Cyber Conflict: Indicators and Assessments

Serghei Ohrimenco[1] Valeriu Cernei[2]

Abstract

Introduction: The history of interactions between states, nations, and alliances of countries dates back thousands of years. These relationships typically progress through several stages, including cooperation, integration, competition, and confrontation. It's important to recognize that these stages encompass a wide array of aspects, including politics, military affairs, finances, technology, society, and ideology. Interaction and confrontation occur at various levels, ranging from global and strategic to tactical and individual. This paper primarily focuses on the stage of confrontation within the relatively new and not yet fully explored realm of cyberspace.

Aim: The aim of this research is to study the cyber domain category and determine the possibilities and peculiarities of information interaction (cyber conflicts, cyber blockades, and cyber sanctions). It also involves analyzing existing models and basic assessment indicators characterizing the level of information technology development in individual countries.

Method: A systematic approach was employed, consisting of several stages, including the formation of the conceptual foundations of the cyber domain, gathering statistical information from scientific and monographic literature, research reports, and data processing and analysis using game theory, econometric analysis, and economic-mathematical modeling.

Findings: A comprehensive study of the nature of cyber conflicts can significantly enhance the process of multilateral cooperation. Future research on conflict dynamics and existing conflict management mechanisms requires further investigation of information security threats and risk management.

Originality and value: Statistics have been collected characterizing the National Cyber Security Index and Global Cybersecurity Index 2020: Country profiles of several countries, including Turkiye, Bulgaria, Romania, Moldova, Ukraine, and Russia. An attempt has been made to correlate the level of Cyber-Dependent Crimes with the level of cyber domain protection.

Key Words: CyberSpace Domain, Cyber Attacks, Cyber Conflict, Cyber Blockade, Cyber Sanctions
Jel Codes: D74 D81 E26 F51 K24

1. INTRODUCTION

The significance of this topic lies in each state's imperative to safeguard its national interests in the realm of cybersecurity. It's important to underscore the distinctions between the cyber domain and other domains, as emphasized in Brantly's work from 2016 (Brantly, 2016). First and foremost, cyberspace is a human-made domain. Secondly, the management of military and civilian capabilities in other domains relies on and operates through the cyber domain. Third, the military and civilian facets of cyber operations are intricately interwoven, making it challenging, and at times impossible, to differentiate between them. Fourth, establishing the attribution of operations in cyberspace is a very difficult and complex task.

[1] DSC, Professor, Laboratory of Information Security, Academy of Economic Studies of Moldova

[2] PhD Student, Partner, IT Audit & Advisory BSD Management SRL, Moldova

Absence of such indicators (or measurement units) as mass, gravity, friction or distance is yet another feature of cyberspace. In addition, the following statements have become widespread: cyberspace is an abstract space; cyberspace has no natural boundaries; cyberspace can obtain any number of subspaces (e.g. Internet, telephone system, radio communication system); cyberspace is not limited in its dimensions (for example, the Internet has an IP address, MAC address, port number, etc.); each dimension of cyberspace has no limits; each cyber object has its own coordinates; one cyber object can belong to more than one subspace; objects in cyberspace can interact with objects in physical space (Sheymov, 2021).

Within the framework of the existing cyberspace, many authors agree that the possibility of an active presence in this domain depends on many political, economic and social factors. The division into certain representative groups determines the ability of an individual state to develop mechanisms for responding to cyber threats, encourage investment in research and development of digital transformation processes, and the adoption of laws on data protection, establishing national computer security incident response teams (CSIRTs), cyber capacity-building (CCB), counteract the cyber attacks and etc.

2. LITERATURE REVIEW

A highly relevant literature source in the cybersecurity field is (Sheymov, 2021). This source offers an extensive analysis of cyberspace and introduces the Variable Cyber Coordinates (VCC) Method of Communications. It delves into the structures, contents, and environments of cyberspace, as well as the laws and regulations governing it, along with insights into the interactions between different subspaces. Another key work, ((Perkovich & Levite, 2017)) provides detailed research of the cyberspace components.

The cyber environment has given rise to a new form of statecraft, enabling the influence of regions in other countries through a combination of military and non-military tactics to achieve objectives via political and military pressures, as articulated by Martti Lehto in 2018 (Martti Lehto, 2018). Lehto's work comprehensively addresses several critical topics, including Deterrence Theory and Practice, Modern Strategies in Cyber Warfare, and the Detection of Domain Generation Algorithms Using Machine Learning Methods and other.

The author ((Maurer, 2018)) raises important questions about the control, authority and use of offensive cyber capabilities. In (Power & Sutton, 2018), issues related to the Main Cybersecurity Issues, Vulnerabilities and Threats, Information on Cybersecurity Controls are studied. The authors of book (Betz, 2011) consider various aspects of the problems of power and cyberspace, cyberspace and sovereignty. A number of books of undoubted interest for the study of cyberspace area should be noted (Friis & Ringsmose, 2016), (Brantly, 2016), (Libicki, 2016), (Laurent, 2022). We should also mention a number of publications describing the problems of identifying cyber threats and their impact (Mishra, 2020), (Lee, 2023), (Yassine Maleh, 2023), (Hari Vasudevan), 2022).

3. RESEARCH METHODOLOGY

The methodology of this research is based on a systemic approach that encompasses several stages, including the formulation of the conceptual foundations of cyber domain security, the structure and components as vital functions of each state, setting the research objectives, collecting statistical information from available sources (scientific and monographic literature, research reports of organizations engaged in cyber domain activities);, processing and analyzing the gathered information using game theory, econometric analysis, and economic-mathematical modeling. This methodical approach serves as the robust foundation for our study.

One of the most important tasks undertaken by the authors was the analysis of categories such as cyberspace, cybersecurity, and the identification of the interconnections among their components - Cyber Attacks, Cyber Conflict, Cyber Blockade, and Cyber Sanctions. In recent years, actions aimed at organizing Cyber Blockades and Cyber Sanctions have become increasingly prevalent, running parallel to political and economic sanctions imposed on specific countries and communities. A new political instrument and a new means of influence have emerged - cyber sanctions. Cyber sanctions are defined as economic, financial, and technological measures aimed at changing the behavior of targets through malicious actions in cyberspace and/or intrusions. An analysis of the theory and practice of interaction between various entities in the cyber sphere indicates that the concept of cyber sanctions and cyber blockade is a relatively new research direction in global politics, demanding in-depth theoretical research and practical development.

The analysis of available sources showed that a significant number of experts highlight the absence of a unified international regulatory body for evaluating state actions in cyberspace and existing mistrust in cyber sanction mechanisms. One important aspect to note is that the applied sanctions are based solely on assumptions and the lack of a factual basis, leading to the unresolved issue of attribution, i.e., identifying the source of a cyberattack. Moreover, contemporary IT allows malicious actors to mask their actions and conceal their true location (e.g., illegal marketplaces, specialized software offering criminal services, the DarkNet environment, etc.). Attribution issues currently have primarily political and declarative characteristics and often remain contentious. The key problems with attribution include:

- The continual advancement of Advanced Persistent Threats (APTs).
- Determining the sources (locations of launch and initialization) of a cyberattack.
- Identifying the party responsible for the cyberattack (the primary actor).
- Handling a large volume of unsorted (raw) data.
- The decentralization and complexity of existing public-private attribution systems.
- The use of methods to simulate cyberattacks with the aim of creating false accusations against a specific violator, cybergroup, and/or state.

Media constantly reports an increase in cyberattacks. Resistance occurs on multiple levels: state versus state, commercial entities versus commercial entities, and individual users versus higher-level entities. Unexplored aspects remain concerning public-private partnerships in the organization of cyberattacks as private companies manage a significant part of communications.

As a result, the challenges require substantial changes to existing legislation, making this the prospective research direction.

The research identifies the primary models (Oxford Cybersecurity Capacity Maturity Model (CMM) and International Telecommunication Union Global Cybersecurity Index (ITU GCI), as well as a basic set of indicators. Statistical data on the basic set were complemented by cyber-dependent crimes.

4. BASIC INDICATORS

Experts utilize two primary models as widely adopted mechanisms for assessing the cyber capabilities of countries: the Oxford Cybersecurity Capacity Maturity Model (CMM) and the International Telecommunication Union Global Cybersecurity Index

(ITU GCI). These models play a crucial role in ranking and evaluating countries based on various indicators, enabling the identification of existing gaps, strengths, and weaknesses.

The Oxford Cybersecurity Capacity Maturity Model is a methodological framework designed to assess a country's cybersecurity capabilities. This model has been continuously refined through the contributions of focus groups, thematic coding, and expert consultations. It has been implemented in over 87 countries. Various methods are employed for selecting and calculating indicators in this model:

1. One of the most significant indicator of the assessment is cyberpower. This indicator, its calculation methodology, is presented in National Cyber Power Index 2022 (NCPI), as an example of a holistic national approach (Julia Voo, 2022). The following indicators were used to calculate this indicator: Cyber Risk Literacy and Education Index; Cyber Military Staffing; Data Privacy Laws; Freedom on the Net; Global Soft Power Index; Mobile/Computer Infection Rate; National Standards Body; Population on the Internet; Social Media Usage; Surveillance.

The 2022 the calculation methodology used 29 indicators. The final aggregated NCPI calculation data for 2022 is shown in the following table.

Table 1. NCPI 2022: Top 10 Most Comprehensive Cyber Power

Ran k	2022
1	US
2	China
3	Russia
4	UK
5	Australia
6	Netherlands
7	ROK
8	Vietnam
9	France
10	Iran

Source: Julia Voo, Irfan Hemani, Daniel Cassidy (2022). National Cyber Power Index 2022. Report September 2022. p.8. www.belfercenter.org/project/cyber-project.

Ratings for various categories were considered for individual states, including Financial, Surveillance, Intelligence, Commerce, Defense, Information Control, Destructive, and Norms.

It is essential to note that elements from the theory of expected utility, widely utilized in the analysis of cyber conflicts, can also be effectively applied to elucidate a broad spectrum of political scenarios and their corresponding solutions. The concept of utility, as expounded by Bueno De Mesquita and other notable scholars (such as Scott Ashworth in 2021 and Ethan Bueno De Mesquita in 2021), may be assessed within a range spanning from +1 to -1, with the pivotal point at 0.

2. Another indexed variable related to the series Cyber Power is Indexing Equation for Cyber Power (Brantly, 2016).

3. In his paper (Kello, 2017), Lucas Kello proposes a deterrence formula for assessing prospective conflicts. This formula posits that the net benefit or cost can be

determined by calculating the ratio of the cumulative benefits and harms suffered by the victim to the cumulative costs and harms anticipated from the victim.

$$AA = \frac{\mathrm{Ba} + \mathrm{H}v}{\mathrm{Ca} + \mathrm{Hv}} \qquad (1)$$

where:

AA - net benefit or cost;

Ba - the benefits the attacker receives;
Ca - the harm the attacker inflicts on the victim (i.e., the relative benefit to the attacker);
Hv - the harm the attacker expects the victim to suffer in retaliation.

In turn, the formula used to measure perceived cyberpower is as follows:

Perceived Cyberpower=(C+E+M+I) *(S+W) + Interrelations (C, E, M, I) (2)

where:
C is the critical mass, which includes the size and age of the population and the level of cyber awareness of the population;
E - economic component, which includes cyberinfrastructure, technology and the development of and access to critical information infrastructure;
M - military component, includes the use of cybernetics in the armed forces;
I - information component, includes communication and information flows between systems and technologies;
S - strategic component, includes implementation of national cyber strategy;
W - influence of people on responsible use of cyber security rules (awareness) and prevention of cybercrime.

4. One of the important evaluation indicators can be the Composite Index of National Capacity (CINC) (Anon., n.d.). CINC is a statistical measure of national power created by J. David Singer for the Correlates of War. Each component is a dimensionless percentage of the world's total.

5. Perceived Cyber Power. This is another additional specific indicator proposed in (Jansen van Vuuren, 2018) (Anon., n.d.).

Let's examine the achievements of individual countries across a set of indicators as presented in the following tables.

Table 2: National Cyber Security Index

Country Name	**Overall Score**	**Regional Rank**	**Criteria**
Turkiye	61,04	55	Cybersecurity Policy Development - 100% Cyber Threat Analysis and Intelligence - 20% Education and Professional Development - 78% Contribution to Global Cybersecurity - 50% Digital Service Protection - 20% Critical Service Protection - 17% Electronic Identification and Trust Services - 78% Personal Data Protection - 100% Cyber Incident Response - 50% Cyber Crisis Management - 60% Combatting Cybercrime - 100% Military Cyber Operations - 17%

Romania	89.61	6	Cybersecurity Policy Development - 100% Cyber Threat Analysis and Intelligence - 80% Education and Professional Development - 78% Contribution to Global Cybersecurity - 83% Digital Service Protection - 80% Critical Service Protection - 100% Electronic Identification and Trust Services - 89% Personal Data Protection - 100% Cyber Incident Response - 100% Cyber Crisis Management - 60% Combatting Cybercrime - 100% Military Cyber Operations - 100%
Ukraine	75.32	24	Cybersecurity Policy Development - 100% Cyber Threat Analysis and Intelligence - 80% Education and Professional Development - 89% Contribution to Global Cybersecurity - 33% Digital Service Protection - 20% Critical Service Protection - 100% Electronic Identification and Trust Services - 100% Personal Data Protection - 100% Cyber Incident Response - 67% Cyber Crisis Management - 60% Combatting Cybercrime - 100% Military Cyber Operations - 17%
Bulgaria	74.03	28	Cybersecurity Policy Development - 71% Cyber Threat Analysis and Intelligence - 80% Education and Professional Development - 100% Contribution to Global Cybersecurity - 33% rDigital Service Protection - 40% Critical Service Protection - 50% Electronic Identification and Trust Services - 89% Personal Data Protection - 100% Cyber Incident Response - 100% Cyber Crisis Management - 20% Combatting Cybercrime - 100% Military Cyber Operations - 67%
Russian Federation	71.43	30	Cybersecurity Policy Development - 86% Cyber Threat Analysis and Intelligence - 60% Education and Professional Development - 89% Contribution to Global Cybersecurity - 17% Digital Service Protection - 40% Critical Service Protection - 83%

			Electronic Identification and Trust Services - 100% Personal Data Protection - 100% Cyber Incident Response - 50% Cyber Crisis Management - 20% Combatting Cybercrime - 78% Military Cyber Operations - 100%
Moldova	57.14	62	Cybersecurity Policy Development - 100% Cyber Threat Analysis and Intelligence - 20% Education and Professional Development - 79% Contribution to Global Cybersecurity - 33% Digital Service Protection - 20% Critical Service Protection - 0 Electronic Identification and Trust Services - 100% Personal Data Protection - 100% Cyber Incident Response - 50% Cyber Crisis Management - 0 Combatting Cybercrime - 100% Military Cyber Operations - 17%

Source: e-Governance Academy Foundation. https://ncsi.ega.ee/ (accessed on October 12, 2023)

The next index will be the Global Cybersecurity Index 2020, developed by the International Telecommunication Union (ITU). The main achievements are presented in the following table.

Table 3. Global Cybersecurity Index 2020: Country profiles

Country Name	**Overall Score**	**Regional Rank**	**Criteria**
Russian Federation	98.06	5	Legal Measures - 20.00 Technical Measures- 19.08 Organizational Measures - 18.98 Capacity Development - 20.00 Cooperative Measures - 20.00
Turkiye	97,50	11	Legal Measures - 20.00 Technical Measures - 19.54 Organizational Measures - 17.96 Capacity Development Measures - 20.00 Cooperative Measures - 20.00
Romania	76.29	62	Legal Measures - 18.60 Technical Measures - 18.40 Organizational Measures - 6.42 Capacity Development Measures - 12.88 Cooperative Measures - 20.00
Moldova	75.78	63	Legal Measures - 16.73 Technical Measures - 16.86 Organizational Measures - 13.21 Capacity Development Measures - 13.09

			Cooperative Measures - 15.89
Bulgaria	67.38	77	Legal Measures - 17.34 Technical Measures - 7.84 Organizational Measures - 13.72 Capacity Development Measures - 14.92 Cooperative Measures - 13.57
Ukraine	65.93	78	Legal Measures - 17.46 Technical Measures - 11.60 Organizational Measures - 13.06 Capacity Development Measures - 10.94 Cooperative Measures - 12.87

Source: Global Cybersecurity Index 2020: Country profiles. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (accessed 12.10.23)

5. CYBER-DEPENDENT CRIMES

We will link the probability of cyber conflicts with cyber-dependent crimes, defined as organized crimes that are dependent on the use of a computer, computer network or other forms of information communications technology (ICT). These include the spread of viruses or other malware, hacking, distributed denial of service (DDoS) attacks, ransomware and cryptocurrency fraud. These activities are considered to be conducted for the purpose of obtaining a monetary or material benefit (as opposed to a political or ideological objective).

Overall, the CDC index for Europe is 5.58. Let's examine the achieved results for individual countries, as presented in the following table.

Table 4. CDC Indexes by Individual Countries

		Turkiye	Bulgaria	Romania	Moldova	Ukraine	Russia
1	Criminality Scores	7,03 (+0,14)	5,65 (+0,23)	4,58 (-0,01)	5,60 (+1,15)	6,48 (+0,31)	6,87 (+0,63)
2	Criminal Market Scores	6,77 (+0,37)	5,40 (+0,30)	5,27 (+0,22)	5,20 (+1,30)	6,27 (+0,67)	6,83 (+0,73)
3	Criminal Actors Scores	7,30 (-0,08)	5,90 (+0,15)	3,90 (-0,23)	6,00 (+1,00)	6,70 (-0,05)	6,90 (+0,53)
4	Resilience Scores	3,38 (-0,17)	5,33 (+0,04)	6,00 (+0,42)	3,92 (+0,21)	4,54 (+0,54)	3,79 (-0,25)
5	Cyber-Dependent Crimes	5,00	6,00	6,00	7,50	8,50	9,00

Source: Global Organized Crime Index 2023. https://ocindex.net/report/2023.html (accessed 12.10.23)

The analysis of the data presented in the table above allows for the following preliminary conclusions. Firstly, the crime rate is increasing in all countries, except for

Romania. Secondly, there is a growth in the criminal market in all countries, with the highest increase in Moldova - 5.20 (+1.30). Thirdly, there is an increase in criminal actors in all countries, except for Turkiye, Romania, and Ukraine. Fourthly, the indicators of resilience show significant variation. Fifthly, the level of cyber-dependent crimes differs significantly: the lowest is observed in Turkiye (5.00), while the highest is in Russia (9.00).

6. CONCLUSION

Cyberspace has become a highly contested virtual territory, with countries, corporations, and individuals using it for both tactical and strategic purposes. This reflects the growing importance of the digital realm in modern society. Today's problems of political, technical and economic issues confront us with cyber espionage, data manipulation and digital disinformation. Addressing these important issues within cyberspace necessitates not only thorough scientific analysis but also effective solutions.

The authors of this study proceeded with the premise that a comprehensive examination of cyber conflict's nature could significantly enhance the multilateral collaborative process. It is important to emphasize that the level of cooperation varies in response to the conflict's dynamics and the local conflict management mechanisms.

A focus should be directed towards recognizing potential cooperative opportunities among conflicting parties, assessing their informational capacities, and considering the impact of external actors.

REFERENCES

Anon., n.d. *Composite Index of National Capability.* [Online] Available at: https://www.wikiwand.com/en/Composite_Index_of_National_Capability#introduction
[Accessed 20 10 2023].

Betz, D. S. T., 2011. *Cyberspace and the state: toward a strategy for cyber-power.* s.l.:The International Institute for Strategic Studies.

Brantly, A. F., 2016. *The decision to attack : military and intelligence cyber decision-making.* s.l.:Athens, GA : University of Georgia Press,.

Friis, K. & Ringsmose, J., 2016. *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives.* s.l.:Routledge Studies in Conflict, Security and Technology.

Hari Vasudevan (editor), S. S. D. (. A. M. (. M. M. (. N. M. S. T. P. N. R. S. M., 2022. *Cyber Security Threats and Challenges Facing Human Life.* s.l.:Chapman and Hall/CRC.

Hari Vasudevan), S. S. D. A. M. M. M. N. M. S. T. P. N. R. S. M., 2022. *Cyber Security Threats and Challenges Facing Human Life.* s.l.:Chapman and Hall/CRC.

Jansen van Vuuren, J., 2018. *Council for Scientific and Industrial Research.* [Online]
Available at: https://researchspace.csir.co.za/dspace/handle/10204/10361
[Accessed 20 10 2023].

Julia Voo, I. H. D. C. 2. N. C. P. I. 2. R. S. 2., 2022. *National Cyber Power Index 2022.* [Online]
Available at: https://www.belfercenter.org/publication/national-cyber-power-index-2022
[Accessed 20 10 2023].

Kello, L., 2017. *The Virtual Weapon and International Order.* s.l.:Yale University Press.

Laurent, S.-Y., 2022. *Conflicts, Crimes and Regulations in Cyberspace, Volume 2.* s.l.:John Wiley & Sons.

Lee, M., 2023. *Cyber Threat Intelligence.* s.l.:John Wiley & Sons Inc.

Libicki, M., 2016. *Cyberspace in Peace and War.* s.l.:Naval Institute Press.

Martti Lehto, P. N., 2018. *Cyber Security: Power and Technology.* s.l.:Springer International Publishing.

Maurer, T., 2018. *Cyber Mercenaries: The State, Hackers, and Power.* s.l.:Cambridge University Press.

Mishra, B. K. P. J. R. C., 2020. *Understanding Cyber Threats and Attacks.* s.l.:Nova Science Publishers Inc..

Perkovich, G. & Levite, A. E., 2017. *Understanding Cyber Conflict: 14 Analogies.* s.l.:Georgetown University Press.

Power, D. J. & Sutton, D., 2018. *Business continuity in a cyber world: surviving cyberattackes.* s.l.:Business Expert Press.

Sheymov, V., 2021. *CYBERSPACE and SECURITY: A Fundamentally New Approach.* s.l.:Cyberbooks Publishing.

Yassine Maleh, M. A. L. T. I. R., 2023. *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence.* s.l.:River Publishers.