DOI: https://doi.org/10.34069/AI/2022.60.12.22
How to Cite:
Pidbereznykh, I., Koval, O., Solomin, Y., Kryvoshein, V., & Plazova, T. (2022). Ukrainian policy in the field of information security. *Amazonia Investiga*, *11*(60), 206-213. https://doi.org/10.34069/AI/2022.60.12.22

Ukrainian policy in the field of information security

Política ucraniana en el campo de la seguridad de la información

Received: November 24, 2022 Accepted: December 27, 2022

Written by:
Inna Pidbereznykh[99]
https://orcid.org/0000-0001-9906-4327
Oleg Koval[100]
https://orcid.org/0000-0001-9578-1759
Yevhen Solomin[101]
https://orcid.org/0000-0001-6770-5505
Vitaliy Kryvoshein[102]
https://orcid.org/0000-0002-3380-7850
Tetyana Plazova[103]
https://orcid.org/0000-0002-8690-1031

Abstract

The article analyzes the modern challenges of the time, which shape the information security policy of Ukraine. The paper analyzes the approaches to the definition of information security to understand this concept. Conclusions are made that information security is a constant movement, changeable, versatile concept, which cannot be stable. The article studies the information security of Ukraine as a component in the system of international information security. It is established that in the conditions of war, the role of information security of Ukraine in the international community has sharply increased. Ukraine's policy in the sphere of economic security is clearly marked in its legislation and meets the challenges of our time. The article presents a list of the main threats to the information security of the country: threats to independence and sovereignty through hybrid, information warfare by the aggressor state Russia, threats in the systems of the interaction of state bodies, threats related to the media, threats due to the lack of awareness and culture of information security among the population. Conclusions are made that future cases in the

Resumen

El artículo analiza los retos modernos de la época, que configuran la política de seguridad de la información de Ucrania. El artículo analiza los enfoques de la definición de seguridad de la información para comprender este concepto. Se llega a la conclusión de que la seguridad de la información es un concepto en constante movimiento, cambiante y versátil, que no puede ser estable. El artículo estudia la seguridad de la información de Ucrania como componente del sistema de seguridad de la información internacional. Se establece que en condiciones de guerra el papel de la seguridad de la información de Ucrania en la comunidad internacional ha aumentado bruscamente. La política de Ucrania en el ámbito de la seguridad económica está claramente marcada en su legislación y responde a los retos de nuestro tiempo. El artículo presenta una lista de las principales amenazas a la seguridad de la información del país: amenazas a la independencia y la soberanía a través de medios híbridos, guerra de la información por parte del estado agresor Rusia, amenazas en los sistemas de interacción de los órganos estatales, amenazas relacionadas con los medios de comunicación,

[99] Doctor of Law, Associate Professor of the Department of History, Faculty of Political Science, Petro Mohyla Black Sea National University, Ukraine.
[100] Candidate of Sciences in Public Administration, Associate Professor Regional Policy Department Taras Shevchenko National University of Kyiv, Ukraine.
[101] PhD in Social Communications, Associate Professor, Head of the Department of Journalism, Faculty of Philology, Uzhhorod National University, Ukraine.
[102] Doctor of Political Science, Professor, Head of the Department of Sociology, Oles Honchar Dnipro National University, Faculty of Social Sciences and International Relations, Ukraine.
[103] Candidate of historical sciences, Associate Professor of Department of Military History, Hetman Petro Sahaidachny National Army Academy, Ukraine.

field of information security will be related to the elimination of threats. A list of goals for achieving information security is presented.

Keywords: cybersecurity, fake, information security culture, information influence of Russia, protection of personal data.

amenazas debidas a la falta de concienciación y cultura de seguridad de la información entre la población. Se concluye que los casos futuros en el ámbito de la seguridad de la información estarán relacionados con la eliminación de las amenazas. Se presenta una lista de objetivos para lograr la seguridad de la información.

Palabras clave: ciberseguridad, falsificación, cultura de la seguridad de la información, influencia informativa de Rusia, protección de datos personales.

Introduction

Ukraine's information security policy in recent years has been aimed at strengthening the development of information technology in the economy and society, as effective information activity of the state can solve many crisis phenomena in the country. With the beginning of a full-scale military offensive in Ukraine, information security has acquired a new urgency. Ukraine's information security has become a link in the system of international security. To cover the issue of Ukraine's information security policy, this paper identified the types of threats to information security in Ukraine, gave clear directions of modern information security, and identified the expected results of its implementation in the future.

Theoretical Framework or Literature Review

Scholars have actively researched the implementation of information security policy. Theoretical and practical aspects of information security have been addressed by van Daalen, (2022), Duan, Xu, Hu & Luo (2022). Scholars agree on the significant role of information security culture among the population (Tejay & Mohammed, 2022), (Kyytsönen, Ikonen, Aalto & Vehko, 2022). Taherdoost (2022) viewed cybersecurity as part of information security. Andersson, Hedström & Karlsson (2022) conducted a structural analysis of information security standardization. Cheng & Bao (2022) analyzed the formation of Chinese universities' attitudes toward the Russian-Ukrainian war from the perspective of media literacy and national security awareness. Steffen & Patt (2022) analyzed early evidence on how the Russo-Ukrainian war changed public support for clean energy policy. Ukraine's information security issues during the war have been addressed by scholars such as Zalievska, & Udrenas (2022), Shopina (2022), Siemko (2022).

Methodology

To implement the objectives, the study was carried out by certain stages in a combination of analysis of theoretical material, legislation of Ukraine, EU norms. Such stages were: search for theoretical data, search for scientific literature; search for legislation; analysis of data and scientific sources; comparison and comparison of the identified data, development of conclusions and recommendations.

The empirical basis of the study were the legislative acts of Ukraine and the EU, scientific works.

For the realization of the set purposes, the research was carried out by certain stages in a combination of analysis of theoretical and statistical material and execution of practical tasks. Such stages were:

1. searching for empirical data and scientific sources;
2. analysis of these data and sources;
3. comparing and contrasting data by year, providing conclusions and recommendations, forecasting.

The system of general scientific and special scientific methods was chosen as a methodological basis. The main method chosen is the analytical method, which allows to identify the impact of current trends in the use and protection of information in Ukraine and the world on the formation of future cases. The integrated method allowed to combine the knowledge and practice of different branches, in particular, sociological, economic, technological, legal research. The synergetic methodology allowed to determine further directions in the field of information policy of Ukraine.

Results and Discussion

Peaceful resolution of crisis phenomena in the state is possible through effective information activity. Ineffective use and distortion of information contributes to negative attitudes in society and negative consequences (Zalievska & Udrenas, 2022). The state, its organizations, and private organizations use information as an asset at different levels of activity. Therefore, these assets are often targeted by cybercriminals and hackers (Andersson, Hedström & Karlsson, 2022). Instead of traditional services, citizens are increasingly being offered electronic services that need information protection skills (Kyytsönen, Ikonen, Aalto & Vehko, 2022). And the right to information is one of the basic human rights secured and guaranteed by the state, such as the right to life, health, freedom, personal security, the standard of living, and culture (Shevchuk, 2021). Information in modern society is of great value, and its security is one of the priority tasks of any state, including Ukraine, which has seen through its own experience the importance of implementing a reliable information policy. As van Daalen (2022) notes, "information security is what you do, not what you have. It is a repetitive process of finding weaknesses and fixing them only to have the subsequent weakness be discovered, corrected, and so on."

International information security occupies a leading place in the system of international information relations. The main components of international information security are: combating cybercrime, countering terrorism, and ensuring security in the military sphere (Siemko, 2022). Ukraine's information security policy is a link in the system of international security, the role of which has significantly increased in wartime.

Considering the conceptual approaches to the definition of information security Shopina (2022) concludes that information security is:

- the current state of information security;
- levels of information development in certain subjects and at certain intervals of time;
- a type of public legal relations arising in the information sphere based on acts of information legislation in order to bring the objects of information security to the desired state for the state and society.
- a set of means, the application of which allows to achieve of the goals set in the system of public administration of the information sphere.
- protection of information and protection of individuals and society from destructive information influences.
- preservation and provision of essential properties of information, in particular its integrity, accessibility, authenticity, and confidentiality.
- process or a set of processes arising and occurring in information and social systems and designed to achieve the goals of public administration in the information sphere.
- the ability of social and information systems to function effectively in the face of intensifying external and internal threats.
- the activity or set of actions with information resources or systems.

Therefore, information security is a constantly changing process, action, and, therefore, the state policy on information security should be active and in constant motion.

Ukrainian legislation defines information security of Ukraine as part of national security, as the state of protection of the basic constitutional norms of independence and sovereignty of Ukraine, and the state of protection of the basic rights of citizens in the field of information, as a system of protection against information influence, propaganda (Decree of the President of Ukraine No. 685/2021, 2021).

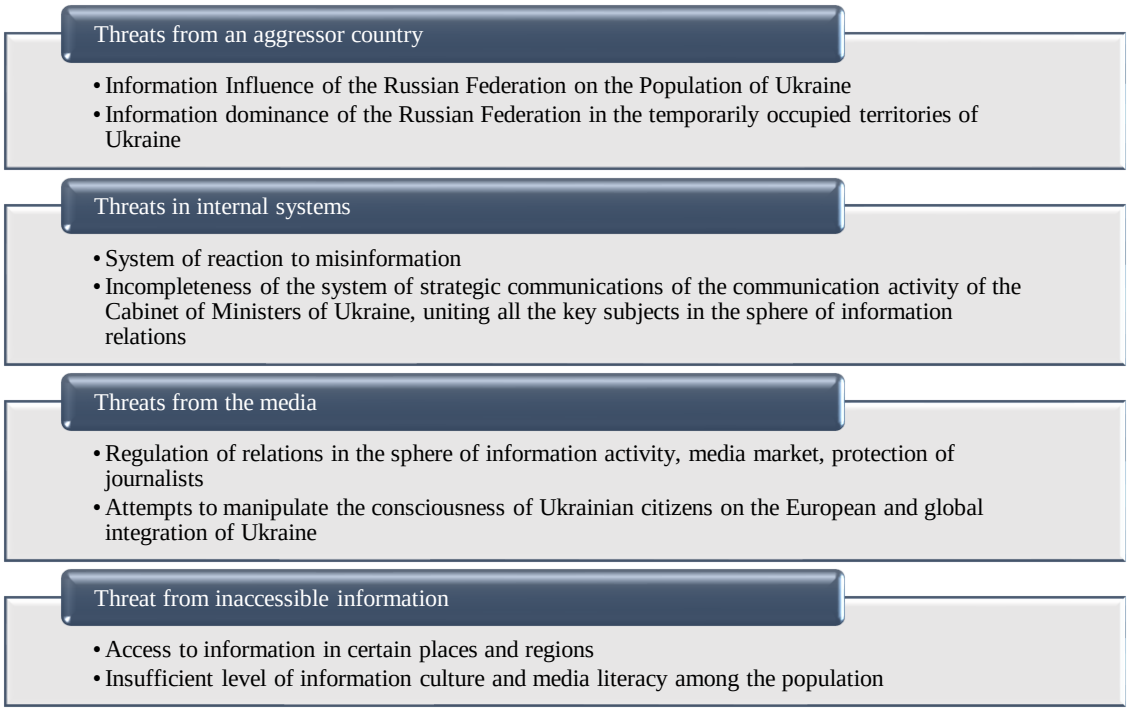

Figure 1. Types of information security threats in Ukraine (Decree of the President of Ukraine No. 685/2021, 2021).

Information security policy primarily depends on existing threats to information security. The above are the main threats to information security in Ukraine. They are the determining directions in the future. With the armed aggression of the Russian Federation, the information threat from this aggressor country has increased, and hybrid information warfare has been added. Therefore, this direction of information security will be decisive and basic in the future. Internal threats included imperfections in the actions and systems of state bodies in the use of information. Russia's war against Ukraine was a test of the maturity of all state bodies of Ukraine (Kaplina, 2022), the war highlighted all problems related to strategic communications. Many were resolved promptly, but further work in this direction should be continued. A separate threat to information security rightly singles out the activities of the media and the protection of the professional activities of journalists, especially in war conditions. Society must have information awareness and consciousness, access to information, and critical perception of it. In order to form information security, it is necessary to carry out a number of measures on the use of information by the population - to provide access in the most remote areas, to carry out information and awareness-raising work with citizens to form their personal information security.

Zalievska & Udrenas (2022) point to the following directions of modern information security in Ukraine:

1. Information security aimed at the protection of values and the state in connection with a full-scale military invasion, against the actions of the aggressor aimed at the independence of Ukraine, its territorial integrity, and sovereignty;
2. Information protection of Ukrainian culture and self-determination;
3. Work to increase the level of consciousness of the society, its media literacy, skills, development of the information society;
4. Work in the sphere of realization of information rights of an individual;
5. Work with information provision of Ukrainian citizens living in the temporarily occupied territories;
6. Strengthening the reliability of the system of strategic communications, information security at the international level.

Ukraine actively pursued a policy of information protection in the pre-war period, but now it is facing new tasks, protection from new threats of hybrid warfare, countering disinformation and “fake” news, and preserving the information stability of society in war conditions. For it is this war that is characterized by encroachment on the information and cybernetic space of Ukraine, on the constitutional foundations of democracy,

independence and on the information and psychological security of the population of Ukraine (Nevelska-Hordieieva & Nechytailo, 2022).

The Russian Federation's full-scale attack on Ukraine has increased the urgency of protecting the information security of the state and society (Shopina, 2022, p. 134). The role of information as a military-strategic resource is increasing and has been compared to the role of military equipment and weapons. Information, its security refers to the defense potential of the country (Toffler, 1993, p. 45). Information technology is widely used for military purposes for the defense of Ukraine and is in the protection of Ukraine from armed aggression, as ammunition, transport, weapons (Zalievska & Udrenas, 2022). Manipulative influence on society has been used to achieve certain political or economic influences and outcomes. Russia's military invasion of Ukraine was preceded by a public information campaign, both within and outside of Ukraine. In a full-scale war, such influences are used for other purposes. The fake news technique is one of the most popular; it is the distribution of false information in social media, to mislead the public. The use of these types of manipulative techniques requires the state to constantly monitor and respond (Nevelska-Hordieieva & Nechytailo, 2022).

The state has a direct influence on the formation of information awareness in society; it regulates, at the legislative level, the flows of information that circulate in society. It depends on its internal policies.

For example, in China, because of restrictions and controls on people's access to foreign sites and other resources, officials have restricted access to information contrary to their views. To maintain social harmony and stability. This information policy allows coverage of events in Ukraine from a different perspective than the Western media (Cheng & Bao, 2022) and shapes public sentiment to support the aggressor state of Russia.

In contrast to China, European countries direct their information policy toward the formation of a culture of information security and legal consciousness. Thus, communication ties are developing between Ukraine and Latvia, covering different spheres of activity of the states, their common historical ties, and common tasks in overcoming the totalitarian Soviet past (Krasnozhon, 2021). “The Russian attack was widely condemned in the West, including by almost all European governments, and was met with military, humanitarian, and financial support for the Ukrainian government, as well as economic and social sanctions against Russia and many of its elites” (Steffen & Patt, 2022).

Duan, Xu, Hu & Luo (2022) have concluded that the weakest links in information security are individuals in organizations, as direct users of the organization's information resources, with access to closed databases that they use in their daily work. Pliekhova & Kostikova (2022) rightly pointed out that the most critical and important decisions must be made by humans, so the protection mechanisms must be hidden from users whose work is under control. All this forms a culture of information security. Its development will further lead to a secure organization. Through surveys, scholars have found that information security culture is influenced by group cohesion, professional code, information security awareness, and informal work practices (Tejay & Mohammed, 2022). Therefore, the information security culture of the state is the information security culture of the individual and society.

The European Union General Data Protection Regulation requires that data be processed in a lawful, fair, and transparent manner and that it be protected from unauthorized and unlawful processing and from accidental loss, destruction, or damage (European Parliament and Council of the European Union, 2016). This is due to the large amount of electronic data, including personal data, requiring confidentiality, integrity, and availability of the generated data. And a breach of personal databases can have dire consequences for both the state and the citizen. Therefore, states must investigate information security vulnerabilities and be sure to conduct research to strengthen information security (van Daalen, 2022). With the rapid development of information technology, states, organizations, and people are becoming dependent on the use of information systems, and the role of information security is increasing. The negative consequences of information security breaches have included decreased consumer confidence, impact on international and national politics (Duan, Xu, Hu & Luo, 2022). In Ukraine, programs are used to enable remote access to various databases, signing documents, indicating the rapid development of information technology. security in these areas.

Cybersecurity, which provides information security in cyberspace, in computer systems against attacks or unauthorized access, occupies

a significant part of the information security of the state. Considering the differences between cybersecurity and information security in different aspects, it should be noted that cybersecurity protects cyberspace from cyber-attacks, while information security considers the protection of information from threats of all forms, both digital and physical (Taherdoost, 2022).

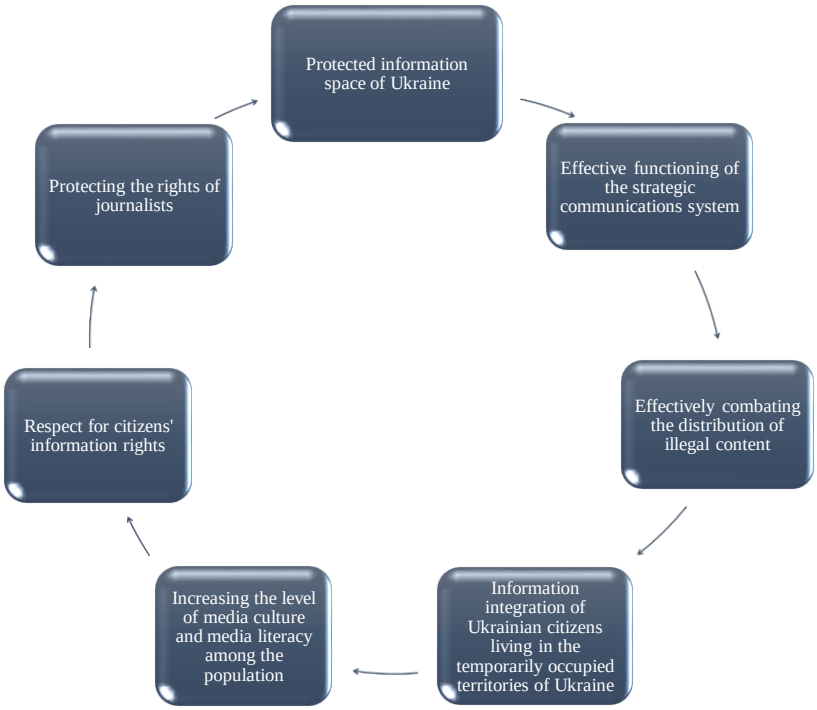

Figure 2. Expected results of the information security policy of Ukraine in the future.
Source: (Decree of the President of Ukraine No. 685/2021, 2021).

Ukraine has clear goals and ideas about the results of activities in the field of information security. Ukraine's information security policy responds to modern information challenges. Through Ukraine's integration into the world community and globalization of the economy, it is actively introducing the latest information technologies and tools, and information is an important part of its activities. Therefore, the future cases of Ukraine in the sphere of information security will concern the development of a culture of information security of citizens, increasing the level of media literacy, compliance with the rights of citizens in the protection and use of information, protection of journalists' rights. Along with global trends in information security, Ukraine has its own, aimed at overcoming Russian aggression in any form.

Conclusions

After conducting this study, we can make a number of conclusions. Information security in the modern world occupies one of the main places in the system of international and national security. As a result of the analysis of scientific literature, we can say that information security is a continuous action, a process aimed at preventing, identifying, and eliminating threats in the field of information management. Ukraine has developed and operates an information security strategy that reflects current challenges, but which needs to be slightly amended and changed due to military actions on the territory of Ukraine. This issue requires further research and developments. We have revealed that threats to the information security of Ukraine are as follows: actions of the Russian Federation in information and cyberspace aimed at the depreciation of the Ukrainian statehood, the overthrow of the state system of Ukraine; advantage of the Russian media and Internet resources on the territory of the temporarily occupied Donetsk and Lugansk regions; imperfect internal information systems and communication of the state authorities; inaccessibility of information in remote, rural and sparsely populated areas, not formed During military operations on the territory of Ukraine, information becomes as important and relevant as equipment and weapons. Information

technology is widely used for military purposes for the defense of Ukraine.

The future of information security in Ukraine lies in the provision of information within the country, taking into account the tasks arising as a result of military action in Ukraine. Violations in the sphere of information security have led to the current situation with the awareness of events, in particular in the territory of Luhansk and Donetsk regions. Now the issue of information security is one of the most discussed and problematic in Ukraine, it has acquired a great solution, improvement, and rapid development. Undoubtedly, taking into account conditions of martial law, Ukraine should take into account global trends in information security. At the same time, the countries of the world are observing the information war in Ukraine and are participants in this war. Because they present information to their citizens, taking into account the political beliefs and economic benefits of politicians. Information security in the modern world is the basis of any country, the legal consciousness of its people, and civil society. At the same time, it is important to build information security skills in each citizen individually. The formation of the information security skills of an individual citizen will prevent the manipulation of information by individual politicians and totalitarian states.

Bibliographic references

Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing information security – a structurational analysis. Information & Management, 59(3), 103623. https://doi.org/10.1016/j.im.2022.103623

Cheng, L., & Bao, R. (2022). Media literacy and national security awareness: The formation of Chinese higher education groups' attitude to the Russia-Ukraine war. Social Sciences & Humanities Open, 6(1), 100373. https://doi.org/10.1016/j.ssaho.2022.100373

Decree of the President of Ukraine No. 685/2021. On Information Security Strategy. of December 28, 2021. https://zakon.rada.gov.ua/laws/show/685/2021#Text

Duan, Q., Xu, Z., Hu, Q., & Luo, S. (2022). Neural variability fingerprint predicts individuals' information security violation intentions. Fundamental Research, 2(2), 303-310. https://doi.org/10.1016/j.fmre.2021.10.002

European Parliament and Council of the European Union. (2016). General Data Protection Regulation 2016/679. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Kaplina, O. (2022). Prisoner of War: Special Status in the Criminal Proceedings of Ukraine and the Right to Exchange. Access to Justice in Eastern Europe, 4-2(17), 8-24. https://doi.org/10.33327/AJEE-18-5.4-a000438

Krasnozhon, N. (2021). Ukrainian-Latvian communication ties in the conditions of informatization and digitalization of societies (1991-2020). Society. Document. Communication. Society. Document. Communication, 11, 160-185. https://doi.org/10.31470/2518-7600-2021-11-160-185

Kyytsönen, M., Ikonen, J., Aalto, A., & Vehko, T. (2022). The self-assessed information security skills of the Finnish population: A regression analysis. Computers & Security, 118, 102732. https://doi.org/10.1016/j.cose.2022.102732

Nevelska-Hordieieva, O., & Nechytailo, V. (2022). The phenomenon of fake news in the context of information security of the state. Vestnik (Herald) of the Yaroslav the Wise National University. Series: Philosophy, Philosophy of Law, Political Science, Sociology, 1(52). https://doi.org/10.21564/2663-5704.52.250655

Pliekhova, H. A., & Kostikova, M. V. (2022). Modeling and information technology in science, technology, cybersecurity, and education. Actual problems of information security. Proceedings of the All-Ukrainian Scientific and Practical Internet-Conference "Modeling and Information Technologies in Science, Technology, Cyber-security, and Education". Kharkov National Automobile and Road University. http://surl.li/eosaf

Siemko, M. O. (2022). UN normative activities on information security in the military sphere. Legal Scientific Electronic Journal, 8/2022, 580-583. https://doi.org/10.32782/2524-0374/2022-8/132

Shevchuk, L. (2021). Environmental rights of citizens and legal safeguards for their protection: challenges for the future. Futurity Economics & Law, 2(1). https://doi.org/10.57125/FEL.2021.06.25.1

Shopina, I. M. (2022). The concept of information preservation: conceptual approaches to the definition. Scientific and Informational Bulletin of Ivano-Frankivsk University of Law named after King Danylo Halytskyi. Law Series, 13(25).

https://doi.org/10.33098/2078-6670.2022.13.25.133-140

Steffen, B., & Patt, A. (2022). A historical turning point? Early evidence on how the Russia-Ukraine war changes public support for clean energy policies, Energy Research & Social Science, 91, 2022, 102758. https://doi.org/10.1016/j.erss.2022.102758

Taherdoost, H. (2022). Cybersecurity vs. Information Security. Procedia Computer Science, 215, 483-487. https://doi.org/10.1016/j.procs.2022.12.050

Tejay, G. P., & Mohammed, Z. A. (2022). Cultivating Security Culture for Information Security Success: A Mixed-Methods Study Based on Anthropological Perspective. Information & Management, 103751. https://doi.org/10.1016/j.im.2022.103751

Toffler, A. (1993). War and Anti-War. N.Y.: Little, Brown and Company, 302 p.

van Daalen, O. (2022). In defense of offense: Information security research under the right to science. Computer Law & Security Review, 46, 105706. https://doi.org/10.1016/j.clsr.2022.105706

Zalievska, I. I., & Udrenas, H. I. (2022). Ukraine's information security in the face of Russian military anger. Law Journal, 20. https://doi.org/10.32850/sulj.2022.1-2.4