RedFame

Studies in Media and Communication
Vol. 11, No. 7; December 2023
ISSN: 2325-8071 E-ISSN: 2325-808X
Published by Redfame Publishing
URL: http://smc.redfame.com

The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War

Serhii Lysenko[1], Oleg Marukhovskyi[2], Andrii Krap[3], Sergii Illiuschenko[4], Oksana Pochapska[5]

[1]PJSC "Higher Education Institution "Interregional Academy of Personnel Management", Kyiv, Ukraine

[2]University of Economics and Law «KROK», Kyiv, Ukraine

[3]Precarpathian Mykhailo Hrushevsky Institute of the Private Joint Stock Company "Higher education institution "The Interregional Academy of Personnel Management, Truskavets, Lviv region, Ukraine

[4]National Defence University of Ukraine, Kyiv, Ukraine

[5]Institute of Philosophy and Sociology, Polish Academy of Sciences, Kamianets-Podilskyi Ivan Ohiienko National University, Kamianets-Podilskyi, Ukraine

Correspondence: Andrii Krap, Precarpathian Mykhailo Hrushevsky Institute of the Private Joint Stock Company "Higher education institution "The Interregional Academy of Personnel Management, Truskavets, Lviv region, Ukraine.

Received: August 2, 2023 Accepted: September 16, 2023 Online Published: September 19, 2023

doi:10.11114/smc.v11i7.6414 URL: https://doi.org/10.11114/smc.v11i7.6414

Abstract

The appearance of significant transnational information processes has given rise to new threats to international security, such as information warfare. The problem of employing information warfare, which has become particularly acute and relevant, can be observed through the example of the full-scale war between the Russian Federation and Ukraine. Numerous information attacks by the aggressor country in the form of fake news dissemination confirm this. The latter requires in-depth study for the development of countermeasures, the application of combat algorithms, and the organization of modern information security.

This article aims to introduce a methodology of information security based on several advanced defensive administrative measures, including a review of a series of response cycles to information attacks, mainly when conducted through hybrid and information technologies in the context of the Russian-Ukrainian war. Given the rapid dynamics of contemporary information processes and associated information threats, a complex set of countermeasures is necessary enabling an effective response to threats and timely prediction.

The research methodology is based on general scientific and empirical methods of analysis and scientific cognition, including observation, systemic analysis, classification, scientific abstraction, statistical analysis, analogy, graphical generalization, and systematization. According to the results of the conducted research, it has been established that the distribution of managerial decisions into "fast" and "slow" allows for combining response to attacks with information accumulation to identify the most vulnerable elements and predict future information warfare. In particular, a process of responding to information attacks consisting of several stages of administrative measures has been proposed. Attention is given to the need to consider the initial data for further use in each relevant war period when repeating the cycle following the completion of the specified four-step countermeasure algorithm. Additionally, it has been identified that transmitting data on unlawful aggressor attacks to the information collection system requires careful planning and coordination among various operations and structures. The authors have substantiated and proposed the necessity and application of coordinated administrative measures among information security entities.

Keywords: information warfare, information weapons, hybrid warfare, information security, information threats, measures to counter informational aggressions, the algorithm of countering in information warfare, information operations and attacks

1. Introduction

The present-day political and military conflicts are creating a new environment of information threats, becoming increasingly complex and dynamic. This issue became evident during the full-scale attack of the Russian Federation on Ukraine, with the aggressor employing malicious information technologies on public information resources and temporarily occupied territories. Other countries have also frequently been targeted by aggressors wielding various instruments and using various constantly evolving tactics. However, the control measures aimed at enhancing information security, which worked effectively just yesterday, may need to be revised to halt the same aggressors' attack literally the next day. That is possible because the vulnerabilities and strengths in information security are not static and often become apparent only after an attack, which may be too late to counter.

The global community is raising the question of effectively countering information attacks (operations) and seeking strategies to deter the aggressor country, necessitating the development of effective tools. In such a complex environment, it is crucial to abandon attempts to create a general list of priorities for ensuring peace and security on a global scale. The most critical issue in international relations remains to recognize the fallacy of such an approach, where attempts are made to protect everything simultaneously. Therefore, the urgent resolution of existing problems, as a primary task of international policy, has determined the subject matter of this study.

2. Literature Review

The problem of studying information warfare and developing algorithms to counter information threats is relatively new and increasingly attracting the interest of the international scientific community. However, ensuring peace and international information security is subject to significant destabilizing influences from global factors and dangers.

Modern military conflicts pose a significant threat to the global community due to their hybrid nature, which combines conventional armed and unconventional information methods of influence and warfare. In October 1998, the US Department of Defense introduced the "Joint Doctrine for Information Operations." This doctrine has consolidated algorithms for developing the concept of information warfare and security and refined key definitions to facilitate uniform approaches and coordination of armed forces command at all levels. Information operations (attacks) are defined in the same document as "actions aimed at complicating the collection, processing, and storage of information by the enemy's information systems while simultaneously protecting one's own information and information systems." Information warfare in the "Joint Doctrine for Information Operations" is described as a "comprehensive influence, a set of information operations (attacks) on the enemy's state and military management system, on its military-political leadership. In peacetime, they compel the opponent to make favorable decisions for the side initiating the information influence and completely paralyzes the functioning of the enemy's management infrastructure during the conflict."

As a result of information attacks, public awareness is clouded by harmful information that alters the system of values and interests of people, undermining a state's sovereignty and violating its territorial integrity. As Dawson (2022) emphasized in his research on the Russian-Ukrainian armed conflict, the use of information operations and prohibited warfare methods calls for reforming international law to address problematic aspects in enhancing overall information security.

In 1995, the National Defense Institute of the United States published M. Libicki's work titled "What is Information Warfare?" which outlined the main characteristics of information weapons as components of an information attack or operation. The primary elements of information weapons were identified as follows:

– duplication of intelligence information.

– disinformation.

– psychological operations.

– physical destruction of enemy information resources.

– attacks (physical and electronic) on their information structure.

– infection of computer networks with viruses, penetration into information networks.

A similar opinion is shared by Lederer (2022), who noted the need to adopt relevant laws at the level of UN member states to restrict and prohibit the use of harmful information resources, the development of an information security model, and control protected societal interests. Varenko, V. M. (2014) established that even large countries with substantial budgets are still forced to compete with others for specialists, and time, unfortunately, will always remain a limited resource. It is not possible to protect everything at once. This truth has been verified by centuries of research by philosophers, politicians, and military thinkers. "He who defends everything defends nothing," claimed King Frederick II of Prussia.

Interestingly, according to Volohin Yu. (2011), the algorithm for ensuring information security somewhat resonates with the classical understanding of management functions. At one time, M. Mescon, M. Albert, and F. Khedouri (1988) proposed four fundamental management functions: planning, organizing, motivating, and controlling. Therefore, information security management can be based on general science principles, even during direct military aggression or hybrid attacks.

Any stage of the administrative process involves the involvement and training of relevant experts to utilize organizational resources, capabilities, and processes in the event of an information attack. In particular, Kai-Fu Lee (2020) notes that selecting institutions for disseminating information resources becomes paramount, as their use for criminal purposes creates conditions for developing information and hybrid military conflicts.

The analysis of conflicts and threats is a systematic process, as Nobel laureate Daniel Kahneman (2017) stated in his book "Thinking, Fast and Slow." Therefore, when conveying the researcher's opinion regarding the influence of information on individuals, it is worth identifying the types of decisions made by people that can be divided into two categories:

– quick decisions that serve as protection against harm and satisfy lower-level needs in Maslow's Hierarchy of Needs.

– slow (deliberate) decisions result from investing time in contemplating causes and consequences and applying the correct information security model to analyze the results.

Levchuk N. (2018) revealed the algorithm of common threat intelligence proposed by Krizan at the US Joint Military Intelligence College. It is designed to ensure a continuous process of developing administrative decisions on urgent issues. Furthermore, the author's approach allows adapting this algorithm to combat information threats during hybrid attacks and information operations.

The scientific approach of Reynolds C. (2020) enables the management of information threats individually while providing each administrative measure with the necessary information for the seamless operation of the country's information security. The relevance of such an approach will continue to grow, considering, for example, the proliferation of e-government technologies.

Examining specific research in creating information security models, one can conclude the existence of clear patterns in their construction. For example, in the study by Lysenko S.O. (2019), it can be noted that the structure of the information security model is formed when there is complete information about losses, including threat information, control weaknesses, and the type of economic impact corresponding to CIA methodologies. Forecasts of maximum losses and damage can be used together with data on attacks to focus the state's resources on specific actions through which aggressors or internal individuals can carry out their attacks.

In current conditions, the problem of countering the use of information weapons has become particularly acute and global. Moreover, certain developments in this field have already been made. Mechanisms and tools for such countermeasures have been formed, one of which is the creation of specific information security models. However, due to significant destabilizing factors of a military nature intensifying in 2022, there is a need for further research to find ways to address the problematic aspects.

3. Aims

The aim of the article is to investigate the theoretical and practical underpinnings and potential strategies for establishing robust information security measures and developing corresponding information security systems within nations. This endeavor seeks to effectively counter information operations, attacks, and warfare. Additionally, the research aims to assess the feasibility of integrating specific response algorithms for addressing information attacks and threats into information security systems through protective administrative actions, thereby strengthening overall information security systems.

4. Materials and Methods

The essence of scientific categories such as "information warfare" "information weapons" and "information threat, attack, operation" was defined in the study. The investigation into the current state and trends in the application of algorithms to counter information attacks for resistance and damage reduction was carried out, with a focus on statistical analysis, comparison, and analogies. The chosen topic underwent empirical research, and graphical and tabular methods were used to present the findings. Lastly, the main conclusions were formulated based on the results of the conducted research, utilizing the methods of generalization and systematization. The informational base of this study comprised the research works of leading scholars in information security and countering information operations.

5. Results

The threats arising from the emergence of new information warfare and personal attacks have been amplified under the influence of contemporary geopolitical challenges and threats. Furthermore, the increasing threats of transnational crime, terrorist organizations, and certain states necessitate constructing and developing an international information security system. These aforementioned threats are becoming more pronounced every day and pose the risk of immediate large-scale destructive effects and the creation of catastrophic situations.

Recent scientific and practical research in this field indicates the impossibility of acquiring ready-made information weaponry, but its creation does not require significant material investment. Certain patterns can be identified by employing an imperative and experienced approach, and administrative rules can be formulated to combat aggressors effectively. The aggression of the Russian Federation against Ukraine has become the first war that is well-documented and observed by the global population through the World Wide Web.

At the outset of the invasion, it was evident that Ukraine gained the upper hand in the information domain, which helped garner significant international support. Within Ukrainian society, for instance, a video clip showing a Ukrainian farmer chasing away a Russian tank with his tractor significantly boosted the morale of the entire population. However, these narratives compete for influence in a space flooded with enormous disinformation from the aggressor. Navigating through this torrent of information warfare is a strategic task for any information security system.

The current adversary of Ukraine operates incessantly within accessible information environments facilitated by widespread internet access and an abundance of virtually unlimited media narratives. However, drawing from the American experience in managing information operations by special units, it is evident that Ukrainian entities responsible for information security will be considerably less effective beyond the territories occupied by Russia if they lack analytical capabilities that enable them to counter unlimited information flows effectively.

Yet, more than developing defensive administrative mechanisms within information security units is required. The clear algorithms and the speed of their implementation are also crucial. Practical studies have shown that simply countering fake news with accurate information is not always effective due to cognitive biases and the misinformation effect. Sometimes, manipulated information alters people's perception of past events. Therefore, it is crucial to include the requirement of speed in the interaction with hostile narratives in protective administrative algorithms before they gain popularity.

The mentioned dynamics are manifested in the war in Ukraine. The adversarial component of information warfare relies on government-funded networks and secret channels to disseminate disinformation. Information warfare, propaganda, and cyber-attacks on Ukrainian infrastructure aim to break the will of the Ukrainian people to resist. Within its own country, Russia directs its efforts towards its citizens, blocking foreign social networks and news platforms to promote its own propaganda of invasion simultaneously. This policy has created a restricted information environment within Russian society and further divided the country between those who trust state-controlled media and those who bypass censorship.

Against this backdrop, for more effective information security management, it is advantageous for entities to implement administrative measures that should be focused on using threat intelligence. These measures will better prepare specialists in gathering external information, who can also be better equipped to defend if they utilize pre-collected data on likely attacks. Such a combination of threat intelligence and information aggression should form the basis of defensive administrative measures to counter them. The established information security system should be the result of combining various algorithms that may differ in their objectives, but their interaction should be mutually beneficial.

Responding to information attacks should consist of the following stages of defensive administrative measures:

– preparation;

– detection and analysis;

– containment and threat elimination;

– recovery after aggression.

After completing this four-step algorithm, the obtained data should be considered for further use in each war period when repeating the cycle.

At the same time, there can be an interpenetration of the mentioned stages of administrative measures and management functions, but not their duplication. Therefore, the researched algorithms become an essential component of effectiveness in the preparation, detection, and analysis and in the process of containment, elimination, and recovery after aggression.

Responding to information attacks is an administrative process that benefits from proper planning, and its *first phase* describes it clearly. In this case, the target of the attack, according to the algorithm of defensive administrative measures, will mobilize the resources necessary for a proper response. For example, it may involve acquiring technologies required to assist, configuring computing assets to search for relevant evidence in the event of an attack, and implementing signals to alert personnel of the occurrence of an attack. Finally, this process stage includes the involvement and training of appropriate personnel to utilize administrative resources and capabilities in the event of a confirmed attack. The first phase is particularly crucial as its successful implementation allows for the most advantageous position, thereby increasing the likelihood of success in subsequent phases. On the other hand, a failed first phase or a lack of response at this stage is difficult, and sometimes impossible, to compensate for in the future.

In the *second phase*, detection and analysis, the need for early threat notification in the environment of the target of the information attack is regulated. It primarily requires the presence of experts who gather information and technical specialists capable of analyzing the collected data based on a set of reference indicators to determine the priority of actions both now and during each subsequent phase. A characteristic feature of this phase is a relatively high degree of positive and negative results that can be obtained from monitoring and making administrative decisions. More advanced countries establish a priority rating scale in such cases, enabling rapid classification of the received information and timely response to specific indicator changes. Implementing these priorities is an excellent opportunity for administrative regulation of threat intelligence processes since knowledge of them at the early stage of the information operation is crucial for optimizing management in the future.

The *third phase* of the algorithm involves implementing defensive administrative measures aimed at localizing and ultimately halting the information operation. It entails, first and foremost, limiting the spread of the information attack, terminating physical access of the aggressor and their equipment to protected objects, as well as ceasing the exchange of data that has been targeted and could be damaged. The most typical situations include:

- data theft.
- personal information compromise.
- financial credentials compromise.
- restricted-access information compromise.
- dissemination of false and harmful information.

However, it should be noted that one of the reasons for an information attack can be indirect damage to the target. For example, it may involve substituting specific data, statistical reporting, or information that undergoes social analysis to deceive state leadership or divert public attention.

It is easy to model a situation where aggressors initially create "information weapons," such as disinformation about the activities of state leaders or partner countries, actual or fictitious compromising materials, and only later generate an attack on related information resources through a different approach. In such cases, the attack's goal is not necessarily the theft of specific information, which can divert the attention of the information security system and provide its experts with a false sense of understanding the situation but rather draw attention to a pre-planned surprise. Moreover, it cannot be excluded that such an information operation can yield double or even triple benefits. For example, an attack allows for the theft of valuable information, damage to other important information, and, at the same time, diverts the attention of the target's leadership toward pre-placed disinformation.

This phase also involves restoring the information security system and returning it to its state before the attack. During this phase, data and evidence should be collected for possible transmission to law enforcement agencies or special services to make decisions regarding further international criminal court proceedings.

The *final phase* of the algorithm is responsible for responding to the attack and essentially focuses on integration with other defense participants. Therefore, carefully collecting data and preparing the obtained information is necessary. This process may include a forecast to be used by other entities to determine where precisely the weaknesses in the information security system are and, accordingly, whether similar attacks can be expected in the future. The preventive component of the final phase involves planning protective administrative measures that will help prevent the recurrence of such information attacks.

Meanwhile, it is necessary to note that countering information operations issues are quite significant. Therefore, an additional characteristic of the phases of the response algorithm should be provided using Table 1.

Table 1. The characteristics of the main phases of the response algorithm

No.	Phase type	Phase characteristics	Main directions of action
1.	First	Proper planning and resource mobilization	Acquiring the necessary technologies to provide assistance, configuring computing assets to search for relevant evidence in case of an attack, and implementing alerts to notify staff of an attack
2.	Second	Detection and analysis	Timely threat notification, analysis of selected information based on a set of reference indicators to determine the priority of actions now and during each subsequent phase
3.	Third	Localization and complete cessation	Limiting the spread of the information attack, preventing physical access by the aggressor, their equipment, and malicious programs to protected objects, as well as halting the exchange of data that has been targeted by the attack and could be damaged
4.	Fourth (the final)	Responding to an attack	Integration with other defense participants, preparing the received information for use, forecasting its use by other entities to identify weaknesses in the information security system, and planning administrative measures to prevent the recurrence of similar information attacks

Author's elaboration

The specified algorithms are intended to minimize threats from an information attack and transform it into a specific information set to optimize the management system further. The level to which actions are taken in the state and society may imply eliminating technical details but will always include a description that summarizes what has happened, transforming it into material that helps decision-makers understand what has occurred. Analysts' assertions regarding necessary defensive administrative actions gain convincing power through this. Information can and should be used as input to the initial phase to aid in preparation for countering the next information attack. This gathered intelligence information on threats can also be used alongside similar externally obtained information on potential threats as a critical contribution to the next cycle of information operations. Sometimes, this information is included in the information security system's data collection and processing array.

As part of the overall algorithm of active measures of the information security system, the intelligence algorithm of general information threats ensures a continuous process of developing administrative decisions on urgent issues.

The first stage of this algorithm is to fully understand the questions that need to be answered during threat intelligence and why they are important. Then comes the assessment of what data needs to be collected to address the specified questions. This part should be familiar to any researcher as it forms the basis of any scientific investigation.

The second stage involves data collection or even just identifying the sources from which the data can be obtained and initiating the necessary technologies and processes for data generation. Once the required data has been collected, the information security entity analyzes, processes, and transforms it into actionable information. Essentially, it involves implementing defensive administrative measures based on various sources of information. Analogous to the algorithm for responding to information attacks, it includes detecting facts, drawing conclusions, and predicting what can be expected next. Ultimately, this information is disseminated in various places, including by threat analysts. In the presented framework, this algorithm sits between the stages of attack response and threat intelligence, thus contributing to both. It allows for managing threats and attacks separately while also providing the necessary information for the uninterrupted operation of the information security system.

Threat analysis is generally less sensitive to administrative protection measures than intelligence. The main reason, in the author's opinion, is that despite the possibility of the aggressor finding ways into the target's information environment through different and numerous means, the attack itself tends to be more fixed. For example, the attacker's ability to exploit vulnerabilities in the country's information systems may change over time, but the result will likely be the same. Therefore, quantitative variables are necessary for threat intelligence and are included in the study. In general, it is helpful to think of the threat intelligence phase as an abstraction of the details needed to implement defensive administrative measures when addressing information security issues.

Considering the importance of the information threat intelligence algorithm, let us update it in Figure 2.

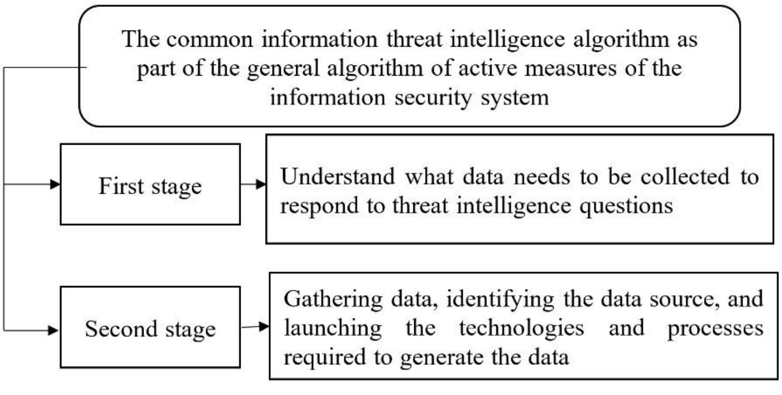
The common information threat intelligence algorithm as part of the general algorithm of active measures of the information security system
First stage
Understand what data needs to be collected to respond to threat intelligence questions
Second stage
Gathering data, identifying the data source, and launching the technologies and processes required to generate the data

Figure 2. Algorithm for common information threats intelligence

Author's elaboration

It is worth noting that the application of algorithmic methods as a tool to counter information operations (attacks) can be implemented concerning individual perpetrators, groups, units, and the aggressor country as a whole. In this regard, the mechanism of applying algorithms involves the implementation of international legal (conventional) and global organizational (institutional) tools. Collectively, they are aimed at preventing and countering information warfare through the use of contractual and customary norms, decisions of international organizations, and the influence of other states and international bodies.

Considering the current state and trends in the use of algorithms as a means of preventing and countering information aggression, it can be observed that they have a coercive nature as a response to criminal actions, aiming to restore violated rights and ensure various forms of accountability for entities carrying out information attacks.

6. Discussion

The preservation of peace and security on a global scale remains one of the priority directions of modern international relations. It is evident that the presence of ongoing military conflicts and the deployment of full-scale combat operations on the territory of the European continent indicate a weakening of security systems. Furthermore, Russia's initiative to initiate the war and its use of informational weapons in information attacks speaks to the implementation of full-fledged information warfare along with its classical components. Mass information attacks demonstrate threatening trends for the further development of events and processes. Undoubtedly, the problem of countering information aggression has become particularly acute and transformed into an active phase in current conditions, necessitating the formation of a set of effective algorithms.

As mentioned above, additional information is used as input data necessary for threat intelligence. This information is characterized by two variables often employed by aggressors regarding internal users. Firstly, it involves information on how often they make mistakes and when they do so. Secondly, it pertains to the resources they can employ to avoid accountability in case of an error. A related variable indicator can be the community profile, which serves as a universal tool for communication in society. It helps determine detailed information about the objectives and tasks of attackers.

For instance, if aggressors can pose a threat with their attacks in terms of time, skills, and resources, it can be said that they are the most dangerous (let's say 99%). Thus, the danger they pose would amount to 99%. These values should also be maintained along with threat data, enabling information security entities to clearly and promptly understand the nature of these attackers. It is important to rely on an assessment that indicates whether an information attack of a particular type has been correlated with society's information security level. Only the question of whether an information attack of such a type is part of broader, abstract information operations (attacks) is relevant.

After completing several cycles of risk analysis, a list of the most significant threats is obtained. It is important to note that they are formed with complete information about the losses, including information about threats, weaknesses in control, and the type of economic impact (corresponding to CIA methodologies). These forecasts of maximum losses can be used in conjunction with information about information attacks to focus management on key actions through which aggressors or internal actors can carry out their attacks.

In summary, each of the aforementioned algorithms has its advantages and usefulness for different protective and administrative measures of information security for the country and society. Combining them allows for a comprehensive view of an organization's data collection. Specifically, it will enable us to observe how these algorithms interact and which administrative measures can be mutually beneficial for each specific managerial decision. As a result, the proposed measures will allow the desired results to be achieved and somewhat reduce the level of impact from threats of information attacks.

7. Conclusion

The conducted research on theoretical and practical bases and the possibilities of using algorithms as a tool to counteract information operations (attacks) and warfare, in general, give reasons to assert that they are a powerful instrument of deterrence, prevention, and resistance to the conduct of information operations (attacks) in the modern era. Based on the obtained results, it can be concluded that the threats of information warfare are constantly escalating and intensifying, which requires the development of effective measures to counteract them.

There is often a certain distance between management functions, threats, the adoption of defensive administrative measures, and the entities involved in information gathering. That is not coincidental, as each function differs significantly in nature. However, only the comprehensive interaction of all these components of information security allows for a better understanding of the role of each of them and a better realization of the reality of the threats faced by everyone in modern warfare.

Risk management teams require professionals in the administrative field and experts in assessing information threats and operations. Using algorithms concerning information attacks as organizational measures grants each group clear rights and responsibilities. It can stimulate cooperation where it may not have existed before and create professional commitments that enable more effective collaboration, thus enhancing the quality of the information security system.

Many countries are working on improving their reporting on information security matters to their leadership and command. For them, searching for effective administrative measures that can lead to positive results and neutralize potential losses in the information space is one of the key tasks. The tight regulation of algorithms, phases, and specific stages, as well as the adoption of defensive administrative measures and data exchange among entities, can help consolidate and optimize approaches to ensure information security and bring about the highest effectiveness of the defensive measures taken. Furthermore, it is essential to consider that the implemented administrative measures should adhere to the principles of balance and equilibrium between the actions of the entities involved in information security.

Acknowledgments

Not applicable

Authors contributions

Serhii Lysenko researched sources of information were responsible for study design and revising. Oleg Marukhovskyi carried out the data collection and was responsible for and was responsible for the layout of the article. Andrii Krap carried out the systematization of the processed sources and made the introduction to the article. Sergii Illiuschenko worked on the research results section and drafted the literature according to requirements. Oksana Pochapska systematized the scientific material in other sections of the article, was responsible for the abstract and keywords.

All authors read and approved the final manuscript.

Funding

Not applicable

Competing interests

Not applicable

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Redfame Publishing.

The journal’s policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

Copyrights

References

Dawson, G. (2022). Options for a Peace Settlement for Ukraine: Option Paper III – Weapons of Mass Destruction. Opinio Juris. Available at: https://opiniojuris.org/2022/05/06/options-for-a-peace-settlement-for-ukraine-option-paper-iii-weapons-of-mass-destruction/

Denning, D. E. (1999). Information Warfare and Security. – Reading, Mass., etc., 323 p.

Forno, R., & Baklarz, R. (1999). *The Art of Information Warfare.* Insight into the Knowledge of Warrior Philosophy.

Kahneman, D. (2017). *Thinking, Fast and Slow.* Kyiv, Nash format, 480 p.

Lee, K. F. (2020). *AI Super-powers.* Kyiv, BookChef, 240 p.

Lederer, E. M. (2022). UN votes to press countries to stop terrorists getting nukes. AP. Available at: https://apnews.com/article/technology-business-united-nations-terrorism-weapons-of-mass-destruction-d20d85c4d9bce0bd0d9912fc73144ce2

Levchuk, N. P. (2018). Rozvytok ekonomichnoi kompetentnosti ofitseriv-mahistrantiv derzhavnoi prykordonnoi sluzhby Ukrainy [Development of economic competence of officers-masters of the State Border Guard Service of

Ukraine]: A dissertation of the Candidate of Pedagogical Sciences, Khmelnytskyi, 309 p.

Libicki, M. C. (1995). What Is Information Warfare?

Lysenko, S. (2019). Informatsiina bezpeka: geneza pryntsypiv i pidkhodiv na prykladi doslidzhen klasykiv viiskovoi dumky [Information Security: Genesis of Principles and Approaches on the Example of Studies by Classics of Military Science]. *International Journal "Supremacy of law,"* 2, 184-192.

Mescon, M. H., Albert, M., & Khedouri, F. (1988). Edition, 3, illustrated. Publisher, Harper & Row。

Reynolds, C. (2020). Global Health Security and Weapons of Mass Destruction Chapter. *Global Health Security,* 187-207. Available at: https://doi.org/10.1007/978-3-030-23491-1_9

United States Department of Defense (1998). The Joint Doctrine for Information Operations.

Varenko, V. M. (2014). *Informatsiino-analitychna diialnist: Navchalnyi posibnyk [Information and analytical activities: A study guide].* Kyiv, Universytet "Ukraina," 417 p.

Volohin, Y. (2011). Stanovlennia ta rozvytok menedzhmentu yak nauky v suchasnykh umovakh rynkovoi ekonomiky [Formation and development of management as a science in the modern market economy]. *Youth & market, 8*(79), 129-133.