ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.39 | *Nº 70*

2021

Cuestiones Políticas Vol. 39, Nº 70 (2021), 250-269
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

The stability of State information in the face of terrorist threats

DOI: https://doi.org/10.46398/cuestpol.3970.16

Yuriy M. Bidzilya *
Yevhen O. Solomin **
Halyna V. Shapovalova ***
Viktoriia V. Georgiievska ****
Nataliya M. Poplavska *****

Abstract

The objective of the study is to identify the key factors of the stability of state information in the face of terrorist threats based on the review of existing research in this area, and to identify the main approaches to ensure the stability of state information in the face of terrorist threats. Based on the analysis of scientific works, the factors of the state's resistance to cyberterrorism are identified and the main approaches are organized to ensure the stability of state information in the face of terrorist threats. The results of the study provide an understanding of the key factors needed to achieve the legal, technical, organizational, and operational areas of state resilience to cyber threats. Further research may aim to perform empirical calculations of indicators from around the world to determine certain dependencies in the field of cybersecurity. It is concluded that factors such as the growing impact of information and communication technologies on public relations, production activities, the operation of infrastructure facilities and the activities of public authorities, indicate that the issue of security as a line of scientific research is urgent.

Keywords: information stability; state; cyberterrorism; cybersecurity; threats.

* Doctor of Social Communications, Associate Professor, Professor, Head of the Department of Journalism, Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine. ORCID ID: https://orcid.org/0000-0001-5134-3239. Email: bidziljau@gmail.com

** PhD in Social Communications, Associate Professor of the Department of Journalism, Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine. ORCID ID: https://orcid.org/0000-0001-6770-5505. Email: yevgensolomin@uzhnu.edu.ua

*** PhD in Philology, Associate Professor of the Department of Journalism, Faculty of Philology, Uzhhorod National University, Uzhhorod, Ukraine. ORCID ID: https://orcid.org/0000-0001-8935-5673. Email: shapovalova@gmail.com

**** Doctor of Social Communications, Associate Professor, Professor of Department of Journalism and New Media, Institute of Journalism, Borys Hrynchenko Kiev University, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-5848-957X. Email: wiolettawwwww@gmail.com

***** Doctor of Philology, Professor, Head of Department of Journalism, Faculty of Philology and Journalism, Volodymyr Hnatiuk Ternopil National Pedagogical University, Ternopil, Ukraine. ORCID ID: https://orcid.org/0000-0003-1100-5002. Email: nataliazai50@gmail.com

Recibido el 05/05/2021 Aceptado el 20/08/2021

La estabilidad de la información del Estado frente a las amenazas terroristas

Resumen

El objetivo del estudio es identificar los factores clave de la estabilidad de la información del estado frente a las amenazas terroristas basándose en la revisión de la investigación existente en esta área, e identificar los principales enfoques para garantizar la estabilidad de la información del estado frente a las amenazas terroristas. Con base en el análisis de trabajos científicos, se identifican los factores de la resistencia del estado al ciberterrorismo y se organizan los principales enfoques para garantizar la estabilidad de la información del estado ante amenazas terroristas. Los resultados del estudio proporcionan una comprensión de los factores clave necesarios para lograr las áreas: legales, técnica, organizacional y operativa de la resiliencia del estado a las amenazas cibernéticas. La investigación adicional puede tener como objetivo realizar cálculos empíricos de indicadores de todo el mundo para determinar ciertas dependencias en el campo de la ciberseguridad. Se concluye que factores como el creciente impacto de las tecnologías de la información y la comunicación en las relaciones públicas, las actividades de producción, el funcionamiento de las instalaciones de infraestructura y las actividades de las autoridades públicas, indican que urge el tema de la seguridad como línea de investigación científica.

Palabras claves: estabilidad de la información; estado; ciberterrorismo; ciberseguridad; amenazas.

Introduction

The threats that pose both local and global dangers are growing with the development of information and communication technologies (ICTs), their spread and penetration into virtually all spheres of human activity. Information and communication technologies allow access to information, doing business, developing and maintaining professional and personal communication, as well as involving public authorities and expanding governance. Cyberspace and ICT provide huge growth potential at virtually every level (United Nations, 2017), which requires the state to provide a clear vision of threats and coordinated action to implement security functions (Kruhlov *et al.*, 2020). The growing number of users, the operation of critical infrastructure systems based on digital software involves incidents of external unauthorised interference with the aim of committing crimes, attacks, fraud and terrorist acts. Today's scale of negative impact on security systems has reached the international level, when terrorist attacks and hybrid information warfare are realised through interventions in the information infrastructure.

Because the cyberspace environment is not limited by any regulatory limits, clandestine cyber-attacks can be carried out by a person or group of people at an incredible speed from a distance of thousands of miles without significant physical cost. The damage from such cyberattacks can be as critical as from ordinary war. A terrorist organisation with limited manpower and infrastructure can carry out cyber-attacks from anywhere, causing significant loss of infrastructure, finances or human life. In the absence of a formal definition of a cyber-terrorist, countries use different strategies to combat this phenomenon, but the very perception of the threat of cyber-attack is fully understood by all countries in the world as regards the possibility of causing significant harm (Albahar, 2019).

The study (UNICRI, 2014) found that, although cyber threats consisted mainly of viruses, Trojans, over time cybercriminals began to take advantage of social engineering technologies, such as phishing, targeting employees with direct access. to databases with confidential information; credit card fraud; special denial-of-service attacks; theft of public and private data. The World Economic Forum estimates that cyber-attacks and cybersecurity violations will be one of the most likely risks to humanity in the next ten years (WEF, 2021).

The FBI said the financial loss from cyberattacks in 2019 exceeded $ 3.5 milliard, and the United States was not ready to defend itself against cyberattacks. Following the 2020 coronavirus pandemic and the implementation of large-scale remote operation plans, the threat of possible attacks and crisis plans have become more dangerous. According to the International Monetary Fund, the number of cyberattacks has increased significantly, with the largest number of victims being government agencies and financial services (IMF, 2020).

As cyberspace evolves rapidly, the cyber threats of the recent past have also changed. Not only have they multiplied in terms of the means to commit them, but they have also grown into cybercrime, cyberterrorism, cyber espionage, and cyberwarfare (United Nations, 2017). At the same time, the threat of terrorism is increasingly being considered as one of the greatest threats to society, affecting the quality of life of people around the world (Kumar *et al.*, 2019). Terrorist acts can destabilise governments, undermine civil society, threaten peace and security, threaten social and economic development, and have a particularly negative impact on certain groups (United Nations, 2008).

Cyberterrorism is defined as terrorism-related activities that can be organised from anywhere in the world using a computer with a hidden Internet Protocol address. Cyberterrorism involves the use of information technology by terrorist groups or individuals to pursue their own goals, which may include organising and carrying out attacks on networks, computer systems and telecommunications infrastructures, as well as exchanging

information or creating threats electronically (Palasinski and Bowman-Grieve, 2017). In the process of an act of cyberterrorism, a deliberate attack or threat is made by private entities based on the use of cyberspace to entail real consequences in order to cause fear, coercion to fulfil social or ideological goals. The consequences can be physical, psychosocial, political, economic, environmental or other problems outside of cyberspace (Plotnek and Slay, 2021).

Cyberterrorism actually uses modern technology to take advantage of the strategic weaknesses of the system and use them to achieve their own goals. Areas of illegal action may be: the use of the Internet for interaction between terrorists; creating access to a variety of information stored on the Internet, indicating possible purposes, as well as providing technical details; use of the Internet to spread terrorist ideas and ideologies of a terrorist organisation and to carry out terrorist attacks via the Internet. Most terrorist groups use basic methods: electronic attack which blocks computer systems; introduction of malware into computer systems and information transmission channels; attack on computer networks using malware and taking advantage of vulnerabilities in computer software in order to steal some data or destroy them (Vilić, 2017).

Cyberterrorism usually involves illicit actions against computer systems, computer networks, and the Internet using malware, viruses, and other technologies to achieve their goals (United Nations, 2017; Backhaus *et al.*, 2020). Contemporary literature offers a conceptual explanation by placing cyberterrorism in a typology of cybersecurity challenges (Veerasamy and Grobler, 2015).

The risk of cyber-terrorist attacks on the country's critical infrastructure is extremely high. Due to their vulnerability and complexity, damage to the country's infrastructure can negatively affect the country's development (Dombe and Golandsky, 2016). A system of targeted cyber-terrorist attacks can include a country's critical infrastructure that creates problems in the telecommunications system, transportation system, power grid system, utility system, and other important systems needed to run the country. The threat of cyber-terrorist attacks will continue to grow as people become addicted to the Internet, increasing the potential for cyber-terrorist attacks. The introduction of mechanisms of secure technologies, policies, actions of law enforcement agencies allow the computer network and systems to be less vulnerable and manage the risk of cyberterrorism, as each mechanism has its own functions in this fight (Ponnusamy and Rubasundram, 2019).

Critical infrastructure refers to organisational and physical facilities and structures that are vital to society and the economy, and failure or degradation will lead to persistent service shortages, significant public safety breaches, or other negative consequences (Rass *et al.*, 2020).

Considering cyberterrorism as illegal actions, causing harm, causing damage and negative impact or violation of the integrity and effectiveness (in some cases — destruction) of critical infrastructure, it can be determined that the actions of the state and entities performing cybersecurity functions should use a wider approach to issues of ensuring information resilience to terrorist threats. The concept of cybersecurity should consider cyberterrorism as one of the most dangerous crimes against individuals, politicians, society, legal entities, information and physical objects and the state. It follows that measures to ensure the information stability of the state to the terrorist threat should include actions provided in the event of the occurrence and detection of cyber fraud, cyber espionage, cybercrime, cyber-attacks and other widespread cyber threats.

Cybersecurity is an important part of local governance based on reliable information technology. Thus, well-defined key factors of information stability of the state to terrorist threats should become an important regulatory development, which can in some way adjust a separate vision of cybersecurity policy and directions of both scientific and practical developments in the field of cybersecurity.

The aim of the study is to identify key factors of information stability of the state to terrorist threats (resilience of the state to cyberterrorism) based on the review of existing research in this area and identify key approaches to ensuring information resilience of the state to terrorist threats. The main research objectives are the following:

1. Develop methodological approaches to the search and identification of modern research related to aspects of information stability of the state to terrorist threats.
2. Identify key factors in the state's resilience to cyberterrorism.
3. Arrange the identified factors and identify the main areas of cybersecurity.
4. Compare the obtained results with the existing methodological approaches of the world's leading institutions on cybersecurity and countering cyberterrorism to identify the reliability of the research results.
5. Propose approaches that can ensure the information security of the state from terrorist threats.

1. Methods

The methodological approach of the study is based on several stages. From 2014 to 2021, the Scopus search was used to identify scientific

publications related to the information stability of the state to terrorist threats. Applying the review method considered by previous researchers (Yi and Chan, 2014; Osei-Kyei and Chan, 2015; Darko and Chan, 2016; Yu *et al.*, 2018), scientific articles on the information stability of the state to terrorist threats are reviewed in order to identify trends in the study of this topic and consider key areas of research. The review method includes: selection of journals (Social Sciences; Computer Science; Business, Management and Accounting; Economics, Econometrics and Finance); selection of relevant articles; identification of factors that ensure the information stability of the state to terrorist threats.

A visual examination of the titles, abstracts and keywords of the articles, which explore the means of ensuring the information stability of the state to cyberterrorist threats, helped to identify the necessary sources. The selected articles identify the key factors of information stability of the state to terrorist threats and provide the classifications. When choosing the key factors, the condition of their research was taken into account in at least two articles for a certain period of time. Suggestions and conclusions are drawn based on the obtained data.

The search in the Scopus database according to the established restrictions found 389 articles. Visual examination of the titles, abstracts and keywords of the articles, which explore the means of ensuring the information stability of the state to cyberterrorist threats, identified 40 articles for further analysis. Although the sample size is small, it may be sufficient for further analysis and can be considered satisfactory for drawing conclusions.

2. Results

As a result, selected 40 articles published in 26 scientific journals were reviewed to identify key factors in the information resilience of the state to terrorist threats. Table 1 summarises the results of the analysis of key factors of information protection of the state, which are published in 26 scientific journals.

Table 1. The results of the analysis of identifying key factors of information resilience of the state to terrorist threats

No	Factors that ensure information stability	Publications	Number of publications
1	Detection of network intrusions and attacks	(Quincozes *et al.*, 2021), (Kannari *et al.*, 2021) (Binbusayyis and Vaiyapuri, 2021). (Moraboena *et al.*, 2020), (Thapa *et al.*, 2020), (Tian *et al.*, 2020), (Handa *et al.*, 2019), (Camacho *et al.*, 2019), (Bhamare *et al.*, 2020), (Jamei *et al.*, 2016), (Taha *et al.*, 2018), (Adhikari *et al.*, 2016), (Rehman *et al.*, 2021).	14
2	Application of international law and legal regulation	(Branch, 2020), (Kulesza and Weber, 2021), (Sturc *et al.*, 2020), (Carvalho *et al.*, 2020), (Markopoulou *et al.*, 2019), (Park *et al.*, 2018), (Kulesza and Weber, 2021).	7
3	Detection of current threats, data anomalies and malware	(Cascavilla *et al.*, 2021), (Sadik *et al.*, 2020), (Lee and Lim, 2016), (Gonzalez-Granadillo *et al.*, 2018), (Catak *et al.*, 2021), (Jagtap *et al.*, 2021), (Ma *et al.*, 2021).	7
4	Cyber intelligence and cyber deterrence	(Yau, 2020), (Wilner, 2017), (Nespoli *et al.* 2021), (Gourisetti *et al.*, 2020).	5
5	Interstate cooperation	(Lee and Lim, 2016), (Cho and Chung, 2017), (Górka, 2018).	3
6	Cybersecurity certification	(Neisse *et al.*, 2020), (Hernandez-Ramos *et al.*, 2021).	2
7	Cyber insurance	(Herr, 2021), (Lau *et al.*, 2020).	2
8	Standardisation of countermeasures and use of cybersecurity standards	(Nespoli *et al.*, 2021), (Syafrizal *et al.*, 2020).	2
9	Threat simulation and risk assessment	(Välja *et al.*, 2020), (Cascavilla *et al.*, 2021).	2
10	Digital forensics	(Lee and Lim, 2016), (Alharbe, 2020).	2

Source: own elaboration.

The above 10 key factors of information stability of the state to terrorist threats are further analysed and classified into different areas of approaches to cybersecurity. Based on the analysis, the identified factors were arranged and three key areas of approaches to cybersecurity were identified, taking into account the tools studied above, which provide information stability (Table 2). As cybersecurity has a wide scope, covering many industries and different sectors, level of development or opportunities, it should be noted that mainly approaches to ensuring information stability of the state to terrorist threats are focused on legal, technical, organisational and operational areas.

Table 2. Analysis of key areas of approaches to information stability of the state to terrorist threats

Key areas of approaches to cybersecurity	Factors that ensure information stability
Legal area	Application of international law and legal regulation. Interstate cooperation. Cybersecurity certification. Cyber insurance.
Technical area	Detection of network intrusions and attacks. Detection of current threats, data anomalies and malware. Standardisation of countermeasures and use of cybersecurity standards.
Organisational and operational area	Cyber intelligence and cyber deterrence (reduction of danger and vulnerability). Threat simulation and risk assessment. Digital forensics.

Source: own elaboration.

According to the analysis, it is necessary to dwell on individual provisions that define the established limitations in the study.

3. Discussion

Thus, after reviewing and analysing the factors of information resilience of the state to terrorist threats, 40 articles were identified from 26 journals that explored various issues related to cybersecurity and cyberterrorism. The review identified 10 key factors in the state's information resilience to terrorist threats. The most widely studied factors were: "detection of network intrusions and attacks", "application of international law and legal regulation" and "detection of current threats, data anomalies and malware". These 10 factors of information stability of the state to terrorist threats were used to develop a generalised approach to determining the legal, technical, organizational and operational areas used in ensuring the resilience of the state to cyberterrorism.

As noted, the search for scientific sources established limits on the time period of the sample. We believe that the found studies for 2014-2021 more relevantly reflect the approaches used to ensure the information stability of the state to terrorist threats. However, a wider period of time would allow identifying additional approaches that are not considered in this study. The use of the Scopus search was substantiated as follows: most scientific publications in the fields of management, accounting, engineering, business and social sciences have been archived in this database (Hong and Chan, 2014). However, the research does not take into account the articles indexed in the Web of Science database, which probably reduces the number of studies addressing the issue of state resilience to cyberterrorist threats. Another feature is the limitation of the number of key factors by the presence of two or more publications where certain factors have been studied. In our opinion, this demonstrates more relevant and interesting areas of research on the state's resilience to cyberterrorist threats.

The current approaches reflected in the study seek new levels of countering cyberattacks, especially when related to government facilities and critical infrastructure, namely power system security, industrial management systems (Handa *et al.*, 2019). Other areas of the fight against cyberterrorism may be: risk, threat and vulnerability assessment; emergency response plan; assessment of security procedures; intelligence data collection; partnership with special rapid response services.

Information security issues are constantly on the agenda in the EU, as member states need strong cybersecurity for their markets, significant progress in countries' technological capabilities and a broader understanding of everyone's role in countering cyber threats. In response, new initiatives are proposed in three key areas: strengthening resilience to cyber-attacks and strengthening the EU's cybersecurity capacity; creating an effective criminal law response; strengthening global stability through international cooperation (Carvalho *et al.*, 2020).

From the point of view of the consequences of measures aimed at ensuring the information stability of the state to terrorist threats, the issue of determining the level of prevention of cyber threats in different countries is methodologically considered by individual research institutions. The E-Governance Academy (eGA), established as a joint initiative of the Estonian government, the Open Society Institute (OSI) and the United Nations Development Programmes, has developed its own methodology for determining the National Cyber Security Index (NCSI). The National Cyber Security Index is a global index that measures countries' readiness to prevent cyber threats and manage cyber incidents. NCSI is also a database with publicly available evidence and tools to build national cybersecurity capacity. NCSI focuses on measurable aspects of cybersecurity implemented by the state: current legislation (legal acts, regulations, orders); provided administrative structures (existing organisations, departments); formats of cooperation (committees, working groups); results (policies, technologies, websites, programmes) (EGA, 2021b).

Analysing the indicators of the National Cyber Security Index of 100 countries in 2018 and 2021, we can see that the vast majority of studied countries have improved their Cyber Security Index (Figure 1).

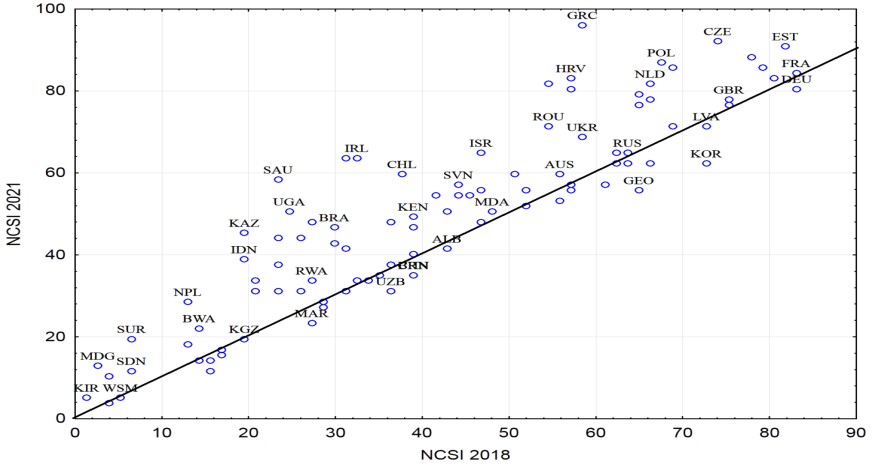

Figure 1. Diagram of the progress of individual countries in the world according to the National Cyber Security Index, 2018-2021 (EGA, 2018; EGA, 2021a)

The readiness of the potential to fight cybercrime is assessed by the following dimensions: political framework; legal framework; criminal law; electronic evidence; jurisdiction; guarantees; international cooperation; capacity building (United Nations, 2017). Another approach to determining the level of cybersecurity in the country is the Global Cybersecurity Index (GCI). International cooperation of many stakeholders in the field of cybersecurity at the initiative of the International Telecommunication Union (ITU) focuses on the following aspects: legal (legislation, regulation, measures based on the legal institutions and entities in the field of cybersecurity and cybercrime); technical (technical mechanisms and capabilities, measures based on the institutions and response entities in the field of cybersecurity); organisational (national cybersecurity development strategies, cybersecurity indicators, policy coordination institutions and cybersecurity development strategies); capacity building (standards of certification and accreditation of cybersecurity specialists and public sector institutions, public information, research and development, educational and training programmes); cooperation (existence of partnerships, cooperation frameworks and information exchange networks, multilateral agreements, participation in international forums). These identified aspects form the basis of the indicators for the Global Cyber Security Index, as they are an integral part of the national cyber security culture (ITU, 2019).

Thus, in addition to traditional methods of action through policies, laws and institutions, governments must also seek additional resources, including consumer information and private sector involvement. The state constantly faces with the problem of ensuring international compatibility. Issues of jurisdiction and international cooperation pose significant difficulties for the investigation and prosecution of multinational cybercrime cases. Moreover, the challenges of some states operating within an insufficiently specific cybercrime legal framework often hinder the fight against transnational acts (United Nations, 2017).

Strategic autonomy in the age of digital technologies allows the EU countries to maintain their independence and authority. The Strategy Paper of the European Political Strategy Centre (EPSC) defines three dimensions of digital sovereignty: industrial, operational and political (EPSC, 2019). Industrial dimension requires meeting digital needs (use of digital technologies to ensure the resilience of infrastructure to cyberattacks). The operational aspect is related to the sustainability of the European communication infrastructure, as well as information and communication technology (ICT) systems. The political dimension determines the impact on norms and standards of information technology and the ability to define one's actions and norms (Debar *et al.*, 2021).

The institutional approach envisages the creation and effective functioning of bodies that shape cybersecurity policy and are at the forefront

of the fight against cybercrime. One such institution is the European Union Agency for Network and Information Security (ENISA), which is the most important institution in the European Union in the field of network and information security, being part of the European cyber security strategy. ENISA was set up to promote better cooperation between the authorities of different Member States. ENISA's role is to establish a high level of network and data security in the European Union, to warn citizens about the risks and to promote a safety culture on the Internet for the benefit of citizens, consumers, businesses and public authorities. ENISA's responsibilities are to support the development of European Union policies and regulations in the field of network and data security; supporting the development of new solutions in the digital world; cooperation between competent authorities and other interested institutions; support for research, development and standardisation; cooperation with EU bodies and organisations, including those responsible for protection against high-tech crimes, confidentiality and data protection; working with international organisations to promote international cooperation in the field of network and data security (Carvalho *et al.*, 2020). ENISA identifies data security, robust software platforms, cyber threat management and response, robust hardware platforms, user-oriented cryptography and security tools, and digital communications security as cybersecurity research priorities as (Debar *et al.,* 2021).

As we can see, the approach used in identifying key factors of information stability of the state to terrorist threats identified the main directions in research on the state's resilience to cyberterrorism: legal, technical, organisational and operational areas. Emphasising the need to further expand the time limits in the study and the use of various scientometric databases, it should be noted that institutions that analyse and ensure cybersecurity around the world mainly focus on legal aspects, technical approaches, organisational and operational areas. This supports the correctness of the methodological approach, as well as the generalisations and conclusions made.

The results of the study allow determining the need to implement approaches that can ensure the information security of the state from terrorist threats. Information protection should be based on the constant study of cyber threats, their evolution, the emergence of vulnerable elements; study of modern changes and monitoring of cyberterrorism technologies; defining goals and priorities of information stability; actions to prevent and respond to unauthorised intrusions and attacks; outsourcing of individual functions; checking the effectiveness of actions related to ensuring information stability.

One of the effective ways to implement cybersecurity should be the use of public-private partnerships, which will attract private businesses that use elements of critical infrastructure; server equipment manufacturers,

software developers. The use of public-private partnership in approaches to protection against cyberterrorism will strengthen the functions of control, coordination and motivation to ensure the information stability of the state.

The studied range of issues should include strategic approaches to the implementation of state programmes to strengthen cyber resilience, establishment of the necessary sectoral institutions, the development of procedures and processes, improving the management of intelligence activities. Separate objectives of further development of the information stability of the state to terrorist threats are the improvement of legislation in the field of cyber defence and cybercrime, protection of critical infrastructure; ensuring standardisation and certification; regulation of technical safety and data processing; expansion of international cooperation; increasing technical support and attracting qualified specialists. The formation of the state's capabilities in the field of cybersecurity involves the implementation of priority projects, strategy development in the field of critical infrastructure protection, cooperation with partners.

Conclusion

The issue of factors of information stability of the state to terrorist threats has become one of the most widely studied, given the penetration of information and communication technologies in critical infrastructure, public authorities, livelihoods, and significant consequences of threats and cyberattacks.

Given the wide scope of cybersecurity, the main approaches to ensuring the information stability of the state to terrorist threats should identify legal, technical, organisational and operational areas. The results allow considering research and monitoring of cyberterrorism technologies; outsourcing of individual functions; use of public-private partnership; implementation of state programmes to strengthen cyber resilience; expansion of international cooperation; technical support, etc. as approaches to ensuring the information stability of the state to terrorist threats.

The results of this study significantly contribute to the existing approaches to finding the state's resilience to cyberterrorism and inform practitioners about the key areas that need to be considered when developing national cybersecurity policies. In addition, the results provide a deep understanding of the key factors necessary to achieve the legal, technical, organisational and operational areas of state resilience to cyber threats.

This study has some internal limitations that affect the generalisation of the research results, namely: the approach to the number of works selected

for further analysis, which does not allow to cover individual research. However, the results are useful for further research, as the aim was to identify and summarise the existing key factors in current research that are important in the cybersecurity system. Further research may accept a certain list of factors of information stability of the state to terrorist threats and make empirical calculations of indicators of different countries to determine the existing dependencies in the field of cybersecurity.

Bibliographic References

ADHIKARI, Uttam; MORRIS, Thomas; PAN, Shengyi. 2016. "Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection" In: IEEE Transactions on Smart Grid. Vol. 9, No. 5, pp. 3928-3941.

ALBAHAR, Marwan. 2019. "Cyber-attacks and terrorism: A twenty-first century conundrum" In: Science and engineering ethics. Vol. 25, No. 4, pp. 993-1006.

ALHARBE, Mahmood Abdulghani. 2020. "Cyber security, forensics and its impact on future challenges in Saudi Arabia smart cities: Case study on the modern, urban planning and design" In: International Journal of Advanced Trends in Computer Science and Engineering. Vol. 9, No. 2, pp. 2464-2470.

BACKHAUS, Sophia; GROSS, Michael; WAISMEL-MANOR, Israel; COHEN, Hagit; CANETTI, Daphna. 2020. "A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure" In: Cyberpsychology, Behavior, and Social Networking. Vol. 23, No. 9, pp. 595-603.

BHAMARE, Deval; ZOLANVARI, Maede; ERBAD, Aiman; JAIN, Raj; KHAN, Khaled; MESKIN, Nader. 2020. "Cybersecurity for industrial control systems: A survey" In: Computers and Security. Vol. 89, Article 101677. Available online. In: https://doi.org/10.1016/j.cose.2019.101677. Date of consultation: 14/09/2020.

BINBUSAYYIS, Adel; VAIYAPURI, Thavavel. 2021. "Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM" In: Applied Intelligence. Vol. 51, No. 2, pp. 980-990.

BRANCH, Jordan. 2021. "What's in a name? Metaphors and cybersecurity" In: International Organization. Vol. 75, No. 1, pp. 39-70.

CAMACHO, Jose; GARCÍA-GIMÉNEZ, Jose Manuel; FUENTES-GARCÍA, Noemí Marta; MACIÁ-FERNÁNDEZ, Gabriel. 2019. "Multivariate big data analysis for intrusion detection: 5 steps from the haystack to the needle. In: Computers and Security. Vol. 87, Article 101603. Available online. In: https://doi.org/10.1016/j.cose.2019.101603. Date of consultation: 14/09/2020.

CARVALHO, João Vidal; CARVALHO, Sandro; ROCHA, Álvaro. 2020. "European strategy and legislation for cybersecurity: Implications for Portugal" In: Cluster Computing. Vol. 23, No. 3, pp. 1845-1854.

CASCAVILLA, Giuseppe; TAMBURRI, Damian; VAN DEN HEUVEL, Willem. 2021. "Cybercrime threat intelligence: A systematic multi-vocal literature review" In: Computers and Security. Vol. 105, Article 102258. Available online. In: https://doi.org/10.1016/j.cose.2021.102258. Date of consultation: 14/09/2020.

CATAK, Ferhat Ozgur; AHMED, Javed; SAHINBAS, Kevser; KHAND, Zahid Hussain. 2021. "Data augmentation based malware detection using convolutional neural networks" In: Peer J Computer Science. Vol. 7, pp. 1-26.

CHO, Yoonyoung; CHUNG, Jongpil. 2017. "Bring the state back in: Conflict and cooperation among states in cybersecurity" In: Pacific Focus. Vol. 32, No. 2, pp. 290-314.

DARKO, Amos; CHAN, Albert. 2016. "Critical analysis of green building research trend in construction journals" In: Habitat International. Vol. 57, pp. 53-63.

DOMBE, Arur; GOLANDSKY, Youram. 2016. A Review and Analysis of the World of Cyber Terrorism. Available online. In: https://cyberisk.biz/cyber-terrorism-review-and-analysis/. Consultation date: 11/02/21.

EGA. 2018. National Cyber Security Index 2018. Tallinn: e-Governance Academy. Available online. In: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf. Consultation date: 11/03/2021.

EGA. 2021a. NCSI: Compare. Tallinn: e-Governance Academy. Available online. In: https://ncsi.ega.ee/compare/. Consultation date: 13/03/21.

EGA. 2021b. NCSI: Methodology. Tallinn: e-Governance Academy. Available online. In: https://ncsi.ega.ee/methodology/. Consultation date: 13/03/2021.

DEBAR, Herve; DI FRANCO, Fabio; GRAMMATOPOULOS, Athanations; MANTZOURANIS, Irene; MARKATOS, Evangelous. 2021. Cybersecurity

research directions for the EU's digital strategic autonomy. ENISA. Available online. In: https://op.europa.eu/en/publication-detail/-/publication/30b09e02-a7cc-11eb-9585-01aa75ed71a1/language-en. Consultation date: 11/03/2021.

EPSC. 2019. Rethinking strategic autonomy in the digital age. European Political Strategy Centre, Strategic Notes, 30. Available online. In: https://wayback.archive-it.org/12090/20191129072400/https://ec.europa.eu/epsc/publications/strategic-notes/rethinking-strategic-autonomy-digital-age_en. Consultation date: 11/03/2021.

GONZALEZ-GRANADILLO, Gustavo; DUBUS, Samuel; MOTZEK, Alexander; GARCIA-ALFARO, Joaquin; ALVAREZ, Ender; MERIALDO, Matteo; DEBAR, Herve. 2018. "Dynamic risk management response system to handle cyber threats" In: Future Generation Computer Systems. Vol. 83, pp. 535-552.

GÓRKA, Marek. 2018. "The Cybersecurity Strategy of the Visegrad Group Countries" In: Politics in Central Europe. Vol. 14, No. 2, pp. 75-98.

GOURISETTI, Sri Nikhil Gupta; MYLREA, Michael; PATANGIA, Hirak. 2020. "Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis" In: Future Generation Computer Systems. Vol. 105, pp. 410-431.

HANDA, Anand; SHARMA, Ashu; SHUKLA, Sandeep. 2019. "Machine learning in cybersecurity: A review" In: Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. Vol. 9, No. 4. Available online. In: https://doi.org/10.1002/widm.1306. Consultation date: 11/03/2021.

HERNANDEZ-RAMOS, Jose; MATHEU, Sara; SKARMETA, Antonio. 2021. "The challenges of software cybersecurity certification [Building Security In]" In: IEEE Security & Privacy. Vol. 19, No. 1, pp. 99-102.

HERR, Tobias. 2021. "Cyber insurance and private governance: The enforcement power of markets" In: Regulation and Governance. Vol. 15, No. 1, pp. 98-114.

HONG, Yuming; CHAN, Daniel. 2014. "Research trend of joint ventures in construction: A two-decade taxonomic review" In: Journal of facilities management. Vol. 12, No. 2, pp. 118-141.

IMF. 2020. Cyber Risk is the New Threat to Financial Stability. Available online. In: https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/. Consultation date: 11/02/2021.

ITU. 2019. Global Cybersecurity Index 2018. Available online. In: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. Consultation date: 11/03/2021.

JAGTAP, Sagar; SHANKAR, Sriram; SUBRAMANIYASWAMY, Vim. 2021. "A hypergraph based Kohonen map for detecting intrusions over cyber-physical systems traffic" In: Future Generation Computer Systems. Vol. 119, pp. 84-109.

JAMEI, Mahdi; STEWART, Emma; PEISERT, Sean; SCAGLIONE, Anna; MCPARLAND, Chuck; ROBERTS, Ciaran; MCEACHERN, Alex. 2016. "Micro synchrophasor-based intrusion detection in automated distribution systems: Toward critical infrastructure security" In: IEEE Internet Computing. Vol. 20, No. 5, pp. 18-27.

KANNARI, Phanindra Reddy; SHARIFF, Noorullah; BIRADAR, Rajkumar. 2021. "Network intrusion detection using sparse autoencoder with swish-PReLU activation model" In: Journal of Ambient Intelligence and Humanized Computing. Vol. 12, No. 3, pp. 3209 - 3212.

KRUHLOV, Vitalii; LATYNIN, Mykola; HORBAN, Alina; PETROV, Anton. 2020. "Public-private partnership in cybersecurity" In: CEUR Workshop Proceedings. Vol. 2654, pp. 619-628.

KULESZA, Joanna; WEBER, Rolf. 2021. "Protecting the internet with international law" In: Computer Law and Security Review. Vol. 40. Available online. In: DOI: 10.1016/j.clsr.2021.105531. Consultation date: 11/03/2021.

KUMAR, Vivek; MAZZARA, Manuel; MESSINA, Angelo; LEE, Joo. 2019. A conjoint application of data mining techniques for analysis of global terrorist attacks-prevention and prediction for combating terrorism. Springer. Berlin, Germany.

LAU, Pikkin; WEI, Wei; WANG, Lingfeng; LIU, Zhaoxi; TEN, Chee. 2020. "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation". In: IEEE Transactions on Smart Grid. Vol. 11, No. 5, pp. 4403-4414.

LEE, Kyungbok; LIM, Jong. 2016. "The reality and response of cyber threats to critical infrastructure: A case study of the cyberterror attack on the Korea Hydro & Nuclear Power Co., Ltd" In: KSII Transactions on Internet and Information Systems. Vol. 10, No. 2, pp. 857-880.

MA, Qian; SUN, Cong; CUI, Baojiang; JIN, Xiaohui. 2021. "A novel model for anomaly detection in network traffic based on kernel support vector machine" In: Computers and Security. Vol. 104, Article 102215.

Available online. In: DOI: https://doi.org/10.1016/j.cose.2021.102215. Consultation date: 11/03/2021.

MARKOPOULOU, Dimitra; PAPAKONSTANTINOU, Vagelis; DE HERT, Paul. 2019. "The new EU cybersecurity framework: The NIS directive, ENISA's role and the general data protection regulation" In: Computer Law and Security Review. Vol. 35, No. 6, pp. 123-136.

MORABOENA, Srikanthyadav; KETEPALLI, Gayatri; RAGAM, Padmaja. 2020. "A deep learning approach to network intrusion detection using deep autoencoder" In: Revue d'Intelligence Artificielle. Vol. 34, No. 4, pp. 457-463.

NEISSE, Ricardo; HERNANDEZ-RAMOS, Jose Luis; MATHEU-GARCIA, Sara Nieves; BALDINI, Gianmarco; SKARMETA, Antonio; SIRIS, Vasilios; NIKANDER, Pekka. 2020. "An interledger blockchain platform for cross-border management of cybersecurity information" In: IEEE Internet Computing. Vol. 24, No. 3, pp. 19-29.

NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Felix; MAESTRE VIDAL, Jorge. 2021. "Battling against cyberattacks: Towards pre-standardization of countermeasures" In: Cluster Computing. Vol. 24, No. 1, pp. 57-81.

OSEI-KYEI, Robert; CHAN, Albert. 2015. "Review of studies on the critical success factors for publiceprivate partnership (PPP) projects from 1990 to 2013" In: International Journal of Project Management. Vol. 33, No. 6, pp. 1335-1346.

PALASINSKI, Marek; BOWMAN-GRIEVE, Lorraine. 2017. "Tackling cyber-terrorism: Balancing surveillance with counter-communication" In: Security Journal. Vol. 30, No. 2, pp. 556-568.

PARK, Sangdon; KIM, Il Hwan; KIM, Jaehyoun; LEE, Kyung Lyul. 2018. "The diagnosis and prescription for cybersecurity in Korea: Focusing on policy and system" In: KSII Transactions on Internet and Information Systems. Vol. 12, No. 2, pp. 843-859.

PLOTNEK, Jordan; SLAY, Jill. 2021. "Cyber terrorism: A homogenized taxonomy and definition" In: Computers & Security. Vol. 102, Article 102145. Available online. In: DOI: https://doi.org/10.1016/j.cose.2020.102145. Consultation date: 16/04/2021.

PONNUSAMY, Suhannia; RUBASUNDRAM, Geetha. 2019. "An international study on the risk of cyber terrorism" In: International Journal of Recent Technology and Engineering. Vol. 7, No. 5, pp. 159-163.

QUINCOZES, Silvio; ALBUQUERQUE, Celio; PASSOS, Diego; MOSSÉ, Daniel. 2021. "A survey on intrusion detection and prevention systems in digital substations" In: Computer Networks. Vol. 184, Article 107679. Available online. In: DOI: https://doi.org/10.1016/j.comnet.2020.107679. Consultation date: 16/04/2021.

RASS, Stefan; SCHAUER, Stefan; KÖNIG, Sandra; ZHU, Quanyan. 2020. Cyber-Security in Critical Infrastructures. Springer. Berlin, Germany.

REHMAN, Shafiq; KHALIQ, Muhammad; IMTIAZ, Mulla; RASOOL, Asif; SHAFIQ, Muhammad; JAVED, Zahira; BASHIR, Khalid. 2021. "DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)" In: Future Generation Computer Systems. Vol. 118, pp. 453-466.

SADIK, Shahrin; AHMED, Mohiuddin; SIKOS, Leslie; NAJMUL, Islam. 2020. "Toward a sustainable cybersecurity ecosystem" In: Computers. Vol. 9, No. 3, pp. 1-17.

STURC, Boris; GUROVA, Tatyana; CHERNOV, Sergei. 2020. "The specifics and patterns of cybercrime in the field of payment processing" In: International Journal of Criminology and Sociology. Vol. 9, pp. 2021-2030.

SYAFRIZAL, Melwin; SELAMAT, Rahayu; ZAKARIA, Nurul Azma. 2020. "Analysis of cybersecurity standard and framework components" In: International Journal of Communication Networks and Information Security. Vol. 12, No. 3, pp. 417-432.

TAHA, Ahmad; QI, Junjian; WANG, Jianhui; PANCHAL, Jitesh. 2018. "Risk mitigation for dynamic state estimation against cyber-attacks and unknown inputs" In: IEEE Transactions on Smart Grid. Vol. 9, No. 2, pp. 886-899.

THAPA, Niraj; LIU, Zhipeng; GOKARAJU, Balakrishna; ROY, Kaushik. 2020. "Comparison of machine learning and deep learning models for network intrusion detection systems" In: Future Internet. Vol. 12, No. 10, pp. 1-16.

TIAN, Qiuting; HAN, Dezhi; LI, Kuan-Ching; LIU, Xingao; DUAN, Letian; CASTIGLIONE, Arcangelo. 2020. "An intrusion detection approach based on improved deep belief network" In: Applied Intelligence. Vol. 50, No. 10, pp. 3162-3178.

UNITED NATIONS. 2008. Human Rights, Terrorism and Counter-terrorism. Available online. In: https://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf. Consultation date: 14/02/2021.

UNITED NATIONS. 2017. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. World Bank and United Nations. Washington, DC, USA.

UNICRI. 2014. Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level, Turin. Available online. In: http://www.unicri.it/in_focus/files/Criminalita_informatica_inglese.pdf. Consultation date: 14/02/2021.

VÄLJA, Margus; HEIDING, Fredrik; FRANKE, Ulrik; LAGERSTRÖM, Robert. 2020. "Automating threat modelling using an ontology framework: Validated with data from critical infrastructures" In: Cybersecurity. Vol. 3, No. 19, pp. 412-420.

VEERASAMY, Namosha; GROBLER, Marthie. 2015. "Logic tester for the classification of cyberterrorism attacks" In: International Journal of Cyber Warfare and Terrorism. Vol. 5, No. 1, pp. 30-46.

VILIĆ, Vida. 2017. "Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace" In: Balkan Social Science Review. Vol. 10, No. 10, pp. 7-25.

WEF (World Economic Forum). 2021. The Global Risks Report 2021. Available online. In: https://www.weforum.org/reports/the-global-risks-report-2021. Consultation date: 11/02/2021.

WILNER, Alex. 2017. "Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation" In: Comparative Strategy. Vol. 36, No. 4, pp. 309-318.

YAU, Hon-Min. 2020. "Evolving toward a balanced cyber strategy in East Asia: Cyber deterrence or cooperation?" In: Issues & Studies. Vol. 56, No. 03, pp. 23-39.

YI, Wen; CHAN, Albert. 2014. "Critical review of labor productivity research in construction journals" In: Journal of Management in Engineering. Vol. 30, No. 2, pp. 214-225.

YU, Yao; OSEI-KYEI, Robert; CHAN, Albert; PING Chuen; CHEN, Chuan; MARTEK, Igor. 2018. "Review of social responsibility factors for sustainable development in public-private partnerships" In: Sustainable development. Vol. 26, No. 6, pp. 515-524.

UNIVERSIDAD
DEL ZULIA

CUESTIONES
POLÍTICAS

Vol.39 Nº Especial

Esta revista fue editada en formato digital y publicada en octubre de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org