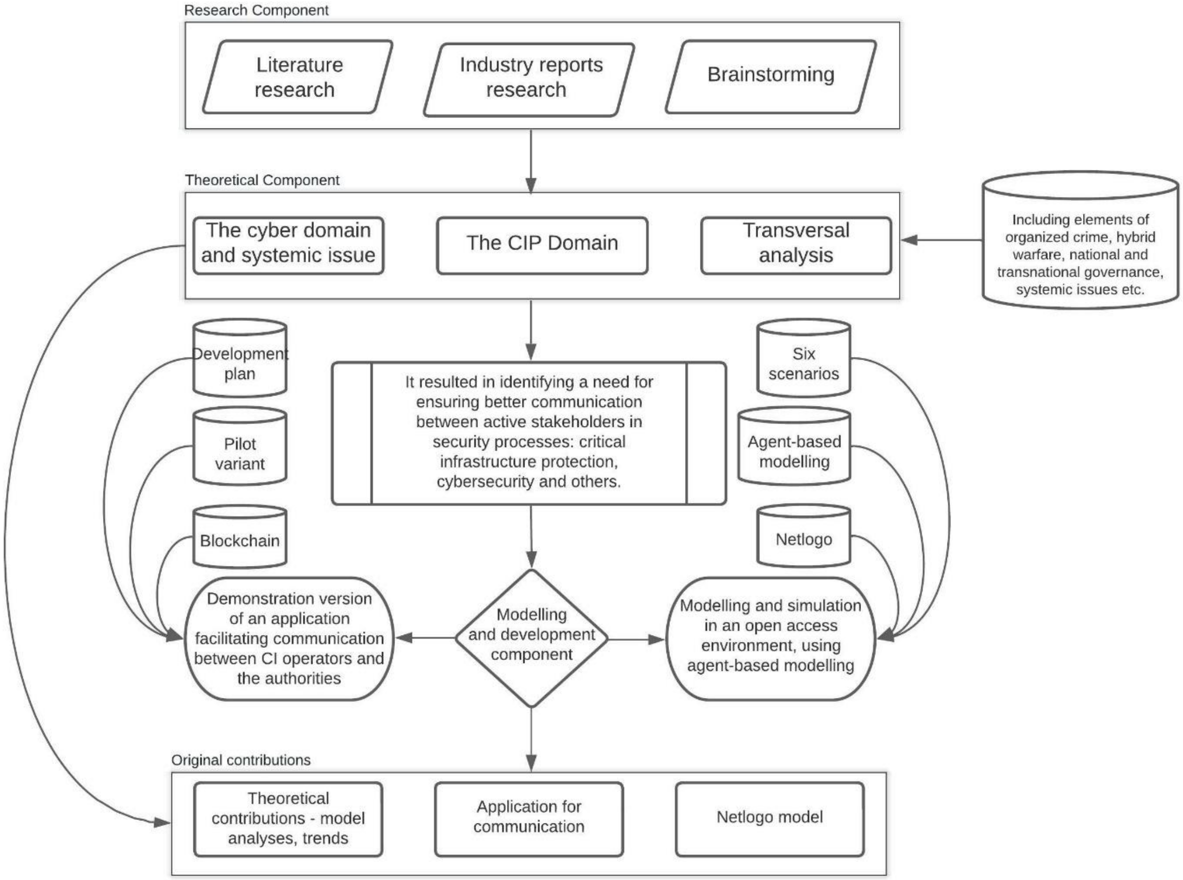

Figure 1. Logical schematic for the research process (source: author)

The research project highlighted the issue of communications between active stakeholders in critical infrastructure protection governance, especially as it relates to cybersecurity issues, which eventually led to the decision to develop a communication application based on blockchain technology which would contribute to the partial resolution of inherent informational asymmetries (for instance, between private companies and the state). The usefulness of this application was explored through agent-based modelling by building a generic critical infrastructure model in the Netlogo program to simulate a multi-stakeholder cyber defense system and to measure the changes in its performance when using a trusted system of information exchange between stakeholders. The simulation parameters were derived from the specialty literature and our own experience in the field. The simulation highlighted the usefulness of such an application, which resulted in the development of a demonstration version of the application for communication based on blockchain.

The thesis "New trends in the transversal analysis of the cyber domain in critical infrastructure protection. A system-of-systems perspective." is organized into the following chapters:

- Introduction;
- "Systemic transformations and the cybersecurity environment" – aspects related to the cyber environment – firstly, we detailed the systemic transformations ongoing in the field

and in the near future. Secondly, an analysis of the cybersecurity environment was made, followed by a strategic perspective on cyber related to Romania;

- “Critical Infrastructure Protection – general elements, European and global practice and systemic governance” – a detailed study of the specialty literature in CIP and system-of-systems engineering, emphasizing not only technical issues, but also considerations on governance;
- “A transversal approach to the cyber domain – European governance, legislative innovation and priority domains” – completed the descriptive and specialty literature analysis components of the thesis. The transformations in European CIP and cybersecurity frameworks were analyzed. The problem of cyber weapons and their proliferation was touched upon. Several original contributions were made, including an analysis of the European system for cyber governance which resulted in an ample graph;
- “High level modelling of cybersecurity for a critical infrastructure to highlight the opportunities stemming from information exchange” details the use of the free program Netlogo to build a model and run simulations with agent-based modelling to validate the theoretical usefulness of an application to safely intermediate communication between cybersecurity stakeholders, especially the actors within the EU governance frameworks for cybersecurity, and critical infrastructure operators under cyber-attack;
- “A blockchain based instrument to ensure communication between critical infrastructure operators and the competent authorities” is the main technical chapter and presents and application at the level of minimum viable product which facilitates the communication between critical infrastructure operators and various stakeholders, such as the actors responsible for cybersecurity that were modelled in the Netlogo simulation. The application is functional and is based on Hyperledger technology. Future versions can be run on EBSI (European Blockchain Services Infrastructure);
- Conclusions.

One of the main barriers hindering research into cybersecurity is the lack of information. Entities affected by cyber-attacks hesitate to inform the authorities or to offer details that would allow an efficient investigation. According to a report cited by the European Court of Audit, a third of European organizations would rather pay a ransom to regain access to their data than report the breaches (ECA, 2019). This is also true for companies with breaches of different types and which hesitate to cooperate with authorities for fear or reputational hits, liability or the exposure of trade secrets. At the same time, a report by the World Economic Forum claimed that the average dwell time (the period between entry and discovery) for an attacker who has penetrated the network of a European company is 99 days (WEF, 2018). This is why access to intelligence by authorities and the entities doing operational research into cybersecurity and assisting in the protection of critical infrastructures must be encouraged. The application developed as part of this thesis offers a potential contribution to the amelioration of this issue.

The Agent-Based Modelling simulation

The simulation was created within the newest stable version of the Netlogo application. This program was chosen because it is freeware, versatile, relatively easy to learn without pre-existing expertise as a programmer and benefits from numerous online resources created by other users that makes it easier to work with.

The simulation uses agent-based modelling, a method that relies on the semi-autonomous activity of agents generated in large numbers by the system in order to advance the model, leading to complex results from relatively simple interactions and rules. The model we created simulates, at a high level, a series of cyber-attacks on a generic critical infrastructure. The purpose is to highlight the benefits of implementing an application for communication between entities which are independent at an organizational level, but must work together to solve the issues. Facilitating the communication between the various security services means that a higher percentage of attacks can be successfully dealt with, while greater knowledge of how the attacks took place can result in a greater system resilience to attacks, including by attriting them without outside intervention. The attacks flow is arbitrary, based on simple decision models which, nevertheless, allows within the formal structure of the model to observe the differences between a simple system for collective defense and one better coordinated through a dedicated application.
The Netlogo model is composed of different types of objects with different visual identities, anchored in their functionality. There is an area for commands and data introduction, an area to visualize the model, an area to monitor important elements and an area for explanatory graphs. Figure 2 presents the complete interface of the model, composed of data entry areas, the model architecture and the graphic representation of its running, and the display zone for results and their interpretative graphs.

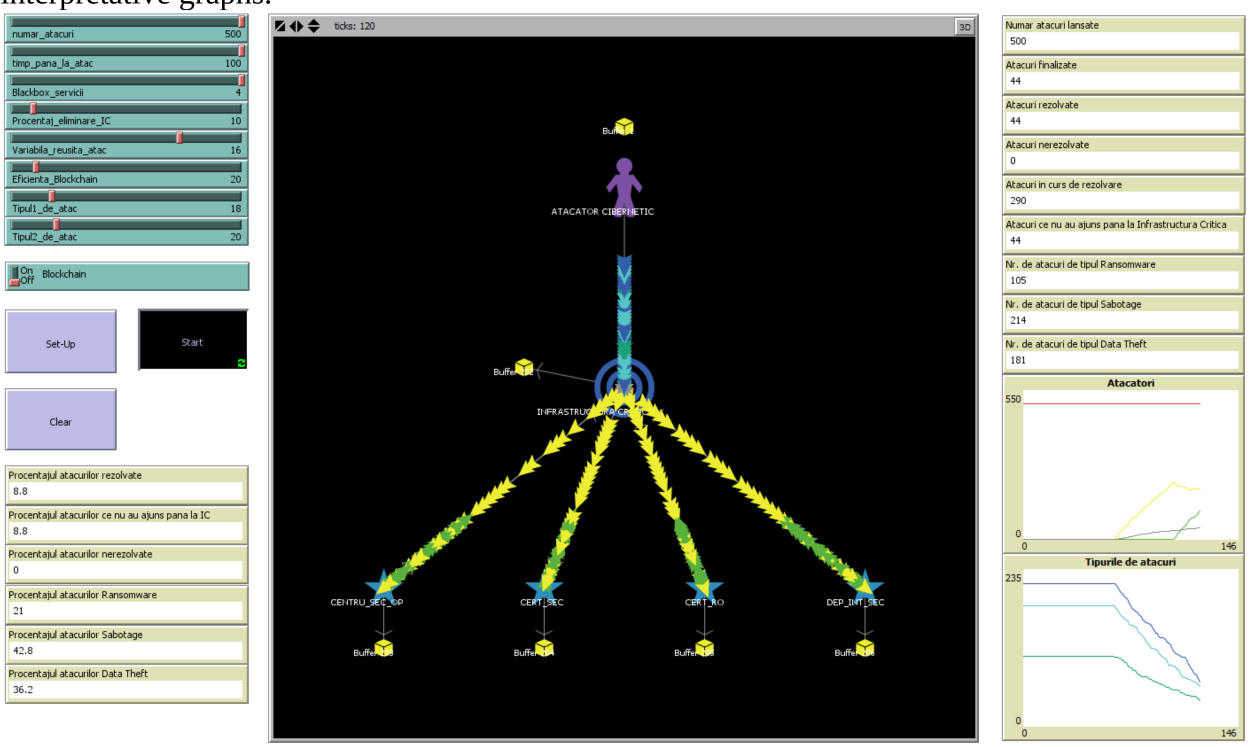

Figure 2. Complete graphical interface for the Netlogo model (source: author)

The principal agent of the system is the attacker, represented dynamically in the model, starting from the Northern end of figure 2 and summing up all the elements of the cyber threat environment in which the critical infrastructure operates. The attacker is, for the current model, a generic one and does not represent a particular type of actor (organized crime, state proxy, lone wolves, enemies within, transborder criminal networks etc.). In order to represent within the simulation the complexity of the security situations which may arise, attackers are generated with a random identification number and are processed individually by every system component in a probabilistic manner, according to internal (invisible) variables or those defined by the user. This is why the model will not generate the same results for every iteration of the model with the same parameters. While not functionally different, we have included three types of attackers to portray the diversity of the attacks, in the idea that future model iterations can implement variations in how the attacks take place, how they resolve, what impact they have and so on. The three types of attackers that the model can represent are as follows:

- Light blue – ransomware (controlled as a probability of appearance by the Tipul1_de_atac slider);
- Dark blue – sabotage (controlled as a probability of appearance by the Tipul2_de_atac slider);
- Light green – data theft (automatically calculated according to the first two sliders).

There are two other types of modelled actors:

- Yellow – actors that inform the entities defending the critical infrastructure;
- Green – actors that provide solutions to the cyber-attack, and which are produced by the defense entities.

All of the attackers pass through a filter which determines, according to a probabilistic formula, whether the attack will fail from the start due to some system quality or passive phenomenon such as the security culture of the employees or the quality of the defenses they employ (antivirus, anti-malware, anti-spyware etc.). Every critical infrastructure operator seeks to increase this passive resistance to deliberate or accidental threats from the security environment, which entails the minimization of vulnerabilities (endogenous) and of risks (exogenous). Attackers eliminated at this stage are also counted, but are placed in an "exit area for solved attacks". Those that pass through the filter will end up in the infrastructure system, where they will reside for an arbitrary span of time, depending on a variable when they were created. They are either solved by the system or the time runs out and the attack is successful by default (in real life, it would be, for instance, undetected or will have managed to fulfill its mission by the time it was detected). In the latter case, they end up in an "exit area for successful attacks" that is defined internally within the system. In the former case, the system first runs an identification function with a random amount of time until it gives a result to see whether the attacker is acknowledged by the system. If it is unsuccessful, a new one is started. When it becomes successful, a yellow information actor is generated and sent to the protectors, starting with the Department for Internal Security (DIS) of the critical infrastructure operator, which is the first responder in such situations. The DIS is an internal part of the operator's organization, but is represented externally in this model to indicate its operational role and the factor of communication with other defense actors. Defenders run a probabilistic function to identify the specific solution to a specific attack, which is characterized by the programmed success rate of each individual center and the random amount of time it takes to generate a possible solution. If successful, then a green solution actor spawns at the center and travels to the infrastructure operator, where it neutralizes the respective attacker, presuming that it has not yet completed its mission. When one center generates a solution for a particular attacker, all of the others give up trying to generate a solution for that particular attacker.

The other three actors, in this particular model, are the national Computer Emergency Response Team (CERT-RO), the sectoral one and an external operational security provider, which can be a private or state entity which offers particular services.

The solution actor can represent any number of possibilities – a particular strategy of approach, a particular piece of code, or various instructions, or a direct intervention by the particular center

and any number of other forms of assistance during crises. The model runs until the pre-programmed number of attackers is exhausted.
Table 1 shows a series of six scenarios. Each one has between 2 and 4 actors (at least one in addition to the DIS, in order to illustrate the gains from communication between defenders). The scenarios feature an experimental application which can be either on or off on the switch in the interface. The application is an intermediary for communication between stakeholders, in a way which fits with the needs stemming from the research into the specialty literature during this project. Running a scenario with the application on changes the Netlogo model by changing predetermined values within the system, representing both operational capacity in real terms during attacks, as well as the positive and diffuse long-term effect of increasing resilience through the value of information sharing. Therefore, we modify not only the probabilistic values of the functions that generate solution actors for attacks, but also the capacity of the filter to eliminate attackers before they reach the critical infrastructure. The reasoning is simple – most attackers are not criminal masterminds. They are attackers primarily out of the wish to gain something from illegal behavior. Many attackers reuse methods of attack, vulnerabilities in the attacked party, software, specific software like malware, patterns of attacks. The lack of communication within the system, often stemming from the desire of the attacked party to avoid bad publicity, financial liability and legal penalties, means that such repetitive elements are not identified in time to neutralize a particular attacker. Every scenario in table 1 had 500 attackers and similar proportions of different types of attackers, drawn from the specialty literature (O'Gorman et al, 2019).

Table 1. The comparative scenarios (source: the authors)

Type of scenario	**4 centers**		**3 centers**		**2 centers**	
	No blockchain	With blockchain	No blockchain	With blockchain	No blockchain	With blockchain
Number of attacks launched	500	500	500	500	500	500
Ransomware	94	90	104	93	93	88
Sabotage	212	219	221	242	212	218
Data Theft	194	191	175	165	195	184
Solved attacks	361	395	305	338	208	239
Unsolved attacks	131	105	195	162	292	261
Attacks that never reached the infrastructure	55	52	60	55	53	46
Percentage of solved attacks	72.20%	79.00%	61.00%	67.60%	41.60%	47.80%
Percentage of unsolved attacks	26.20%	21.00%	39.00%	32.40%	58.40%	52.20%
Percentage of attacks that never reached the infrastructure	11.00%	10.40%	12.00%	11.00%	10.60%	9.20%

We can observe the capacity of the model to generate different results based on probabilistic calculations, rather than deterministic ones. We can also see differences in success rates stemming from the use of our theoretical communication application between protectors. The simulation also highlights the importance of collective defense, by increasing the capacity of the critical infrastructure operators to respond to challenges in the security environment.

The demonstration application for blockchain-based communication

The justification for the need for the application

Our review of the specialty literature highlighted the importance of collective effort in defending critical infrastructures, especially from cyber threats. In such a system, the internal security department of a critical infrastructure operator is just one important component in a comprehensive system of cyber defense, which includes state agencies, European entities but also private contractors. The problem of communication between these actors becomes paramount and is acknowledged, as an issue, in official strategies and legislative and governance efforts. But this is not necessarily so at technical levels. Therefore, we have chosen to develop a demonstration level application that ensures the communication of different types and formats between critical infrastructure operators and the competent authorities.

The "Indicator Sharing for Critical Infrastructure Protection" application was inspired by the "Automated Indicator Sharing" (AIS) program. This is a model for encouraging exchanges between the authorities and critical infrastructure operators. This program is run through the Cybersecurity and Infrastructure Security Agency (CISA) of the Department for Homeland Security in the US. AIS is an automated initiative and is therefore fast, bidirectional (involving also the authorities exchanging pertinent information with the non-governmental participants), and also voluntary, offering inducements to prospective members in order to apply (CISA, 2021). It functions through members generating cyber threat indicators and defensive measures descriptions which are then distributed within the AIS network using standardized machine-readable message formats, such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII). This solves on of the important problems of cyber governance and diplomacy – the willingness and ability to share sensitive information securely and in a timely fashion. To protect the information, there is a combination of automated and human-based mechanisms to reduce the data transmitted to the minimum necessary, to only store important information and to only use it for security purposes. Enrolling in the program is free and its technical implementation is also a service that can be contracted to third party companies. The AIS program has become a basic infrastructure for ensuring cybersecurity in the select group of participants, but also for research, and its usefulness grows the more participants are enrolled in it and the more dangerous the cyber threat environment becomes.

The purpose of the application developed within this research project is to facilitate the reduction of information asymmetries between the actors and entities involved in operating, protecting and coordinating critical infrastructures. There are two types of actors that can be involved in the network:

- Critical infrastructure operators;
- Competent authorities of all types.

In practice and as a result of how the application was developed, there is no difference between types of entities involved, only between their roles and user privileges. In order to establish hierarchies and flows. This simplification also corresponds to the complex reality that the authorities are also, sometimes, operators of critical infrastructures, as are the dedicated defenders, public or private. The information flows are not just one way, between operators and authorities, but also two way, since authorities may share information to reduce asymmetries in the understanding of the evolution of the security environment and of the wider picture of the system-of-systems which, generally, only the state authorities possess. The information can also flow between operators, who are maybe connected through a relationship of interdependence between critical infrastructures. Information flows also between authorities, since they have a hierarchy and a need to coordinating and ensure the adequate provision of information between the strategic and operational levels of governance.

Unlike the "Automated Indicator Sharing" program, this application is based on a blockchain network component to mediate the sending of messages. This is a fundamental design decision that provides an original contribution from this research and results in different patterns in the use of the AIS program of the application detailed herein.

Blockchain as an emerging technology

Blockchain is a new technology with applications in numerous economic, administrative and governance related domains. It makes possible the transactions and database modifications that do now require an intermediary, while still ensuring integrity and greater security, thereby revolutionizing mass models for the organization and delivery of key services. At its most basic, the blockchain is a distributed database which is kept by every node or even every participant within the network and using specific algorithms, which are under continuous development, to automatically validate changes to the database without needing a central coordinating authority.

A new Industrial Revolution is underway through this solution to a key problem in the organization of human activity, that of trust and control. The applications of blockchain technology are much more varied than the media fixation on cryptocurrencies like Bitcoin and other financial instruments would have us think. We are seeing new domains of business using "smart contracts", supply chain management, fast transaction clearance and many more. From the perspective of national authorities, there are numerous potential applications for blockchain as part of governance and administrative systems, within the wider framework of e-government, such as electronic voting, database maintenance, cadaster management, information exchanges between different authorities etc. The application developed as part of this doctoral research project addresses security governance issues for critical infrastructures through the facilitation of information flows.

To implement the concept and developed the application, given the high level of competence and resources required to build a new blockchain protocol, we chose to use the Hyperledger technology, defined as a development center for applications that will be released open-source. Hyperledger gives user advantages such as high performance, ease of use, scalability and various data selection mechanisms. In the development process for the application, we used two specific instruments from the Hyperledger suite – Hyperledger Indy and Hyperledger Aries (Dhillon et al., 2017): Indy facilitates the solution to the issue of identity and data sovereignty, while Aries facilitates data exchanges and interoperability.

The latter is important because part of the usefulness of the application that we identified is the possibility of it being integrated with and running on the EBSI system (European Blockchain Services Infrastructure), whose first nodes in Romania have already been implemented. EBSI is a European project that provides infrastructure to accelerate the development of blockchain applications of public and private interest in the European Union, and reduce the gap between the EU and countries such as the US and China in the field of blockchain. The EBSI architecture contains multiple layers that provide generic capabilities and where every service can be built, documented and run. These layers were built with the idea of facilitating unknown future demands as efficiently as possible. The use of EBSI infrastructure allows an application to have a faster launch, with a higher degree of security, reliability and functionality, but with lower overheads. It also uses proof-of-authority to validate changes in the blockchain, which emphasizes consensus between preset nodes, thereby using already implemented systems and not requiring great initial expenses and buy-in from outsiders to provide mining and pooling capabilities. Proof-of-authority was selected because it requires the fewest resources and the least amount of monetization and financialization. Neither does it require high levels of electricity consumption to function. The control of node distribution ensures trust that the network cannot be subverted by coalitions of third party entities with decision rights, as sometimes happens with the miners for commercial blockchain networks.

The usefulness of the application

AIS transmits all data instantaneously, while the application here can register delays, according to the time needed for the transaction to be validated in the blockchain. Given the limited number of participants to the network (and the implicitly low number of users), which is hinted at by the limited number of entities on the lists of designated critical infrastructures and competent authorities, we can anticipate that the network of our application will be much smaller than those of commercial blockchain networks and that transactions will validate in a short period of time, a few minutes at most.

Even this small delay limits the usefulness of applications for the operational portion of crisis and emergency situation management. Rather the application for "Indicator Sharing for Critical Infrastructure Protection" can run before, after and in parallel with a crisis to enable trust in the integrity of the information received, a transparent custody chain for the information and trust in its confidentiality. We believe that the application will most likely be used for routine messaging and for reports on time-inelastic crises, as well as reports which become part of post-incident analyses to extract information, generate lessons and refine the system. The main facilitator for collective crisis management would be an AIS type structure, which prioritizes transmission speed. The blockchain network only send a cryptographic key to decrypt the message, not the message itself, which is transmitted via normal channels and may consist of a wide variety of content. In our vision, messages can be of four types, but only the first was implemented in the demonstration version of the application, being the simplest and facilitating two of the other ones:

1. Messages deliberately formulated by a human user, consisting of text, multimed content and other types of attachments, including files with data from the next three message types;
2. Messages which are formulated and sent automatically, at predefined intervals or whenever and abnormal situation occurs. The messages contain technical data regarding the functioning of the critical infrastructure, such as temperature, environmental indicators and other elements, especially for industrial infrastructures or other complex infrastructures. These messages may be parsed and read through automated systems, but solutions have to be tailored to each individual case<
3. Messages which are formulated and sent automatically, and consist of a standardized, machine-readable text such as one in the standards Structured Threat Information Expression (STIX), which codifies data on an ongoing cyber-attack;
4. Messages which are formulated and sent automatically, containing information codified under the Trusted Automated Exchange of Intelligence Information (TAXII) standard,

which is used to collect information on defensive measures undertaken by the actor affected.

The application can be developed in the future through the automation of message transmission and through the development of modules allow for standard communication exchanges. These messages can also become attachments in the manual communications between users. The development of these modules, even in pilot format, is beyond the scope of this research projects, but is possible by appealing to existing standards or by integrating ready-made modules from suppliers in the field, most of them being American.

The application will contribute to a better knowledge of the state of our critical infrastructure and to a better reconstruction of the crisis period events in order to extract useful conclusions that can become the basis of measures to be implemented to increase resilience. The application is suited for the following risks:

Gradual and undetected internal sabotage, manifested through anomalies in system functioning;

Risks regarding the falsification of data sent to partners during moments of crisis or their use as vectors for malware or spyware;

Risks of counter-intelligence operations to prevent the analysis of attacks, in order for the attacker to protect sources and methods. These are often reused by attackers and, therefore, incident analyses, the extraction of conclusions, the formulation of recommendations and the distributions towards operators can significantly increase systemic resilience.

Figure 3 shows one main element of the user interface for the application, a main dashboard area which allows various functions such as account generation, message redacting, their transmission and the reading of received messages.

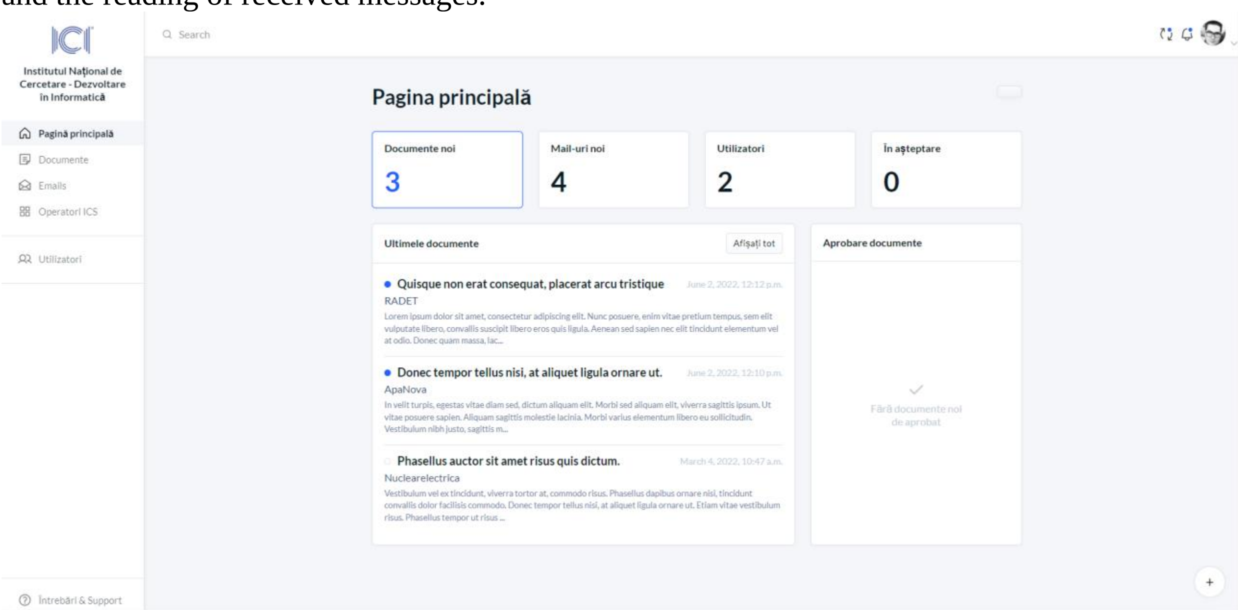

Figure 3. Dashboard, main page of the application’s user interface.

Through the way in which it was built, the application accommodates a wide variety of information flows – for example, a message flow can be sent from a CI operator to the authorities but also other CI operators, given (inter)dependencies that justify these flows to increase risk awareness regarding the security environment. We chose to use blockchain technology to also highlight the role this emerging technology can play in governance processes and to explore the flexibility of the technology in relation to the diverse needs of potential users.

The application currently runs on virtual machines but, for obvious reasons, it has not been tested in real conditions or between separate entities. This is possible with the application as it is right now, because it was built with generic components, especially the blockchain portion, which guarantees that it will function. In its current iteration, the application has two major features missing, because of the effort they would have required:

Messages are limited to those defined and written by the user, with documents attached. The application was can be further developed to transmit standardized messages automatically or on a regular schedule, containing technical indicator readouts for the critical infrastructure, but also standardized message types already in use in AIS to inform key stakeholders on the state of the cyber system's security and on the defensive measures being implemented;

The implementation of these standardized messages should also be accompanied by automated reading and interpretation modules, which are currently missing. Infrastructure data requires custom development for every important indicator of each infrastructure type, keeping in mind the specifics of each sector or each individual asset.

This demonstration application has the potential to be developed for use in certain situations, based mostly on the advantages and disadvantages of the blockchain solution, as mentioned before. Even if it was conceptually inspired by the American AIS program, its reconfiguration to work with a blockchain component has led to a complete paradigm shift and a novel contribution with potential use in physical but especially cyber security. With the use of the Hyperledger blockchain, the application is further compatible with EBSI, which improves its chances for future development outside of the research project. The development of the application represents the culmination of the doctoral research program and is the result of the theoretical study and the impact simulation developed over the various phases of the project. Overall, the research project makes an important original contribution to the study of the impact of emerging digital technologies on the critical infrastructure system-of-systems

Conclusions and original contributions

Numerous original contributions were made during the research period, which are highlighted as part of the doctoral thesis documentation. The following is an exhaustive list of these contributions:

- The analysis of the systemic transformation phenomena caused by the cyber revolution, also from the perspective of critical infrastructures;
- The analysis of the transformations in the cybersecurity environment;
- A framework perspective on systemic cyber governance based on the framework of Complex System Governance;
- A perspective on the synergies at governance level between multiple transnational critical infrastructure networks (BRI, 16+1, 3SI);
- A systemic analysis of a global geopolitical initiative from the perspective of critical infrastructure theory (BRI);
- An analysis of the systemic impact of the new legislative proposals at EU level (the CER and NIS2 Directives) which, at the moment of finalization of the research, had just been approved politically at EU levels;
- An analysis of the European cybersecurity ecosystem, finalized with a graph chart that highlights its complexity;

- A series of priority domain proposals to develop new cyber capabilities at national level that would be useful not just economically, but also from the perspective of enhancing Romanian cybersecurity;
- An open-source analysis of the problem of cyber weapons proliferation, focused on Wikileaks documentation;
- The development of a high-level Netlogo model that can underline the role of cooperation between the critical infrastructure operator and various entities and agencies involved in cybersecurity issues in order to ameliorate the negative impact of exposure to a cybersecurity environment that is beset by deliberate threats;
- The development of a demonstrative application based on blockchain technology which can mediated communications between the critical infrastructure operators and various stakeholders and other entities with a role in the national CIP efforts. The previously developed Netlogo model validated the usefulness of such an application, which was initially suggested from the literature review, and the documentation includes also suggestions of future development for the application to increase its usefulness.

This application is an original contribution in three ways:

1. It demonstrates how the emerging blockchain or Distributed Ledger technology can be used to mediate secure communications between critical infrastructure operators and the competent authorities as part of the Critical Infrastructure Protection process and the governance of security;
2. Even though it was built using Hyperledger technology, the application can function within the EBSI infrastructure and demonstrates a potential new application area for EBSI (the European Blockchain Services Infrastructure) which does not feature so many applications at the current moment and most of them are geared towards identity management and validation of claims;
3. Contributes to the understanding the impact of blockchain technology implementation at critical infrastructure management level (through communications), including from the perspective of Complex System Governance.

We consider that the research project has reached its goal – through a thorough review of specialty literature and through our own experience working in this field and in inter-institutional cooperation, we explored the systemic effects of the digitalization of critical infrastructures and of the emerging digital technologies. Numerous original contributions were made, on a point-by-point basis, to the analysis and the understanding of these phenomena. From the research, we concluded that it is very important to optimize the collective cyber defense process for critical infrastructures and to explore innovative ways to enhance the effectiveness of governance. We chose to address the issue of the communication between various entities involved in the protection of a critical infrastructure. The first original contribution was to use a program for modelling and simulation with wide use in the academic world in order to implement an agent-based modelling solution to illustrate the importance of communications and information exchanges in order to address cybersecurity issues facing critical infrastructure operators. The second contribution was to develop a demonstration application that facilitates this communication and to which also integrates an emerging digital technology, which is the blockchain technology. The application is functioning and usable.

The final conclusion of the research efforts is that the security environment is complex, dynamic and challenging, and digital trends will amplify our uncertainties and our exposure to deliberate threats stemming from financial, criminal and even military motives. Even worse, these attacks will target the critical socio-technical systems which produce critical goods and services which facilitate the economic, social and political lives of our nation and of the European Union. Despite these issues, we can advance our knowledge of these trends to improve the security governance processes, and we can develop new instruments to ensure successful governance of these complex critical infrastructure systems.

List of published works

Book Chapters:

1. Vevera, A. V., Cirnu, C.E., Georgescu, A. (2021). Blockchain in the management of complex system – impact on sustainable development. In Ranf, D.E., Bucovețchi, O., Badea, D. (eds) (2021). Sustainability management and managerial sustainability between classic and modern paradigms. Pag 214-233, Ed. Academiei Forțelor Terestre Nicolae Bălcescu Sibiu 2021, ISBN 978-973-153-419-0
2. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020). "A Critical Infrastructure protection Perspective on Counter-Terrorism in South-Eastern Europe". In Caleta, D., Powers, J.F. (2020) Cyber Terrorism and Extremism as a Threat to Critical Infrastructures. published by Slovenian MoD and Special Forces University in Tampa, Florida, ISBN 978-961-94011-2-5, Ljubljana, September2020
3. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020), "Critical Space Infrastructures – a comparison to terrestrial CI", în Tatar, U., Gheorghe, A.V., Keskin, O.F., Muylaert, J. (Eds.) (2020), "Space Infrastructures: From Risk to Resilience Governance", p. 7-21, DOI 10.3233/NICSP200004, IOS Press, Vol. 57 din NATO Science for Peace and Security Series - D: Information and Communication Security, ISBN 978-1-64368-072-9
4. Vevera, A. V., Georgescu, A., Cirnu, C.E. (2019). The paradigm of complex system governance, necessary in an interconnected world. In Badea, D., Bucovetchi, O, Iancu, D. (coord) (2019). The management of capabilities and managerial capability within critical infrastructure systems. pg. 270-283, Ed. Academiei Forțelor Terestre Nicolae Bălcescu Sibiu, ISBN 978-973-153-375-9

Articles:

1. Vevera, A.V. (2022). Critical Infrastructure Diplomacy – Tracing the Contours of a New Practice. International Journal of Cyber Diplomacy, ISSN 2668-8662, vol. 3, pp. 41-49, 2022. https://doi.org/10.54852/ijcd.v3y202205
2. Vevera, A.V., Cirnu, C.E, Rădulescu, C.Z. (2022). A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection. Studies in Informatics and Control, ISSN 1220-1766, vol. 31(1), pp. 13-23, 2022. https://doi.org/10.24846/v31i1y202202 (WOS:000779783700002)
3. Vevera, A.V., Cirnu, C.E., Georgescu, A. (2022). A Critical Infrastructure Perspective and Systems Perspective on Hybrid Threats in the Black Sea Region. Gândirea Militară Românească, nr. 1 (2022), ISSN Print: 1454-0460, ISSN Online: 1842-8231 și Romanian Military Thinking nr. 1 (2022), 1841-4451, ISSN Online, 1842-824X (indexat EBSCO și CEEOL)
4. Vevera, A. V., Georgescu, A., Cirnu, C.E. (2021). "Opportunities for Cybersecurity Research in the New European Context", In Romanian Cyber Security Journal, vol. 3 (1), pag 79-88, ISSN 2668-1730, ISSN-L 2668-1730 (indexat BDI, CNKI, Crossref)
5. Sarfraz, M., Ivascu, L., Khawaja, K.F., Vevera, A.V., Dragan, F. (2021). ICT Revolution from Traditional Office to Virtual Office: A Study on Teleworking During the COVID-19 Pandemic. Studies in Informatics and Control, ISSN 1220-1766, vol. 30(4), pp. 77-86, 2021. https://doi.org/10.24846/v30i4y202107 (WOS:000732461100007)
6. Vevera A.V. (2021). Promoting digital diplomacy through education. "Carol I" National Defence University Publishing House Bucharest, Bulletin of "Carol I" National Defence University, nr. 4, 2021, pp 22-27, ISSN 2284-936X

7. Vevera A.V. (2021). Evaluation of Digital Diplomacy as a form of soft power projection in European Union CSDP Mission. “Carol I” National Defence University Publishing House Bucharest, Bulletin of “Carol I” National Defence University, nr. 3, 2021, pp 41-46, ISSN 1584-1928;
8. Vevera A.V., Topor S. (2021). The communicational dimension of digital diplomacy. Scientific Research and Education in the Air Force -AFASES, NR. 22, 2021, pp 79-84, ISSN 2247-3173; (indexat EBSCO)
9. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020). Cyber as a Transformative Element in the Critical Infrastructure Protection Framework. In Romanian Cyber Security Journal, ISSN 2668-1730, ISSN-L 2668-1730, vol. 2 (1), 37-44 (indexat BDI, CNKI, Crossref)
10. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2020). The Diplomacy of Systemic Governance in Cyberspace. International Journal of Cyber Diplomacy, Volumul 1, Nr. 1, pag. 79-88
11. Vevera A.V. (2020). Diplomația digitală ca strategie de gestionare a schimbărilor din mediul internațional. Editura Universității Naționale de Apărare ”Carol I”, Impact Strategic, nr.. 4, 2020, pp 113-123, ISSN 1582-6511
12. Boncea R., Petre I., Vevera A.V. (2019). Building trust among things in omniscient Internet using Blockchain Technology. Romanian Cyber Security Journal, no. 1, vol 1, pp 25-33, 2019, ISSN 2668-1730 (indexat BDI, CNKI, Crossref)
13. Georgescu, A., Vevera, A. V., Cirnu, C.E. (2019). The Proliferation of Cyber Weapons - Theory and Mitigation-. In Romanian Cyber Security Journal, ISSN 2668-1730, ISSN-L 2668-1730, vol. 1 (2), 37-46 (indexat BDI, CNKI, Crossref)
14. Vevera, A.V., Onofrei-Riza, D.B. (2019). Investigații mobile – captură, analiză și stocare a datelor senzitive. Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control), ISSN 1220-1758, vol. 29(1), pp. 45-50, 2019. https://doi.org/10.33436/v29i1y201904 (indexat ESCI)

Conference proceedings:

1. Vevera, V., Georgescu, A. Cirnu, C.E., Nate, S. (2022). Critical Infrastructure Protection - resilience in an uncertain future. În Ioanid, A., Fleacă, B., Moiceanu, G. (Eds.) (2022). International Conference of Management and Industrial Engineering 2021 “Business Change and Digital Transformation in A World Moving Through Crisis”. Pag. 209-222 FAIMA, UPB, București, România, ISSN 2344-0937, ISSN-L 2344-0937
2. Vevera, V., Georgescu, A., Cîrnu, C-E. Critical Space Infrastructures - a New Frontier for Security, Chapter 7, In Minchev, Z. (Editor), Digital Transformation in the Post-Information Age, SoftTrade &Institute of ICT, Bulgarian Academy of Sciences, 2022, ISBN 978-954-334-251-8, proceedings ale Conferinței International Conference on Advanced Research and Technology for Defence, organizată în Varna, Bulgaria, în perioada 29-30 iunie 2021
3. Vevera A.V., Topor S. (2021). Digital diplomacy in the context of promoting a strategy for a comprehensive approach to the common security and defence policy missions and operations. “Carol I” National Defence University Publishing House Bucharest, Proceedings, The International Scientific Conference “Strategies XXI”, Global Security and National Defence, pp 371-377, 2021, ISSN 2668-2281;
4. Vevera A.V. (2021). National level implementation of digital diplomacy mechanism and functions based on EU experience. “Carol I” National Defence University Publishing House Bucharest, Proceedings International Scientific Conference Strategies XXI, 2021, pp 135-142, ISSN 2668-6511.

Bibliography

1. *** (1998). Presidential Decision Directive/NSC-63. Casa Albă, Washington DC, referire ca PDD-63. https://clinton.presidentiallibraries.us/items/show/12762
2. *** (2006). Report on System of Systems Engineering: Submitted to the Secretary of Defense. Stevens Institute of Technology: Hoboken, NJ, SUA, 2006, referință ca Stevens (2006).
3. *** (2008). Directiva 114/2008 a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora. Comisia Europeană, ca CE (2008). https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32008L0114
4. *** (2013), Joint publication 3-12: Cyberspace operations, Departamentul Apărării al SUA, scris ca DoD (2013), https://fas.org/irp/doddir/dod/jp3_12r.pdf
5. *** (2015). National Guidelines for Protecting Critical Infrastructure from Terrorism Comitetul Contra-Terorism al Australiei și Noii Zeelande, referit ca ANZCTC (2015), ISBN: 978-1-925290-43-1, https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf
6. *** (2017) 2017 Cybercrime Report. Cybersecurity Ventures / Herjavec Group, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
7. *** (2017), A guide to the Internet of Things Infographic, Intel Corporation, https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
8. *** (2017), Gartner Says Worldwide Wearable Device Sales to Grow 17 Percent in 2017, Gartner, 24 august 2017, https://www.gartner.com/newsroom/id/3790965
9. *** (2017), Global Cybersecurity Index (GCI) 2017, Uniunea Internațională de Telecomunicații, Organizația Națiunilor Unite, disponibil online la adresa https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
10. *** (2017), Measuring the Information Society Report 2017 Volume 1, Uniunea Internațională de Telecomunicații, Organizația Națiunilor Unite, disponibil online la adresa https://read.itu-ilibrary.org/science-and-technology/measuring-the-information-society-report-2017_pub/80f52533-en (ITU, 2017, 2)
11. *** (2017). Ascunderea de date în imagini. Wikileaks, scris ca Wikileaks (2017o), https://wikileaks.org/ciav7p1/cms/page_13763247.html
12. *** (2017). Building the Belt and Road: Concept, Practice and China's Contribution. Office of the Leading Group for the Belt and Road Initiative. mai 2017, Foreign Language Press, ISBN 978-7-119-10810-0, ca OLG (2017), https://www.tralac.org/images/docs/11613/building-the-belt-and-road-concept-practice-and-chinas-contribution-may-2017.pdf
13. *** (2017). Componente colecție de date. Wikileaks, scris ca Wikileaks (2017d), https://wikileaks.org/ciav7p1/cms/page_2621753.html
14. *** (2017). Datele din pachetul Vault. Wikileaks, scris ca Wikileaks (2017a), https://wikileaks.org/ciav7p1/
15. *** (2017). Ghid de utilizator Hive. Wikileaks, scris ca Wikileaks (2017s), https://wikileaks.org/ciav7p1/cms/files/UsersGuide.pdf
16. *** (2017). Ghid pentru dezvoltator Hive. Wikileaks, scris ca Wikileaks (2017t), https://wikileaks.org/ciav7p1/cms/files/DevelopersGuide.pdf

17. *** (2017). Hacking pentru autovehicule. Wikileaks, scris ca Wikileaks (2017j), https://wikileaks.org/ciav7p1/cms/page_13763790.html
18. *** (2017). Indexul datelor pe proiecte CCI, după ramură. Wikileaks, scris ca Wikileaks (2017f), https://wikileaks.org/ciav7p1/cms/index.html
19. *** (2017). Module de persistență. Wikileaks, scris ca Wikileaks (2017r), https://wikileaks.org/ciav7p1/cms/page_13763650.html
20. *** (2017). Organigramă centru de inginerie cyber CIA. Wikileaks, scris ca Wikileaks (2017b), https://wikileaks.org/ciav7p1/files/org-chart.png
21. *** (2017). Produsul Brutal Kangaroo Wikileaks, scris ca Wikileaks (2017p), https://wikileaks.org/ciav7p1/cms/page_13763236.html
22. *** (2017). Produsul Hammer Drill. Wikileaks, scris ca Wikileaks (2017m), https://wikileaks.org/ciav7p1/cms/page_17072172.html
23. *** (2017). Programul Hive. Wikileaks, scris ca Wikileaks (2017l), https://wikileaks.org/ciav7p1/#HIVE
24. *** (2017). Proiectul Weeping Angel. Wikileaks, scris ca Wikileaks (2017i), https://wikileaks.org/ciav7p1/cms/page_12353643.html
25. *** (2017). Ramura de dezvoltare dispozitive încorporabile. Wikileaks, scris ca Wikileaks (2017h), https://wikileaks.org/ciav7p1/cms/space_753667.html
26. *** (2017). Ramura de dezvoltare pe platforme mobile. Wikileaks, scris ca Wikileaks (2017g), https://wikileaks.org/ciav7p1/cms/space_3276804.html
27. *** (2017). Ramura de dispozitive de rețea. Wikileaks, scris ca Wikileaks (2017c), https://wikileaks.org/ciav7p1/cms/space_15204355.html
28. *** (2017). Resolution 2341: Threats to international peace and security caused by terrorist acts. Rezoluția 2341 (2017) adoptată de Consiliul de Securitate ONU la cea de-a doua 7882a întâlnire, 13 februarie 2017, S/RES/2341 (2017), referit în text ca UNSC (2017), http://unscr.com/en/resolutions/doc/2341
29. *** (2017). Viruși prin medii de stocare date. Wikileaks, scris ca Wikileaks (2017n), https://wikileaks.org/ciav7p1/cms/page_13762636.html
30. *** (2017). Vulnerabilități Android. Wikileaks, scris ca Wikileaks (2017e), https://wikileaks.org/ciav7p1/cms/page_11629096.html
31. *** (2017). Vulnerabilități Windows. Wikileaks, scris ca Wikileaks (2017k), https://wikileaks.org/ciav7p1/cms/page_11628612.html
32. *** (2018) Rightscale 2018 State of the Cloud Report. RightScale, https://www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf
33. *** (2018). Cyber Resilience Playbook for Public-Private Collaboration. Forumul Economic Mondial si Boston Consulting Group, scris ca WEF (2018), http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf
34. *** (2018). Prevention is better than cure. Risk:Value 2018 Report. NTT Security, apud Curtea Europeană de Audit (2019). Challenges to effective European cybersecurity. Briefing paper, martie 2019, scris ca ECA (2019) https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
35. *** (2019) Proiecte prioritare de interconectare – raport 2019. Site-ul principala al 3SI, referință în text ca 3SI (2019), https://www.three.si/progress-report
36. *** (2019) The Digital Three Seas Initiative: a call for a cyber upgrade of regional cooperation. White Paper, Institutul Kosciuszko, Varșovia, 2019, referință ca Kosciuszko

(2019), https://digital3seas.eu/wp-content/uploads/2019/12/ik_policy_brief_3si_updated_11122019.pdf
37. *** (2019). BRI Connect: An Initiative in Numbers. Refinitiv, RE955166/6-19, ca Refinitiv (2019), https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/refinitiv-zawya-belt-and-road-initiative-report-2019.pdf
38. *** (2019). Date EUROSTAT cheltuieli nationale cu cercetare si dezvoltare. Eurostat, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20201127-1
39. *** (2019). Fondul de Apărare. Comisia Europeană, scris sub forma Comisia Europeană (2019d), https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-eu-defence-fund_en_0.pdf
40. *** (2019). Fondul de Securitate Internă. Comisia Europeană, scris sub forma Comisia Europeană (2019c). https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-internal-security-fund_en.pdf
41. *** (2019). Programul InvestEU. Comisia Europeană, scris sub forma Comisia Europeană (2019b), https://ec.europa.eu/commission/sites/beta-political/files/what_is_investeu_mff_032019.pdf
42. *** (2020). Blue Dot Network. Departamentul de Stat al SUA, referire ca USDS (2020), https://www.state.gov/blue-dot-network/
43. *** (2020). COM(2020) 823 final - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Scris în text ca Comisia Europeană (2020b), https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0823&from=EN
44. *** (2020). COM(2020) 829 final - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. Scris în text ca Comisia Europeană (2020a), https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0829&from=EN
45. *** (2021), Digital Economy and Society Index 2021, Comisia Europeană, https://ec.europa.eu/digital-single-market/en/desi
46. *** (2021). Date EUROSTAT cheltuieli guvernamentale cu cercetare dezvoltare, Eurostat, https://ec.europa.eu/eurostat/databrowser/view/sdg_09_10/default/table?lang=en
47. *** (2021). Documentația Automated Indicator Sharing. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, SUA, scris ca CISA (2021), https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
48. *** (2022). Documentație Kubernetes – componente Kubernetes. Site de documentație, scris ca Kubernetes (2022). https://kubernetes.io/docs/concepts/overview/components/
49. ***(2013) Cybercriminals Today Mirror Legitimate Business Processes, Fortinet Cybercrime Report 2013, Fortinet, https://cybersafetyunit.com/download/pdf/Cybercrime_Report.pdf
50. Albrycht, I., Brzęcka, W., Felici, F., Konkel, A., Mikulski, K., Siudak, R., Świątkowska, J. (2019). Securing the Digital DNA – the Three Seas Region. Institutul Kosciuszko, 2019, https://ik.org.pl/wp-content/uploads/raport_securing_digital_dna_3si.pdf
51. Barrio Juárez, F.A., Granadino, P.R., Thill, F., Rhodes, S., Laukka, L., Salonen, M., Mägi, K., Mõtus, M., Průša, J., Raposo, R., Rosenkranz, W., Borchert, H., Jendricke, U., Alink, H.O., Peeters, G.J.P., Reichard, A., Pyznar, M., Kavcic, M., Sordyl, J., Halásová, Z., Grebáč, P., Nikkel, B. (2017), Public Private Partnerships (PPP) Cooperative models, raport ENISA,

noiembrie 2017, https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models
52. Bauer, J. M., van Eeten, M. (2009) Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy 33(10-11):706-719, https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options
53. Bauer, J. M., Van Eeten, M., Chattopadhyay, T., Wu, Y. (2008) Financial implications of network security: Malware and spam. Report for the International Telecommunication Union (ITU), Geneva, Switzerland, July 2008, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf
54. Baugh, D. (2015). Environmental Scanning Implications in the Governance of Complex Systems. Int. J. Syst. Syst. Eng. 2015, 6, 127–143.
55. Bryce Space and Technology (2019) Smallsats by the numbers 2019, https://brycetech.com/downloads/Bryce_Smallsats_2019.pdf
56. Carus, S.W. (2012), Defining "Weapons of Mass Destruction", Occasional Paper 8, Center for the Study of Weapons of Mass Destruction, National Defense University, https://www.researchgate.net/publication/281863975_Defining_weapons_of_mass_destruction
57. Centrul pentru Securitate Cibernetică (2019), Forumul Economic Mondial, https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications
58. Cheney, C. (2019). China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. ISSUES & INSIGHTS, Vol. 1 9, WP8, July 2019, Pacific Forum, https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf
59. Coburn, A.W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., Harvey, T. (2019). Cyber risk outlook. Centre for Risk Studies, University of Cambridge, în colaborare cu Risk Management Solutions, Inc.
60. Cohen, D., Rotbart, A. (2013). The proliferation of weapons in cyberspace. în Gabi Siboni (ed.) (2013), Cyberspace and National Security, pag. 105-127, Institute for National Security Studies, Tel Aviv, Israel, ISBN: 978-965-7425-51-0
61. Comisia Europeană (2016) DIRECTIVA 2008/114/CE A CONSILIULUI din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora. Bruxelles, 23.12.2008
62. Comisia Europeană (2016) JOIN(2016) 18 - COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU – Cadrul comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene. Bruxelles, 06.04.2016
63. Comisia Europeană (2016) JOIN(2016) 18 - COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU – Cadrul comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene. Bruxelles, 06.04.2016
64. Constantin, A. (2021). Study: Romanian companies plan to spend 14 percent of their IT budgets on cybersecurity in 2021. Business Review, 5 ianuarie 2021, https://business-review.eu/tech/it/study-romanian-companies-plan-to-spend-14-percent-of-their-it-budgets-on-cybersecurity-in-2021-216185
65. Delanoë, I. (2015), Weapons of Mass Destruction – a Persisting Security Challenge in the Black Sea Region, Neighborhood Policy Paper no. 16, Center for International and European

Studies, Kadir Has University, iulie 2015, https://www.files.ethz.ch/isn/193512/NeighbourhoodPolicyPaper(16).pdf
66. DeLaurentis, D. (2005) Understanding transportation as a system-of-systems design problem. În 43rd AIAA Aerospace Sciences Meeting. Reno, NV: American Institute of Aeronautics and Astronautics, https://doi.org/10.2514/6.2005-123
67. Dewar, R. (2017), Active Cyber Defense, ETH Zurich, noiembrie 2017, DOI: 10.13140/RG.2.2.19236.17287
68. Dhillon, V., Metcalf, D. & Hooper, M. (Eds.). (2017). The Hyperledger Project. Blockchain Enabled Applications,139-149. Florida: Apress Media.
69. Eder, T., Arcesati, R., Mardell, J. (2019). Networking the "Belt and Road" - The future is digital. Mercator Institute for China Studies, 28 August 2019, https://merics.org/en/analysis/networking-belt-and-road-future-digital
70. Falco, G. (2018) Job One for Space Force: Space Asset Cybersecurity. Cyber Security Project, Belfer Center, Harvard University, 12 iulie 2018, https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity
71. Fingleton, E. (2014). Boeing goes to pieces. The American Conservative, 8 ianuarie 2014 https://www.theamericanconservative.com/articles/boeing-goes-to-pieces/
72. Finklea, K. (2017) Dark Web. US Congressional Research Service Report, Congresul SUA 10 martie 2017, https://fas.org/sgp/crs/misc/R44101.pdf
73. Geers, K. (2010), Cyber Weapons Convention, Computer Law & Security Review, Volume 26, Issue 5, September 2010, Pages 547-551, https://doi.org/10.1016/j.clsr.2010.07.005
74. Georgescu, A. (2017). Critical infrastructure protection for the Belt and Road Initiative. în Duško Dimitrijević, Huang Ping, " Initiatives of the 'New Silk Road' Achievements and Challenges ", pg. 191-204, Institutul pentru Studii Politice si Economice din Belgrad si Academia de Stiinte Sociale a Chinei, ISBN 978-86-7067-246-8
75. Georgescu, A. (2018), "Critical infrastructure protection – challenge and opportunity for the Belt and Road Initiative", in Jurnalul Diplomatic Bulgar 20/2018, pg 265-274, ISSN 1313-6437
76. 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, vo. 1 (1), 93-100
77. Georgescu, A., Cirnu, C.E. (2019). Industry 6.0 – new dimensions for industrial cooperation on the Belt and Road. în Valentin Katrandzhiev (ed.) (2019), "The 16+1 Sofia Think Tanks Conference 'Advancing 16+1 Cooperation Platform – the Way Ahead'", Institutul Diplomatic Bulgar, ISBN 978-619-7200-14-0
78. Georgescu, Gheorghe, A., Piso, M.-I., Katina, P.F. (2019). Critical Space Infrastructures: Risk, Resilience and Complexity, Topics in Safety, Risk, Reliability and Quality. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-12604-9
79. Gharajedaghi, J. (1999) Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture. Butterworth-Heinemann: Waltham, MA, USA, 1999, ISBN-13 : 978-0123859150
80. Gheorghe, A. (2017) Internet of Space: Issues for a System of Systems Engineering Approach, prezentare în cursul celei de-a 7a conferințe anuale pe tema Space Systems as Critical Infrastructure organizată de către Agenția Spațială Română și Academia Internațională de Astronautică

81. Gheorghe, A., Bouchon, S., Birchmeier, J. (2005) Toward Guidelines for Regional Assessment of Vulnerability against Service Disruption of Critical Infrastructures. Proceedings: Al 29lea seminar EsReDa - Analiza sistemelor pentru o lume mai sigură. p.81-95, http://publications.jrc.ec.europa.eu/repository/handle/JRC32271
82. Gheorghe, A.V., Schlapfer, M., 2006. Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures, în: 2006 IEEE International Conference on Systems, Man and Cybernetics,pp. 580–584. https://doi.org/10.1109/ICSMC.2006.384447
83. Gheorghe, A.V., Vamanu, D.V., Katina, P.F., Pulfer, R. (2018) Critical Infrastructures, Key Resources, Key Assets. Risk, Vulnerability, Resilience, Fragility, and Perception Governance, Topics in Safety, Risk, Reliability and Quality, Series 34, eBook ISBN 978-3-319-69224-1, DOI 10.1007/978-3-319-69224-1, Springer International Publishing
84. Gordon, K., Dion, M. (2008) Protection of critical infrastructure and the role of investment policies relating to national security. Divizia de Investiţii din cadrul Directoratului pentru Afaceri Financiare şi ale Întreprinderilor, Organizația pentru Cooperare și Dezvoltare Economică (OECD), [Online], disponibil la https://www.oecd.org/investment/investment-policy/40700392.pdf
85. Hahn, A., Govindarasu, M. (2011) An evaluation of cybersecurity assessment tools on a SCADA environment, in IEEE Power and Energy Society General Meeting, doi: 10.1109/PES.2011.6039845.
86. Hammond, D. (2002) Exploring the Genealogy of Systems Thinking. Syst. Res. Behav. Sci. 2002, 19, 429–43, https://doi.org/10.1002/sres.499
87. Harnish, R. (2017). What It Means To Have A Culture Of Cybersecurity. Forbes, 21 septembrie 2017, https://www.forbes.com/sites/forbestechcouncil/2017/09/21/what-it-means-to-have-a-culture-of-cybersecurity/#189651c4efd1
88. Hatch, B. B. (2018), Defining a Class of Cyber Weapons as WMD: An Examination of the Merits, Journal of Strategic Studies, 11, no. 1 (2018): 43-61, https://doi.org/10.5038/1944-0472.11.1.1657
89. Healy, A. (2016). The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers. Journal of International Affairs, Universitatea Columbia, 1 noiembrie 2016, https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process
90. Helbing, D., (2013). Globally networked risks and how to respond. Nature 497, 51–59. https://doi.org/10.1038/nature12047
91. Hughes, D., Colarik, A.M. (2016), Predicting the Proliferation of Cyber Weapons into Small States, Joint Force Quarterly, 2016, 4th Quarter 2016 (83), pp. 19 - 26 (8), http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-83/Article/969646/predicting-the-proliferation-of-cyber-weapons-into-small-states/
92. Jiang, H. (2018). The Spatial Information Corridor Contributes to UNISPACE+50. Presentation to UN Committee on the Peaceful Uses of Outer Space, 2018, https://www.unoosa.org/documents/pdf/copuos/stsc/2018/tech-08E.pdf
93. Johnsen, S. (2010). Resilience in Risk Analysis and Risk Assessment, in: Moore, T., Shenoi, S. (Eds.), Critical Infrastructure Protection IV, IFIP Advances in Information and Communication Technology. Springer, Berlin, Heidelberg, 2010, pp. 215–227. https://doi.org/10.1007/978-3-642-16806-2_15
94. Johnson, J., Gheorghe, A. (2013) Antifragility Analysis and Measurement Framework for Systems of Systems. International Journal on Disaster Risk Science. 4(4). p.159–168.

95. Jones, J., Olechnowicz, P. (2014) Completing Europe – From the North-South Corridor to Energy, Transportation, and Telecommunications Union. Raport al Atlantic Council și Central European Energy Partners, https://www.atlanticcouncil.org/in-depth-research-reports/report/completing-europe-from-the-north-south-corridor-to-energy-transportation-and-telecommunications-union/
96. Karnouskos, S. (2011) Stuxnet Worm Impact on Industrial Cyber-Physical System Security, IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, pp. 4490–4494, doi:10.1109/IECON.2011.6120048
97. Katina, P. F. (2016a). Systems theory as a foundation for discovery of pathologies for complex system problem formulation. În Masys, A. J. (ed.) (2016) Applications of Systems Thinking and Soft Operations Research in Managing Complexity. Springer, pp. 227–267, ISBN 978-3-319-21106-0
98. Katina, P. F. (2016b). Metasystem pathologies (M-Path) method: phases and procedures. Journal of Management Development. Journal of Management Development 35(10):1287-1301, DOI: 10.1108/JMD-02-2016-0024
99. Katina, P. F., Keating, C. B., Sisti, J. A., Gheorghe, A. V. (2019) Blockchain governance. International Journal of Critical Infrastructures, 2019, vol. 15, issue 2, 121-135, http://www.inderscience.com/link.php?id=98835
100. Katina, P.F., Keating, C.B., Bobo, J.A., Toland, T.S. (2019). A Governance Perspective for System-of-Systems. Systems 2019, 7(4), 54, EISSN 2079-8954, https://doi.org/10.3390/systems7040054
101. Kaur, P., Pawar, N., Ansari, F.T., Samad, R.K. , Gyan Prakash Roy, G. (2021). Docker and its features. International Journal of Computer Science Trends and Technology (IJCST) – Volume 9 Issue 2, Mar-Apr 2021, http://www.ijcstjournal.org/volume-9/issue-2/IJCST-V9I2P17.pdf
102. Keating, C. B., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A. A., Safford, R., Rabadi, G. (2003) System of systems engineering. Engineering Management Journal. 15(3). p.35–44.
103. Keating, C.B., Bradley, J.M., 2015. Complex system governance reference model. International Journal of System of Systems Engineering 6, 33–52.
104. Keating, C.B., Katina, P.F., 2012. Prevalence of pathologies in systems of systems. International Journal of System of Systems Engineering 3, 243–267.
105. 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
106. 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, 263–288.
107. Keating, C.B., Katina, P.F., Bradley, J.M., 2015. Challenges for developing complex system governance, in: IIE Annual Conference. Proceedings. Institute of Industrial and Systems Engineers (IISE), pp. 2943–2952.
108. Kerravala, Z. (2017). Cisco to network engineers: Get comfortable with software. It's here to stay. Network World, 25 mai 2017, https://www.networkworld.com/article/3198474/lan-wan/cisco-to-network-engineers-get-comfortable-with-software-it-s-here-to-stay.html
109. Konkel, A., Przywała, M. (2019) The Digital 3 Seas Initiative - Mapping the challenges to overcome. Institutul Kosciuszko, Varșovia, https://digital3seas.eu/wp-content/uploads/2019/12/digital3seas_initiative_roadmap_report_2018.pdf

110. Lazari, A., Simoncini, M. (2016). Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC, Global Jurist, 16(3), 267-289. doi: https://doi.org/10.1515/gj-2015-0014
111. Lepore, D., Siudak, R. (2019) Cybersecurity leaders and followers in the EU with a focus on the 3 Seas Region. Policy Brief, Institutul Kosciuszko, august 2019, ISSN 1689-9873, https://ik.org.pl/wp-content/uploads/ik_policy-brief_cybersecurity-leaders-and-followers-in-the-eu.pdf
112. Leuprecht, C., Szeman, J., Skillicorn, D.B. (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. Contemporary Security Policy, Vol. 40 (3), 2019, ISSN 1743-8764, pag. 382-407, https://doi.org/10.1080/13523260.2019.1590960
113. Litwak, R., King, M. (2015) Arms Control in Cyberspace?, Wilson Center Policy Brief, https://www.wilsoncenter.org/publication/arms-control-cyberspace
114. Madiega, T.A. (2019) EU guidelines on ethics in artificial intelligence: Context and implementation. Raport al Think Tank-ului Parlamentului European, 19 septembrie 2019, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)640163
115. Maier, M.W. (1996) Architecting Principles for Systems-of-Systems. în 6th Annual INCOSE Symposium; INCOSE: Boston, MA, USA, 1996; p. 567–574., https://doi.org/10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D
116. Maynard, P., McLaughlin, K., Haberler, B. (2014) Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks, in 2nd International Symposium for ICS & SCADA Cyber Security Research 2014. BCS Learning & Development. doi: 10.14236/ewic/ics-csr2014.5.
117. Medin, M., Louie, G. (2019). The 5G Ecosystem: Risks & Opportunities for DoD. Raport Defense Industrial Board, Departamentul Apărării SUA, 3 aprilie 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF
118. 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.
119. Moore, J. (2020). Server hardware guide to architecture, products and management. Tech Target, 16 iunie 2020, https://www.techtarget.com/searchdatacenter/Server-hardware-guide-to-architecture-products-and-management
120. Morgan, S. (2017) 2017 Cybercrime Report. Herjavec Group și Cybersecurity Ventures, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
121. Morgan, S., Carson, J. (2018) The World Will Need to Protect 300 Billion Passwords By 2020. 4 iulie 2018, https://3erczm2x84t2p8xnj226kmxx-wpengine.netdna-ssl.com/wp-content/uploads/sites/4/2018/07/cybersecurity-ventures-thycoti_70778.pdf
122. Morgus, R., Smeets, M., Herr, T. (2017), Countering the proliferation of offensive cyber capabilities, in Global Commission on the Stability of Cyberspace (2018), Briefings from the Research Advisory Group, GCSC Issue Brief No. 1, pag. 161-187, New Delhi, noiembrie 2017, https://cisac.fsi.stanford.edu/publication/countering-proliferation-offensive-cyber-capabilities
123. Morris, T., Gao, W. (2013) Industrial Control System Cyber Attacks, ICS-CSR 2013, Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research

2013, pp. 22–29, ISBN: 978-1-780172-32-3, http://ewic.bcs.org/content/ConMediaFile/22618
124. Moteff, J.D., Copeland, C., Fischer, J.W. (2002). Critical Infrastructures: What Makes an Infrastructure Critical?. UNT Digital Library, 2002. https://digital.library.unt.edu/ark:/67531/metacrs3176/
125. Mureşan, L., Georgescu, A. (2017) Non dimenticate il Mar Nero! La Romania e il Trimarium. Limes Revista Italiana di Geopolitica, Available online at https://www.limesonline.com/cartaceo/non-dimenticate-il-mar-nero-la-romania-e-il-trimarium
126. Mureşan, L., Georgescu, A. (2019). A Critical Infrastructure Perspective on the Belt and Road Initiative and its Opportunities and Challenges". în Yang Jiemian, Zarko Obradovic (2019), "The Belt and Road and Central and Eastern Europe", p. 205-228, Shanghai Foreign Language Education Press, ISBN 978-7-5446-5465-4
127. National Institute for Standards and Technology, Joint Research Centre (2012) The Benefits of U.S.-European Security Standardization. NISTIR 7861, June 2012, http://dx.doi.org/10.6028/NIST.IR.7861
128. 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.
129. 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, februarie 2019, https://www-west.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
130. OECD (2018). The Belt and Road Initiative in the global trade, investment and finance landscape. în OECD Business and Finance Outlook 2018, OECD Publishing, Paris, https://doi.org/10.1787/bus_fin_out-2018-6-en
131. Organisation for Economic Cooperation and Development (2016) International Regulatory Co-operation: The Role of International Organisations in Fostering Better Rules of Globalisation. OECD, 2016, ISBN 978-92-64-24404-7, DOI:https://dx.doi.org/10.1787/9789264244047-en
132. Osawa, J. (2017), The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?, Asia Pacific Review 24(2):113-131, iulie 2017, DOI: 10.1080/13439006.2017.1406703
133. Perrow, C. (1999) Normal Accidents: Living with High-Risk Technologies, Princeton University Press, ISBN: 9781400828494
134. Pescaroli, G., Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat Hazards 82, 175–192. https://doi.org/10.1007/s11069-016-2186-3
135. PwC (2019), Global Economic Crime and Fraud Survey 2018 – A front line perspective on fraud in Romania, https://www.pwc.ro/en/services/advisory/forensic-services1.html
136. Rayapati, V. (2019). Next Generation Military Satellites with Built-in Cyber Security Implementation: A Case Study & Recommendations, prezentare ăn cadrul NATO ARW pe tema Space Critical Infrastructures: from Risk to Resilience, Norfolk, 23 mai 2019.
137. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine 21, 11–25. https://doi.org/10.1109/37.969131

138. Rockefeller, Arup (2014). Rockefeller: City Resilience Index, Rockefeller Foundation and Arup Development Group, 2014. https://www.arup.com/perspectives/themes/cities/city-resilience-index
139. Rogers, J., Foxall, A., Henderson, M., Armstrong, S. (2020). Breaking the China Supply Chain: How the 'Five Eyes' can Decouple from Strategic Dependency. Henry Jackson Society, 14 mai 2020, https://henryjacksonsociety.org/publications/breaking-the-china-supply-chain-how-the-five-eyes-can-decouple-from-strategic-dependency/
140. Rosenstein, R. (2017) Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit, discurs, Departamentul de Justiție, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit
141. Seely, B., Varnish, P., Hemmings, J. (2019) Defending our Data: Huawei, 5G and the Five Eyes. Henry Jackson Society, 16 mai 2019, https://henryjacksonsociety.org/publications/defendingourdata/
142. Site Connect44, https://www.connect44.com/5g-engineering-service
143. Slaughter, A. M. (2004) A New World Order. Princeton; Oxford: Princeton University Press. doi:10.2307/j.ctt7rqxg
144. Smeets, M. (2018), Integrating offensive cyber capabilities: meaning, dilemmas, and assessment, Defence Studies 18(1):1-16, August 2018, scris ca Smeets (2018b), DOI: 10.1080/14702436.2018.1508349
145. Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations, Strategic Studies Quarterly, august 2018, scris ca Smeets (2018a), https://www.ctga.ox.ac.uk/article/strategic-promise-offensive-cyber-operations
146. Sousa-Poza, A. A., Kovacic, S., & Keating, C. B. (2008), "System of systems engineering: An emerging multidiscipline", Jurnalul internațional al ingineriei sistemelor-de-sisteme, 1(1/2), 1–17.
147. Steer Davies Gleave (2018). The new Silk Route – opportunities and challenges for EU transport. Research for TRAN Committee, Policy Department for Structural and Cohesion Policies, Parlamentul European, Bruxelles, IP/B/TRAN/IC/2017-006, PE 585.907, ISBN 978-92-846-0555-2, ianuarie 2018, doi:10.2861/349796
148. Stevens, J. (2018), Internet Stats and Facts for 2018, Hosting Facts, 10 iulie 2018, https://hostingfacts.com/internet-facts-stats-2016/
149. Tatar, U., Geers, K., Georgescu, A. (2017). "A Framework for a Military Cyber Defence Strategy Workshop– Final Report", in Tatar, U., Gokce, Y., Gheorghe, A., (2017), "Strategic Cyber Defense - a Multidisciplinary Perspective", IOS Press, NATO SPS Series D Vol. 48, ISBN 978-1-61499-770-2
150. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D. (2009), Risk Based Critical Analysis. In Palmer, C.C. & Shenoi, S. (eds.). Critical Infrastructure Protection III - Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. IFIP Advances in Information and Communication Technology Series (311). Hanover, New Hampshire, SUA: Springer, ISBN 978-3-642-04797-8
151. Triantaphyllou (2012). The Uncertain Times of Black Sea Regional Security. Euxeinos nr. 6, p. 4-10, Center for Governance and Culture in Europe, 2012, ISSN 2296-0708, https://gce.unisg.ch/en/euxeinos/archive/06
152. Turan, M.S., Barker, E., Burr, W., Chen, L. (2010). NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation. National Institutes for Standards and

Technologies, SUA, disponibil la https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf
153. Turnbull, J. (2014). The Docker Book: Containerization is the new virtualization. B00LRROTI4
154. Union of Concerned Scientists (2019) UCS Satellite Database, accesat 5 mai 2020, https://www.ucsusa.org/resources/satellite-database
155. Vugrin, E.D., Warren, D.E., Ehlen, M.A., 2011. A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Safety Progress 30, 280–290. https://doi.org/10.1002/prs.10437
156. Wiener, J. B., Alemanno, A. (2015) The Future of International Regulatory Cooperation: TTIP as a Learning Process Toward a Global Policy Laboratory. 78 Law and Contemporary Problems 103-136, https://scholarship.law.duke.edu/lcp/vol78/iss4/5
157. Young, A. R. (2015) The European Union as a global regulator? Context and comparison. Journal of European Public Policy 22(9), pp. 1233-1252, https://doi.org/10.1080/13501763.2015.1046902
158. Zdrojowy, E., Kurasz, J., Gołebiewski, M., McMillan, J. (2017). The Road Ahead – CEE Transport Infrastructure Dynamics. PWC & Atlantic Council, https://www.pwc.pl/pl/pdf/the-road-ahead-raport-pwc-atlantic-council.pdf
159. Zhu, B., Joseph, A., Sastry, S. (2011) A Taxonomy of Cyber Attacks on SCADA Systems, in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. IEEE, pp. 380–388, doi: 10.1109/iThings/CPSCom.2011.34
160. Żurawski vel Grajewski, P. (2017) Trimarium: A View from the North. In Redlowska, K. (ed.) (2017) Adriatic – Baltic – Black Sea: Visions of Cooperation, Institute for Eastern Studies, Warsaw, http://www.forum-ekonomiczne.pl/wp-content/uploads/2017/08/Adriatyk-Ba%C5%82tyk-Morze-Czarne16x24_2017en_PDF.pdf