UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

Facultatea de Istorie și Filosofie
Str. M. Kogălniceanu nr. 1
Cluj-Napoca, 400084
Tel.: 0264 405 300 int.5275
Fax: 0264 405 326
hiphi@ubbcluj.ro
hiphi.ubbcluj.ro

”BABEȘ-BOLYAI” UNIVERSITY, CLUJ-NAPOCA

FACULTY OF HISTORY AND PHILOSOPHY

DOCTORAL SCHOOL *INTERNATIONAL RELATIONS AND SECURITY STUDIES*

Cybersecurity of Critical Infrastructure in International Relations. Case study: The health sector in Romania

PhD THESIS SUMMARY

Scientific adviser

Univ. Prof. Dr. ADRIAN-LIVIU IVAN

PhD student

DARIUS-ANTONIU FERENȚ

Cluj-Napoca

2026

TABLE OF CONTENTS

Keywords: cybersecurity, critical infrastructure, IT&C infrastructure, ransomware, information system, cyberwarfare, cyber defense, national security, international security, cyber power, security culture, cybercrime, Man-in-the-Middle.

Cybersecurity is currently a concern for individuals, organizations, companies, and states, and cyberattacks on critical infrastructures are a constant and serious issue for national security. The research topic falls within the vast field of security studies, located on the border between this area and the sciences in the field of IT&C (Information Technology and Communication).

In national and international specialized literature, cybersecurity has a multitude of definitions. However, I chose to use the following definition in the research: cybersecurity is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." [1]

In scientific research I used both quantitative and qualitative methods. An advantage of quantitative research is that the entire scientific endeavor is verifiable and becomes objective and legitimate. Quantitative research is scientifically useful because it develops concrete information and involves testing research hypotheses and/or theories, identifying relationships between variables, and drawing a forecast based on true results. [2] Adherents of the quantitative method frequently look for correlations between variables but are usually reluctant to move from correlational to causal statements because the sheer complexity of social life makes it difficult to be absolutely certain that a particular variable is the sole cause of a particular phenomenon.[3]

The quantitative research was based on the creation of a questionnaire, through which to highlight the level of cybersecurity culture of the employees of the Cluj-Napoca County Emergency Clinical Hospital (SCJU Cluj). We also studied some of the specialized literature that addresses the field of cyber security. The qualitative research was based on the realization of a case study, in which we demonstrated that ransomware cyberattacks launched by cybercrime groups are very dangerous for organizations, and the development of the cybersecurity culture of end users/employees within medical institutions in Romania is an essential condition to prevent a ransomware attack from materializing. The quantitative-qualitative methodological mix is the most appropriate approach to

[1] International Telecommunication Union (ITU-T), *Series X: Data networks, open system communications and security. Telecommunication security*, Overview of cybersecurity, ITU-T X.1205, April 2008, p.2.
[2] Edward Barroga, Glafera Janet Matanguihan, „A Practical Guide to Writing Quantitative and Qualitative Research Questions and Hypotheses in Scholarly Articles", in *Journal of Korean Medical Science*, April 12, 2022, available at https://jkms.org/pdf/10.3346/jkms.2022.37.e121, accessed on August 25, 2023.
[3] Charles Ragin, Lisa Amoroso, *Constructing Social Research. The Unity and Diversity of Method*, Thousand Oaks, London, 2011, p.4.

the subject of this paper. The main advantage of this method concerns the representativeness of the obtained data. They best represent the opinion of the entire population under investigation. A limitation of the research method is the aggregation of the opinions of people with different experiences regarding the use of computer equipment and their cybersecurity.

Taking into consideration the high interest of institutions, companies, states and international organizations to ensure the cybersecurity of the information technology infrastructure and the small number of scientific researches in the Romanian space that address the issue of cybersecurity in national and European infrastructures in the health sector, I opted for a methodological device that allowed me to effectively combine theoretical and scientific aspects in the field of security studies with an empirical research based on case studies and specialized analyses, carried out by studying primary, secondary and tertiary sources. In order to obtain relevant data, I took into consideration the exploration of causal relationships and the interdependence between risks, threats and phenomena in cyberspace, the realization of SWOT analyses, the use of structural and comparative analysis, tools that favored scientific objectivity. I considered it appropriate that a large part of this work should be based on a consistent empirical foundation, which would clearly emphasize the novelty of the research and the personal contribution brought to the development of the fields of studies of security and international relations.

In order to achieve the research objectives of this work, I used both specialized books in the fields of cybersecurity, international relations, and security studies, as well as valuable scientific articles that address the issue of critical cyber infrastructure security and cybercrime.

The original elements of my research are represented by the exposure of a potential matrix through which cyberattacks could be identified and their classification according to intensity and impact. In the same note of originality, the present study presented the "picture" of a cybersecurity diagnosis of the IT&C infrastructure and information systems within the Cluj-Napoca County Emergency Clinical Hospital, based on the data and information collected regarding the IT&C systems and the network of institution computers (only non-confidential data for said organization was collected). In addition, we determined the level of cybersecurity culture of SCJU Cluj-Napoca employees.

I also developed a SWOT analysis of the operating mode (*modus operandi*) of a domestic cybercrime group that launched cyberattacks (with minor impact) and wanted to affect the IT&C infrastructure of some medical institutions in Romania, by carrying out ransomware-type attacks (cyberattacks with major impact). The chosen group was PentaGuard. At the same time, I highlighted a *modus operandi* of hackers who launch MitM (Man-in-the-Middle) cyberattacks, because the results of the questionnaires applied to the employees of the Cluj-Napoca County

Emergency Clinical Hospital, showed that the cyber terminals of these users are vulnerable to Man-in-the-Middle attacks.

I also defined the three types of infrastructures on the territory of Romania (ordinary infrastructures, special infrastructures, and critical infrastructures), aiming to formulate definitions as exhaustive as possible, which was not found in the specialized literature, related to the fields of studies of security and international relations.

In the paper, I demonstrated that the cyber power of a state actor refers to its cyber defense capabilities, but also to the offensive capacities and capabilities necessary to conduct operations in the adversary's computer networks, including cyber espionage, the ability to compromise data networks and IT&C systems of the enemy and to take administrator control over cyber terminals through rootkits or trojans. In addition, I made graphical representation of the place of cyberwarfare in the gradation of the intensity of cyberattacks. In cyberwarfare, a state actor can affect the national security of an adversary by disrupting, for a period of time, the operation of an essential or critical infrastructure component (for example, the IT systems of healthcare institutions).

Security has become a necessary ingredient in many sectors of activity and has evolved in the last decade as a response to the risks and threats generated by the globalization of contemporary society. The rapid evolution of technologies has brought to the attention of specialists, practitioners and political decision-makers concepts such as protection of critical cyber infrastructures, borderless security, cloud computing, and electronic information security[4].

There are numerous academic debates and discussions about these dimensions/sectors of security, and any new perspective and scientific research determines new discoveries and implications for the security of individuals, human communities and states. This can be explained by the nature and diversity of security risks and threats. The five dimensions or sectors identified by Barry Buzan play an analytical role, following the decomposition of the „national security of states" into smaller elements, making it easier to discuss, depending on what a society considers dangerous[5]. The national security of a state must be viewed at all levels: the military defense of the country, energy security, economic security, public order and safety, or cyber security of special and critical infrastructures.

The 21st century is characterized by the implementation of cyber security in the national security agenda of states, being seen as a vital pillar in maintaining the *status quo* of a state actor[6].

4 Tiberiu Tănase (coord.), Șerban-Dan Predescu, Petru Ștețcu, *Managementul securității informațiilor - suport de curs*, Editura Concordia, Arad, 2022, p.86.

5 J Baylis, „International and global security", *The Globalization of World politics An introduction to international relations*, Sixth edition, Baylis, Smith, Owens (coord.), Oxford University, 2014, p.231.

6 Ionela Maria Ciolan „Defining cybersecurity as the security issue of the twenty first century. A constructivist approach", în The Public Administration and Social Policies Review, VI, 1(12), iunie 2014, p.122, disponibil la https://revad.uvvg.ro/files/nr12/8.Ionela_Ciolan.pdf, accesat în 22 iulie 2023.

States' national security tends to be seen as a responsibility of governments and depends on internal and external policies, military capabilities, as well as the effectiveness of intelligence services in the area of conducting intelligence-operational actions and processing information, to obtain the analytical intelligence product. However, the protection and security of a country's critical infrastructures must be seen as a shared responsibility between states, because a single government cannot fully ensure the necessary protection of these categories of infrastructures[7]. In addition, both supporting the commitment of non-state actors (firms, companies, institutions, organizations, individuals) in ensuring the security of their own computer networks, and national and international attempts to protect cyberspace, are of equal importance[8].

Joseph Nye offers a description of the distribution of power between nations, which he analyzes as a complex „three-dimensional chess game". The three chessboards are represented by a different state actor, each emphasizing a different dimension. In Joseph Nye's vision, the first chessboard is represented by the military dimension, which is predominantly unipolar, being concentrated on a single pole of power (the USA). The middle chessboard is represented by the economic dimension, which is multipolar, with power being distributed among several state actors or poles of power (the USA, the European Union, Japan and China). The third chessboard is represented by the dimension of transnational relations, which has crossed the national borders of states and escaped government control, including state actors of various types, among them cybercrime groups or hackers[9].

In his book *The Future of Power* (2011), Joseph Nye makes several new clarifications and additions, compared to the ideas mentioned a year ago, in the work *Cyberpower*. We appreciate that the changes brought by the author are consistent with the developments in the international security environment specific to the 21st century. Nye emphasizes the idea of the diffusion of power, especially „cyberpower", to other actors, besides the nation state[10]. „Cyberpower is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain."[11] In view of the above, it is necessary to update the "complex three-dimensional chess game", introducing the concept of cyber warfare, defined by Paul Robinson as "warfare waged via computers and the Internet. It includes both offensive measures designed to cause damage opponents' information systems and defensive measures, to protect one's own systems from hostile

7 J. Eriksson, G. Giacomello, „The Information Revolution, Security and International Relations: (IR)relevant Theory?", în International Political Science Review, 27(3), 2006, pp.221-244.

8 Ionela Maria Ciolan, op.cit., p.132.

9 Joseph Nye, „Cyber Power", Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, mai 2010, disponibil la https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf, accesat în 22 iulie 2023.

10 Joseph Nye, Viitorul puterii, Editura Polirom, Iași, 2012, p.113.

11 Ibidem, p.123.

attack"[12]. Joseph Nye also believes that the most visible change is taking place in the areas of application of the third level. Consequently, cyberspace is becoming increasingly relevant, bringing with it implications for international politics.

We consider that the cyberpower of a state refers to the cyber defense capabilities, but also to the offensive capacities and capabilities necessary to conduct operations in the computer networks of the adversary, including cyber espionage, the ability to compromise enemy networks and ICT systems and to gain administrative-level control over computer devices or systems, through rootkits or trojans. Cyberpower is a security resource for states, along with political, military, diplomatic, economic-financial or informational power. The capacity of the armed forces to carry out a complex set of defensive and offensive actions on ICT systems and data networks is one of the determinants of state power.

By using the technical support of information and communications technology, a pragmatic change occurs in the configuration of power relations between non-state actors and states, resulting in a war in the realm of virtual reality (a cyber war) that may target states' critical infrastructures (electricity distribution systems, industrial and defense industry facilities, government communications, the financial-banking system or medical services)[13].

Kenneth Waltz mentions that interdependence is a relationship between equals[14]. When the parties are not equal in the cyber sphere, there may be a degree of dependence and, at the same time, vulnerability, since the relationship between the actors is not balanced[15]. The skepticism and distrust of states are enhanced by several factors. One of these refers to the fact that state actors have different capabilities in the cyber domain. Some states focus their efforts and economic and financial resources on the development, at the level of the armed forces, of cyber defense capabilities and capabilities, as well as capabilities necessary for conducting operations in the computer networks of a potential enemy. Although some cyber-attacks are launched by individual hackers and cybercrime groups, there are also attacks or operations in cyberspace carried out by hacker groups supported by state actors. In this sense, several examples can be given: cyber-attacks targeting the critical infrastructure of some states, a state actor's involvement in another state's domestic politics, the theft of intellectual property or the sabotage of an entity (the case of North Korea with Sony Pictures)[16].

12 Paul Robinson, Dicționar de securitate internațională, Editura CA Publishing, Cluj-Napoca, 2010, p.164.

13 Gheorghe Arădăvoaice, Valentin Stancu, Războaiele de azi și de mâine - agresiuni neconvenționale, Editura Militară, București, 1999, p.43.

14 Kenneth Waltz, Theory of International Politics, Editura Waveland Press, Long Grove, 2010, p.144.

15 Brandon Valeriano, Ryan C. Maness, Cyber war versus cyber realities: cyber conflict in the international system, Editura Oxford University Press, Oxford, 2015, p.13.

16 Richard Haass, Lumea în care trăim. O scurtă introducere, Editura Nemira, București, 2021, p.257.

Although North Korea is an economically poor country, it has quite sophisticated cyber capabilities and capacities[17].

The infrastructure on the territory of Romania falls into 3 classes: critical infrastructures, special infrastructures, ordinary infrastructures[18].

Next, we want to define the 3 types of infrastructure as exhaustively as possible, to highlight the links that can be established between them and the functional characteristics of each type of infrastructure, in close correlation with the national security area.

We consider that ordinary infrastructures refer to structures, constructions, which ensure the proper functioning of economic, financial, social, cultural, military, and administrative systems. The category of ordinary infrastructures includes those systems and components of systems that do not require special security and protection measures. These infrastructures ensure the maintenance of certain functions of society, being necessary for people and communities. In the event of disruption or cessation of their functioning, for a short period of time, economic, social, political, and military processes are not significantly affected. This category includes schools, libraries, and roads that are not of major importance for the field of civil or military transport (rural roads). These infrastructures may become special or critical, for a determined period of time, depending on the social, economic and military developments in certain regions or areas of the country.

Special infrastructures can make an important contribution to the functionality of economic, social, political, military, financial systems or processes. In the event of their disruption, social and economic stability may be affected, without jeopardizing the overall functioning of systems and processes assimilated to the economic, social, military, political, and informational sectors. An airfield built in a locality may be classified in this category depending on its importance within a process (commercial, military transport), the security vulnerabilities identified, or potential threats that could render it non-functional for a short time. Depending on the consequences that the disruption or shutdown of the functioning of a subsystem could have on the functioning of processes and systems, it will also be classified in the category of critical infrastructures, for a determined or indefinite period.

Critical infrastructures represent a system or subsystem that is important for maintaining vital functions of society, their disruption and/or destruction being felt at local, regional or national level, significantly affecting the proper functioning of social, financial, economic, military processes, some damage and dysfunctions even endangering national security. These infrastructures require special

17 Ibidem, p.258.

18 Grigore Alexandrescu, Gheorghe Văduva, Infrastructurile critice: pericole, amenințări la adresa acestora; sisteme de protecție, Editura Universității Naționale de Apărare „Carol I", București, 2006, p.6.

security and protection measures, because the disruption of their functioning, even for a short time, can produce negative effects at social, economic, financial, and military levels: International airports, strategic military bases, the national power grid, the state border, high-speed roads (motorways, expressways), strategic roads from a military point of view (facilitate the rapid movement of armed forces and military equipment), important sea and river ports (along with their related infrastructure), hydroelectric power plants with installed capacity of hundreds and thousands of MW, large thermal power plants of regional importance (the Rovinari and Turceni thermal power plants are of regional importance and can be classified as critical infrastructure), nuclear power plants, ammunition, fuel and weapons depots, national telephone networks, relays, computer networks (metropolitan networks, wide area networks), IT systems and services, oil and gas pipelines, hospitals of regional importance.

==========

SELECTIVE BIBLIOGRAPHY:

I. Official documents from electronic sources:

1). „Executive Order EO 13010 Critical Infrastructure Protection, July 15, 1996, available at https://fas.org/irp/ offdocs/eo13010.htm.

2). Hotărârea Guvernului nr. 585/2002, pentru aprobarea standardelor naționale de protecție a informațiilor clasificate în România, in *Monitorul Oficial al României*, Part I, no. 485, July 5, 2002.

3). UNODC, „Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation", http://www.unodc.org/documents/congress//Declaration/V1504151_English.pdf.

4). *Declarația Summit-ului NATO din Țara Galilor*, Paragraph 72, available at https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

5). Cybercrime Convention Committee (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, Strasbourg, July 2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

6). Official site of Administrația Prezidențială: *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*, Bucharest, 2020, available at https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

7). Guvernul României, *Strategia de Securitate Cibernetică a României din 30 decembrie 2021, pentru perioada 2022-2027*, January 3, 2022, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235.

II. Legislation:

1). „Ordonanța de urgență nr. 61/2019 pentru modificarea și completarea Ordonanței de urgență a guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice", August 30, 2019, available at https://lege5.ro/Gratuit/gm2deojsg4zq/ordonanta-de-urgenta-nr-61-2019-pentru-modificarea-si-completarea-ordonantei-de-urgenta-a-guvernului-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.

2). „Legea nr. 255/2018 pentru modificarea și completarea Ordonanței de urgență a guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice", August 3, 2018, available at https://lege5.ro/Gratuit/gi4tamrrg44a/legea-nr-225-2018-pentru-modificarea-si-completarea-ordonantei-de-urgenta-a-guvernului-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.

3). „Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică", May 23, 2013, available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf.

4). "Prevenirea și combaterea criminalității informatice - Legea nr. 161/2003", available at https://lege5.ro/gratuit/hezdgobv/prevenirea-si-combaterea-criminalitatii-informatice-lege-161-2003?dp=giztimztg4ytk.

5). "Regulamentului General european 2016/679 privind protecția datelor cu caracter personal (GDPR)", Article 32 - *Securitatea prelucrării*, available at https://www.privacy-regulation.eu/ro/32.htm.

6). „Noul Cod Penal actualizat 2024 - Legea 286/2009", https://legeaz.net/noul-cod-penal/.

7). The Legislative Portal of the Ministry of Justice: „Legea nr.58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative".

III. Reports and newsletters:

1). International Telecommunication Union (ITU-T), Series X: *Data networks, open system communications and security. Telecommunication security, Overview of cybersecurity,* ITU-T X.1205, April 2008.
2). Check Point Research Team, „Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks", January 5, 2023, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks.
3). Official site of the Romanian Intelligence Service: *Protecția infrastructurilor critice,* disponibil la https://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf.
4). Romanian Intelligence Service, *Buletin Cyberint - semestrul 1 (2022)*, available at https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2022-RO.pdf.
5). Romanian Intelligence Service, *Buletin special Cyberint în contextul COVID-19*, available at https://www.sri.ro/assets/files/publicatii/buletin-special-covid-cyber-2020.pdf.
6). Romanian Intelligence Service, *Buletin Cyberint*, *nr.2 - 2021*, available at https://www.sri.ro/assets/files/publicatii/buletin-cyber-nr2.pdf.
7). Official site of the Romanian Intelligence Service: *Ghid de bune practici pentru securitate cibernetică*, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf.
8). Centrul de Management și Transfer Tehnologic și Cognitiv, Universitatea Babeș-Bolyai, *QTSTRAT Newsletter*, no. 1, December 2021.
9). Center for Management and Technological and Cognitive Transfer, Babeș-Bolyai University, *QTSTRAT Newsletter*, no. 3.
10). Center for Management and Technological and Cognitive Transfer, Babeș-Bolyai University, *QTSTRAT Newsletter*, no. 5.
11). General Secretariat of the Council of the European Union, *EMPACT 2022 Results, Factsheets*, 2023, available at https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf.
12). EU Agency for Criminal Justice Cooperation, *Annual Report 2022: Criminal Justice across borders*, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2022-en.pdf.
13). Official site of EUROPOL: *The European Union Agency for Law Enforcement Cooperation*, Luxembourg: Publications Office of the European Union, 2022, available at https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20in%20Brief.pdf.
14). Official site of Council of Europe: „Council of Europe action against Cybercrime", available at https://www.coe.int/en/web/portal/coe-action-against-cybercrime.
15). United Nations Office at Vienna, Centre for Social Development and Humanitarian Affairs, *International Review of Criminal Policy, Nos. 43 and 44, 1994, United Nations Manual on the*

prevention and control of computer-related crime, available at https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF.
16). Council of the European Union, *Cybersecurity: how the EU tackles cyber threats*, last update January 11, 2023, https://www.consilium.europa.eu/en/policies/cybersecurity/.
17). Institute for Security and Technology, *Combating Ransomware. A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, available at https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.
18). IBM Security, *Cost of a Data Breach - Report 2022*, July 2022, United States, available at https://www.ibm.com/downloads/cas/3R8N1DZJ.
19). Matt Ahlgren, „Peste 50 de statistici, fapte și tendințe în domeniul securității cibernetice pentru 2023", August 2023, https://www.websiterating.com/ro/research/cybersecurity-statistics-facts/.
20). The Engine Room, Internews, *Case study: Watering hole attacks*, June 2020, available at https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-Watering-Hole-Junio-2020.pdf.

IV. Specialized works (Books):

1). ABLON, Lillian, BOGART, Andy, *Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, Santa Monica, 2017.
2). ALEXANDRESCU, Grigore, VĂDUVA, Gheorghe, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare Carol I, Bucharest, 2006.
3). ARĂDĂVOAICE, Gheorghe, STANCU, Valentin, *Războaiele de azi și de mâine - agresiuni neconvenționale*, Editura Militară, Bucharest, 1999.
4). BARBU, Alida Monica Doriana, *Inteligența artificială: cum vor schimba AI, Deep Learning și robotica domeniul militar*, Editura Militară, Bucharest, 2023.
5). BAYLIS, John, SMITH, Steve, OWENS, Patricia (coord.), *The Globalization of World Politics: an introduction to international relations*, Sixth edition, Oxford University Press, Oxford, United Kingdom, 2014.
6). BLOKDYK, Gerardus, *SWOT Analysis - A Complete Guide*, The Art of Service - SWOT Analysis Publishing, 2021.

7). CHAWKI, Mohamed, DARWISH, Ashraf, KHAN, Mohammad Ayoub, TYAGI, Sapna, *Cybercrime, Digital Forensics and Jurisdiction*, Studies in Computational Intelligence, Volume 593, Springer International Publishing, 2015.
8). CLARKE, Justin et all., *SQL Injection Attacks and Defense*, Syngress Publishing, Burlington, 2009.
9). CURELEA, Mihai Bogdan, ȘTEȚCU, Petru, *Criminalistica*, Editura Concordia, Arad, 2023.
10). DEAC, Aron Liviu, IRIMIA, Ion, *Securitate și apărare națională - culegere de lecții*, Editura Academiei de Înalte Studii Militare, Bucharest, 1999.
11). ELISAN, Christopher C., *Advanced Malware Analysis*, McGraw-Hill Education, New York, 2015.
12). FINE, Lawrence, *The SWOT Analysis: Using your Strength to overcome Weaknesses, using Opportunities to overcome Threats*, CreateSpace Independent Publishing Platform, 1st edition, 2010.
13). FREEDMAN, Lawrence, *Viitorul războiului: o istorie*, Editura Litera, Bucharest, 2019.
14). FERENȚ, Darius-Antoniu, *Introducere în securitatea cibernetică*, Editura Limes, Florești, 2023.
15). GERCKE, Marco, International Telecommunication Union, *Understanding cybercrime: Phenomena, challenges and legal response*, Geneva, 2014.
16). GOODMAN, Marc, *X-Cyber: viitorul începe azi*, Editura RAO, Bucharest, 2016.
17). GOLDSTEIN, Joshua S., PEVEHOUSE, Jon C., *International Relations*, Tenth edition, Pearson Publishing, 2014.
18). GRAHAM, James, HOWARD, Richard, OLSON, Ryan, *Cyber Security Essentials*, CRC Press Taylor&Francis Group, New York, 2011.
19). GRIFFITHS, Martin (ed.), *International Relations Theory for the 21st Century: An Introduction*, Routledge, London, New York, 2007.
20). HAASS, Richard, *Lumea în care trăim. O scurtă introducere*, Editura Nemira, Bucharest, 2021.
21). HIRST, Paul, *Război și putere în secolul XXI. Statul, conflictul militar și sistemul internațional*, Editura Antet, 2003.
22). HOFSTEDE, Geert, HOFSTEDE, Gert Jan, MINKOV, Michael, *Culturi și organizații: softul mental. Cooperarea interculturală și importanța ei pentru supraviețuire*, Editura Humanitas, Bucharest, 2012.
23). IONIȚĂ, Gheorghe-Iulian, *Infracțiunile din sfera criminalității informatice*, Editura Universul Juridic, Bucharest, 2018.
24). JENKINSON, Andrew, *Ransomware and Cybercrime*, CRC Press, Taylor&Francis Group, Londra, 2022.

25). KATZ, Jonathan, LINDELL, Yehuda, *Introduction to Modern Cryptography*, 2nd edition, CRC Press, Taylor & Francis Group, 2015.
26). LUCAS, George, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*, Oxford University Press, New York, 2017.
27). KEYTON, Joann, *Communication and Organizational culture: A Key to Understanding Work Experiences*, Sage Publications, 1st edition, 2005.
28). LISKA, Allan, GALLO, Timothy, *Ransomware: Defending Against Digital Extortion*, O'Reilly Media, Sebastopol, USA, 2017.
29). MANCI, Ioan, PREJA, Corneliu, *Introducere în studii de securitate și strategice*, Editura CA Publishing, Cluj-Napoca, 2014.
30). MEARSHEIMER, John, *The Tragedy of Great Power Politics*, W.W. Norton & Company, London, 2014.
31). MELINESCU, Nicolae, *Noțiuni introductive pentru studiul relațiilor internaționale*, Editura CA Publishing, Cluj-Napoca, 2014.
32). MIROIU, Andrei, UNGUREANU, Radu-Sebastian, BIRO, Daniel, DÎRDALĂ, Lucian-Dumitru, TODEREAN, Olivia, *Manual de relații internaționale*, Editura Polirom, Iași, 2006.
33). NIEBUHR, Reinhold, *Moral Man and Immoral Society. A Study In Ethics and Politics*, Presbytherian Publishing Corporation, 2021.
34). POPA, Eliza-Tatiana, TĂNASE, Tiberiu, *Riscuri și amenințări ale mileniului III - Volumul 1*, Editura Concordia, Arad, 2022.
35). PREJA, Amos Corneliu, BOGDAN, Ioan, *Introducere în teoria generală a informației și studii de intelligence,* Editura CA Publishing, Cluj-Napoca, 2017.
36). ROBINSON, Paul, *Dicționar de securitate internațională*, Editura CA Publishing, Cluj-Napoca, 2010.
37). RYAN, Matthew, *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, Springer, Cham, Switzerland, 2021.
38). SFETCU, Nicolae, *Beginner's Guide for Cybercrime Investigators*, Editura MultiMedia Publishing, Bucharest, 2014.
39). SFETCU, Nicolae, *Introducere în inteligența artificială*, Editura MultiMedia Publishing, Bucharest, 2021.
40). SFETCU, Nicolae, *Amenințările persistente avansate în securitatea cibernetică. Războiul cibernetic*, Editura MultiMedia Publishing, Bucharest, 2024.
41). SHIMONSKI, Robert, *AI in Healthcare: How Artificial Intelligence Is Changing IT Operations and Infrastructure Services*, Wiley, 2021.

42). TĂNASE, Tiberiu, ȘTEȚCU, Petru, *Investigarea infracțiunilor informatice*, Editura Concordia, Arad, 2021.
43). TANCO, Alexandru (coord.), NERON, Mircea, ȘTEȚCU, Petru, *Prevenirea și combaterea infracționalității*, Editura Concordia, Arad, 2023.