Conflict Analysis in the "Subject-to-Subject" Security System

Svitlana Shevchenko[1], Yuliia Zhdanova[1], Halina Shevchenko[2], Olena Nehodenko[3], and Svitlana Spasiteleva[1]

[1]*Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[2]*The National University of Ostroh Academy, 2 Seminarska str., Ostroh, 35800, Ukraine*
[3]*State University of Telecommunications, 7 Solomyanska str., Kyiv, 03110, Ukraine*

Abstract

The concept of conflict theory is widely used in various sectors of society. This study examines the problem of using the main provisions of the theory of conflicts in the field of information security. With the development of information technologies, the risk of information conflicts is increasing, which can create threats to the integrity, availability, and confidentiality of information, which determines the relevance and importance of this research. The presented work is a continuation of developments describing the applied aspects of the theory of conflict theory in information security systems through the interaction of data streams in the "subject—subject" perspective. It is proposed to analyze the problem at four levels: the level of the individual (criminal—user); business level (internal and/or external violator—company manager); state level (violators/hackers—state institutions, state officials); the level of international relations (states, a group of subjects/hackers—institutions and/or political leaders of another state). Each level is defined as a complex conflict system that has a corresponding structure and stages. It was determined that the main characteristics of an information conflict in cyberspace are: unlimited territory, globality, the problem of attribution, and the superiority of attack over defense. It is substantiated that information security systems have all the features of complex conflict systems, which implies the application of the mathematical theory of conflict, namely, the Lotka-Volterra "predator—predator" model and the conflict triad model. The innovative function of information conflict is determined. The concept of conflict theory is widely used in various sectors of society. This study examines the problem of using the main provisions of the theory of conflicts in the field of information security. With the development of information technologies, the risk of information conflicts is increasing, which can create threats to the integrity, availability, and confidentiality of information, which determines the relevance and importance of this research.

Keywords

Conflict, information conflict, information security systems, cyber system, cyber conflict, conflict structure, conflict stages, mathematical model of conflict.

1. Introduction

Our society, in the center of which is a person and his activities, is a complex dynamic system, which is characterized by many connections, interactions, and relations in different spheres and at different levels. Existence in such a system is impossible without disagreements, confrontations, contradictions, and conflicts.

More and more scientists are turning to theoretical and practical developments in conflict theory. This is connected not only with the problem of studying man as a conflicted creature, but also with the growing tension in various spheres of social interaction of the participants of the organization, the state, and the world.

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); halyna.shevchenko@oa.edu.ua (H. Shevchenko); negodenkoav@i.ua (O. Nehodenko); s.spasitielieva@kubg.edu.ua (S. Spasiteleva)
ORCID: 0000-0002-9736-8623 (S. Shevchenko); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0002-8717-4358 (H. Shevchenko); 0000-0001-6645-1566 (O. Nehodenko); 0000-0003-4993-6355 (S. Spasiteleva)

There is no unequivocal opinion about the concept of "conflict". In modern literature, there are more than a dozen different definitions of conflict. All of them have the right to exist because each emphasizes one or more characteristics of this multifaceted phenomenon.

For the term "conflict" we come across several synonyms: clash of opposing interests, and views; a sharp dispute; extreme aggravation of contradictions, which leads to complications or acute struggle [1]. However, contradiction and conflict should not be equated. Contradiction (opposite as its component) is a defining feature of any phenomenon or event. Contradictions turn into conflict if their level increases to a critical limit and at the same time a subject is formed, which will deliberately exacerbate them in its interests [2].

At the same time, the authors of the study [3] emphasize that outside the subjects and independently of them there are contradictions, but not conflicts. The concept of conflict is not a fixation, but a qualification of the state of relations in a certain situation, which defines conflict as an assessment of the nature of interaction. Such a definition makes it possible to preserve the name conflict for situations of the opposition of the parties to each other, which are traditionally called conflict, and at the same time to extend this concept to situations of incompatibility of certain elements in the composition of the whole [3, p. 41]. This interpretation will allow us to describe conflicts of various natures, for example, a conflict of immunities, a conflict between software and a security system, and others.

The transition of society to the information age gave rise to innovative conflicts—informational. Modern informational conflicts have significantly transformed on both the micro and macro levels: starting from communication in social networks and ending with cyberespionage, cyberattacks, cyberwars, and involvement of non-state actors in relations in the international arena. With the development of information technologies, the risk of new conflicts that may threaten the integrity, availability, and confidentiality of information increases [4–6].

The beginning of the discussion of these aspects of the analysis of information conflicts in security systems was presented by us in the study [7]. The analysis of the literature made it possible to determine the following approaches to the definition of conflicts in security systems:

1. Information conflicts as a part of conflicts in various spheres and industries, since information is a strategic resource, the value of which acquires especially in the process of creation, therefore it needs to be protected.
2. Information conflicts as conflicts in information systems between implemented programs or in telecommunication systems between radio-electronic means and security systems.
3. Cyber conflicts are part of international information conflicts and are most often associated with information wars, cyber espionage, and cyber operations.

It is substantiated that it is advisable to consider the coverage of this problem through the interaction of the planes of the theory of conflict theory and the theory of information and cybernetic security in three perspectives:

- "subject—subject" or "person—person", possibly "group of people—group of people", "person—group of people".
- "subject—object" or "man—machine".
- "object—object" or "machine—machine".

Within the scope of this article, it is intended to consider the applied aspects of the theory of conflict theory in information security systems through the interaction of data flows from the perspective of "subject—subject". In particular, analyze the issues at four levels:

1. Personality level (criminal—user)
2. Business level (internal and/or external offender—company manager)
3. State level (violators/hackers—state institutions, state officials)
4. The level of international relations (states, a group of subjects/hackers—institutions and/or political leaders of another state).

2. Mathematical Models of "Subject-Subject" Information Conflict

Conflict is a very complex system with adaptive structures and evolutionary mechanisms. It is a system made up of interconnected parts that, as a whole, exhibit properties that cannot be easily understood just by disassembling and analyzing the properties of the individual components. A deep understanding of conflicts requires, on the one hand, a systems thinking approach, and on the other, a combination of many social and scientific disciplines [8]. The analysis of analytical reports and scientific literature confirms the fact that together with the development of hardware and software means of information protection, the

number of malicious software that allows one subject (group) to gain unauthorized access to the information resources of another subject (institution) is growing rapidly. As a result of the implementation of such a threat, information protection is violated, and its destruction and/or theft, loss of integrity, availability, and confidentiality are possible. The interaction of these parties is conflictual. The modern theory of conflict systems allows for building and researching models of real processes using the mathematical theory of conflict. In this case, we will use the well-known "prey—predator" model, which is based on a system of two first-order ordinary differential equations. The equation was proposed independently by scientists Alfred James Lotka and Vito Volterra in 1925 and 1926 [9]. The classical Lotka-Volterra "predator—prey" mathematical model is used in many fields of science and technology due to its successful combination of relatively low complexity and strong nonlinearity. The model has a high degree of universality when describing the behavior of complex systems operating in the mode of self-oscillations [10, 11]. It should be noted the existence of spot developments for the implementation of this model in the security system [12–13].

In general, the model looks as follows:

$$\begin{cases} \frac{dx}{dt} = (p_1 - p_2 y)x, \\ \frac{dy}{dt} = (-p_3 + p_4 y)x, \end{cases}$$

where x is the amount of information available to the user and interest to the attacker,

y is the amount of information obtained by hacking,

t is the duration of the process,

p_1 is the probability that the volume of information of interest to the attacker is well Protected,

p_2 is the probability that an attacker will obtain the information,

p_3 is the probability that an attacker will not be able to obtain the information,

p_4 is the probability that an attacker has sufficient potential to breach the user's protection.

However, the presented model is of a generalized nature, since this information security system is not isolated from others and is in a complex relationship with them. To bring the model closer to real data, various modifications are used. Thus, work [14] presents an approach where *x* and *y* are vector values:

$$x = (x_1, x_2, \ldots, x_n),$$
$$y = (y_1, y_2, \ldots, y_n), n > 1.$$

Therefore, the values *x* and *y* can be represented not only by the volume of information but also by other characteristics of the security system.

The model can also be improved by introducing the delay time of the argument *t*, the value of which is determined by the method of experimental selection.

The next conflict system that can be modeled in security systems is the conflict triad model [15]. The dynamic model of the conflict triad is a model that is defined by the interaction between three natural substances: the population of a biological species (life), the environment (resource of existence), and negative factors for existence (virus).

Let's apply the described model to the security system. Let us denote by *P, R, Q* substances that exist in a common space and interact with each other in a certain way. Then, in the conflict system of the "subject—subject" security system, we get the following subsystems at different levels (see Table 1):

Table 1

Substances in the conflict triad of information security

Subject—subject level	**Space Ω**	Substance P	Substance R	**Substance Q**
Business level	Information system	Company management	Technical, legal, organizational tools	Anthropogenic sources of threats
State level	Information system of state institutions	State figures, state institutions	Technical, legal, organizational tools	Anthropogenic sources of threats
International relations level	Virtual space	Politicians, state institutions	All existing	Any subject (group of subjects) of another state

Interdependence between substances P, R, Q [15] is depicted by the diagram in Figure 1, where an arrow with a certain sign corresponds to the direction of positive or negative dependence of one substance on another.

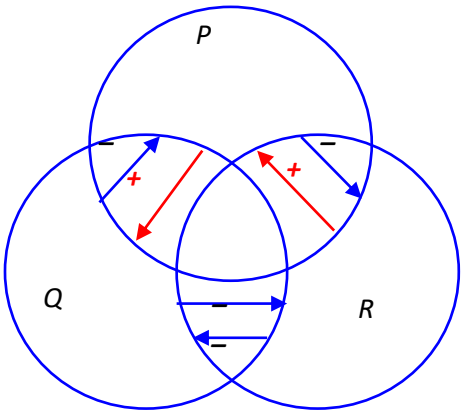

Figure 1: Interdependence between substances

Two-way pairwise interdependence "plus-minus" is an analog of the "prey-predator" model. Interdependence "minus-minus" models the conflict struggle of irreconcilable alternative substances (anthropogenic source of threats—security policy).

The conflict triad is a complex dynamic system since each of the three substances has an internal structure $P = (P_1, P_2, \ldots, P_n)$, $R = (R_1, R_2, \ldots, R_n)$, $Q = (Q_1, Q_2, \ldots, Q_n)$.

Also, all the formulas for the interaction of each substance with a pair of others are different from each other: P with a pair $\{Q, R\}$, Q with a pair $\{P, R\}$, R with a pair $\{P, Q\}$.

The formulas defining the dynamic system of the conflict triad are given in [15].

The nature of things in the world is such that any conflict process is endless. In each act, the conflict transforms the content of the contradiction into a new, possibly hidden, form. From the point of view of mathematics, this means a change in the spectral structure of the conflicting distributions.

It should be noted that managing information conflict in information security systems is a major problem today. This is explained by the fact that in the virtual space, criminals have unprecedented opportunities to mask their actions, as a result—their impunity. The geography and time of such conflicts are unlimited.

2.1. Subject—Subject Informational Conflict: The Level of the Individual

The birth of the Internet in 1989 caused a rapid growth of computer equipment, in particular, personal. The use of the World Wide Web led to the creation of new interactions and relationships between people—virtual, the era of digital society began. Persons, relationships, and social institutions are formed by both software and hardware [16]. Along with this, where there are new social facts, new habits, new ways to meet, buy, pay, store, protect, and transfer assets, new digital identities, and new systems for gathering information, it is only natural that new crimes appear, related to information technologies [17].

According to an analytical report [18] in 2022, the frequency of email attacks has increased to reach 86% of all file-based in-the-wild attacks, Zip files are the most common format for hiding malware, Joker mobile malware, which accesses contact lists by hiding in at least 8 Google Store apps, has been downloaded more than 3 million times, allowing attackers to obtain relevant information. accesses users' contact lists and sends information to attackers. Every day, the AV-TEST Institute registers more than 450,000 new malicious programs (malware) and potentially unwanted programs (PUAs), in the last year there have been about 70 million malicious programs for Windows, which is 5000 times more than for macOS (where only about 12,000 samples) and 60 times more than the corresponding figures for Linux (2 million samples) [19]. Thus, in the information sphere, a conflict situation is defined, as one which was intentionally created by one of the parties (criminal) to achieve their goals or orders.

An information conflict in "subject-subject" security systems at the "criminal-user" level is the result of the process of the criminal overcoming the resistance of the protection means of the user's information system, which enables the loss of confidentiality, availability, and integrity of information.

Such a conflict occurs in the user's information system, usually two participants (however, there may be a third person—the customer). The duration of such a conflict is determined by the strength of the defenses and capabilities of the attacker. Table 2 presents the stages of this conflict.

Table 2
Stages of information conflict at the attacker-user level

Stages	Description
The emergence of a conflict situation	Creating malicious software on purpose (using someone else's) to achieve one's goals (revenge, financial gain, emotional satisfaction)
Latent stage	The attacker deliberately and actively searches for vulnerabilities in the user's information system
Active stage	Destruction, forgery, modification, blocking, theft of information
The stage of ending the conflict	The user provides redemption; acts through the legal field; loses information

Regulation of this conflict is possible at a latent stage, if the user has a high level of information protection, following the basic rules: password management; use of at least two-factor authentication; use of licensed antivirus programs; control over personal information transmitted over the Internet; avoiding the use of public Wi-Fi networks.

2.2. Subject-Subject Information Conflict: Business Level

The direction of our research will further be directed to the analysis of possible conflict situations between the head of the company and a subordinate in the context of the existence of an information conflict, which causes a violation of the information protection system.

Information conflict in security systems "subject-subject" at the level of business "internal employee—manager" is defined as the result of an employee's insider activity, which led to a violation of the security policy in the company's information system.

Insider activity—directed actions of motivated subjects who have legitimate access to information assets and skills to obtain valuable information, know the vulnerabilities of information systems and business processes, to cause material losses and/or reputational losses of the organization [20].

As the 2022 Cost of Insider Threats: Global Report reveals, insider threat incidents have risen 44% over the past two years, with costs per incident up more than a third to $15.38 million; the cost of credential theft to organizations increased 65% from $2.79 million in 2020 to $4.6 million at present; the time to contain an insider threat incident increased from 77 days to 85 days, leading organizations to spend the most on containment [21].

The authors [22] propose to consider the portrait of an insider from the point of view of psychological characteristics and activities: low-class and high-class insiders. The activities of low-class insiders have been exposed and punished. The profile of such a violator includes the following features: these people do not have high-quality technical education; worked in various positions; are motivated by personal gain and are influenced by emotions; are not aware of the potential negative consequences of their actions; their behavior arouses suspicion on the part of colleagues.

High-class insiders see their malicious mission as their career decision. The portrait of such a violator is high-quality professional abilities, diligence, reliability, leadership, and dedication. Such insiders are very dangerous. The structure and stages of the informational conflict are different for each of these types. The description is presented in Table 3 and Table 4.

Table 3
Stages of information conflict at the level of an internal employee (low-class insider)—the head of the company

Stages	Description
The emergence of a conflict situation	An unfair decision by the manager, resentment, and lack of respect, as a result of the desire for revenge
Latent stage	Unauthorized/privileged access to IS
Active stage	The violator was found and detained
The stage of ending the conflict	Firing from a job; punishment by law

Table 4

Stages of information conflict at the level of an internal employee (high-class insider)—the head of the company

Stages	Description
Emergence of a conflict situation	The temptation to get hidden profit; sharp sensations; boasting
Latent stage	Unauthorized/privileged access to IS
Active stage	Loss of confidentiality, integrity, and availability of information (material and reputational damage to the organization)
The stage of ending the conflict	The possibility of purchasing information; actions through the legal field; involvement of third parties in negotiations

It should be noted that an insider can be an external actor, for example, a former employee, whose motive may be revenge for, in his opinion, unfair dismissal from work.

An information conflict is also possible if the insider activity was unintentional, but the loss of the company's information data occurred. Moreover, the manager learned about this event after this incident. The structure of such a conflict does not contain a latent stage, since the informational conflict has occurred. The stage of the end of the conflict is the punishment of the employee (verbal or written penalty, material penalty, dismissal from work).

The conflict struggle is most often caused by a primitive perception of reality, as if one of the parties is capable of winning, and the other—is defeated. There is some redistribution of the spectral characteristics of the opposing sides in the conflict. The victorious gain in one aspect means inevitable loss, defeat, and loss in another. The essence of the contradiction is transformed and appears again in the future at another level of gradation of the complex structure of interests [14]. This process is demonstrated by an example of a dismissed employee. Therefore, it is important to understand the problem of conflict prevention. The authors of the study [23] proposed three approaches to detecting insider threats:

- Sociological, psychological, and organizational.
- Socio-technical.
- Technical.

In our opinion, this will make it possible to stop the informational conflict before the active stage.

The current stage is characterized by the introduction of mixed systems and methods of detecting insider threats [20]. Scientists are trying to combine two approaches in this direction:

- Psychosocial approach, the basis of which is the analysis of the mental and emotional states of employees, and it is possible to predict the behavior of an insider.
- Continuous monitoring in the network.

A large business has the material resources to implement software products to detect insider threats, for example, the CHAMPION system (Columnar Hierarchical Autoassociative Memory Processing in Ontological Networks), small and medium-sized businesses practically do not deal with this issue. In this regard, we offer the following recommendations regarding the possible forecasting of conflicts in the company's information security. This process is based on two components:

1. Software for determining the user's computer activity, the main of which is:
   - Role-based access policy.
   - Restrictions on data transmission and copying.
   - Using MPI (Microsoft Purview Insider or DLP (Digital Light Processing).
2. Psychological methods for personality profiling can be used:
   - "Big Five" test
   - Test "Ability to self-govern"
   - Individual psychological test.

As a result of processing the obtained results, if everything is satisfactory, then there is constant monitoring of the information system on the one hand and training with employees on the other. Otherwise, the security policy should be further reviewed and additional methods of detecting and countering insiders should be added. Fig. 2 presents the algorithm of this process.

Therefore, increasing investments in the company's information security will reduce the likelihood of information conflicts. However, companies stop at a level of rational investment that is equal to or less than the expected losses from a hack. This leads to a gap in investments (Fig. 3) in the cyber defense of companies [24]. Special measures of the government would allow the filling of this delta. For example, to subsidize equipment, software, and training, and increase the number of cyber specialists who know how to work with systems, programs, and equipment and ensure the functioning of all these components.

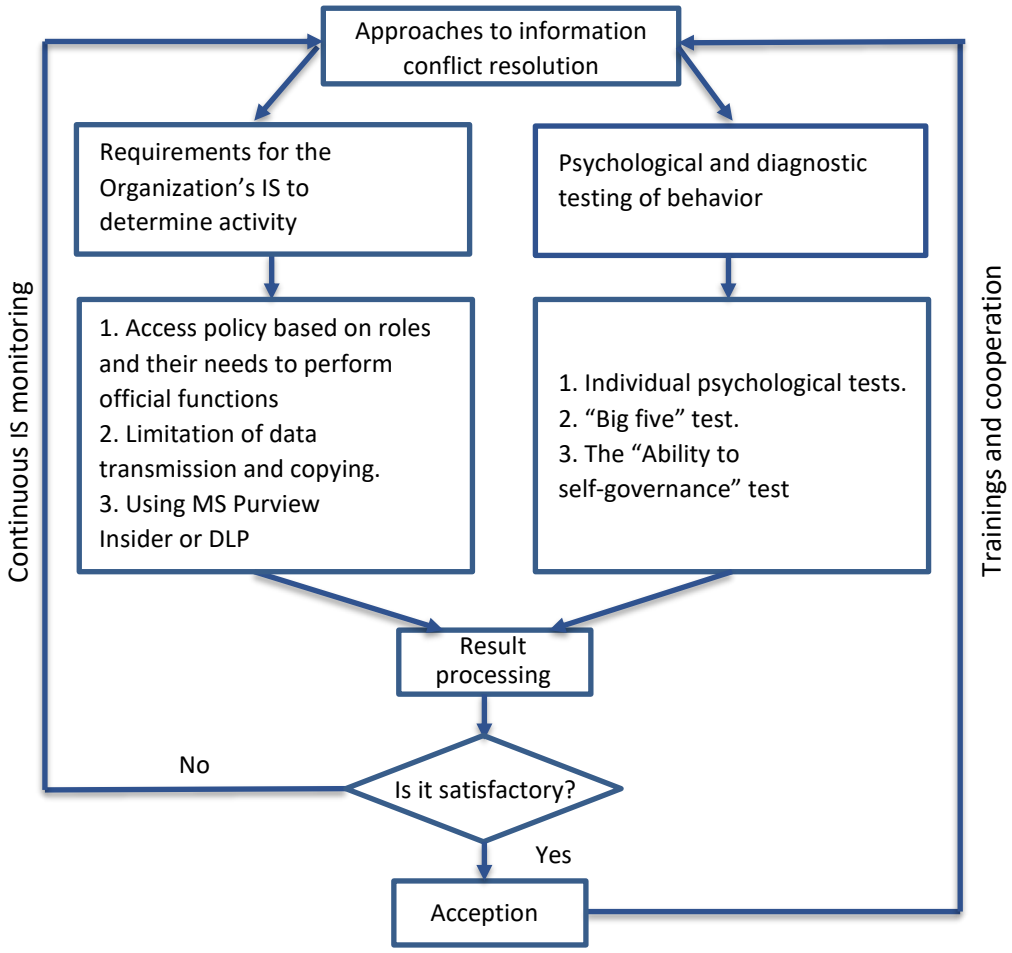

Figure 2: Approaches to the resolution of informational conflicts at the level of an insider-head of the company

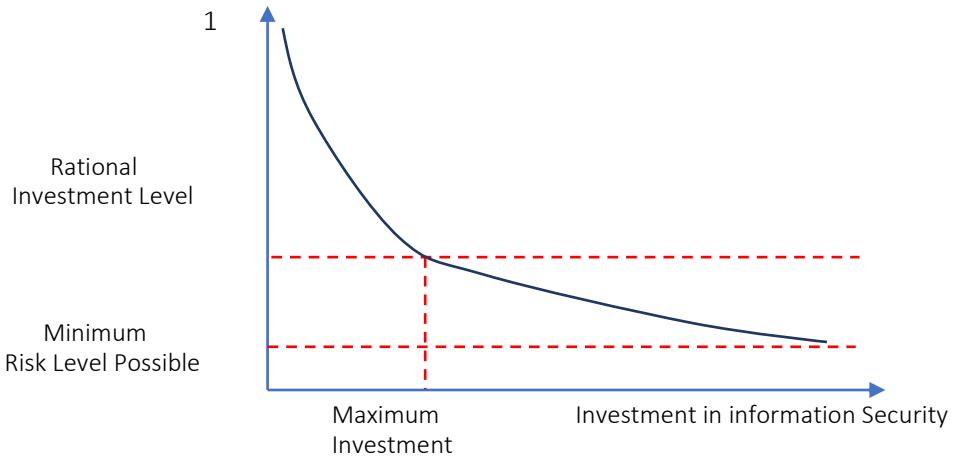

Figure 3: Rational Investment Level

2.3. Information Conflict "Subject-to-Subject": State Level

Information conflict in security systems "subject-subject" at the level of the state "hackers—state institutions, state officials" is the process of resisting hacker attacks on the information systems of critical infrastructure objects of the state, as a result of which there is a possible disruption of the functioning of data about objects

It should be noted that most of the incidents are disclosed by the relevant state structures. Table 5 presents the structure of this conflict.

Table 5

Stages of information conflict at the level of hackers—state institutions, statesmen

Stages	Description
The emergence of a conflict situation	Preparation for a cyber attack on critical infrastructure facilities. Motivation: - material component - sharp sensations - leadership.
Latent stage	Unauthorized interference (use of malicious software); bribery of insiders; blackmail of politicians.
Active stage	Violation of integrity (manipulation of data or introduction of data to influence the political and economic activities of the government). Violation of availability (refusal to service critical infrastructure objects). Violation of confidentiality (extraction of personal data of members of the government, political figures; espionage).
The stage of ending the conflict	If the active stage has taken place, then a violation of the regular mode of operation of the critical infrastructure object. In the opposite case: the use of the legal field, meeting the requirements of the opposite party

Combating online threats requires the state to go beyond the whole government paradigm and adopt a public-private partnership approach, as the tools needed to respond are often in the hands of others [24, 25]. This cooperation should include specialized information and cyber security firms, IT companies, hardware companies, banks and financial sector entities, politicians and members of government, and private entities. The effectiveness of work is monitored through reporting and transparency of their activities, which will reduce the likelihood of information conflicts.

2.4. Information Conflict "Subject—Subject": International Relations Level

The relevance of the issue of information conflict at the level of international relations is confirmed by a large number of studies in the field of politics, law, military affairs, and cyber security [26–35].

Analysis of the literature made it possible to identify the following features and characteristics of information conflict in security systems:

- the geography of the conflict (in traditional battles, the defender has an advantage due to his knowledge of the terrain and the direction of the attack, in the cyber world these advantages disappear, since states often do not know where the attack will come from or even if an attack is happening [30]).
- the globality of the conflict (in any conflict, cyberattacks quickly become global as secretly acquired or hacked computers and servers around the world are brought into action [30]).
- responsibility for the conflict (in the digital sphere, identifying perpetrators is more difficult: most states deny any involvement in actions that can be considered military in cyberspace; it is easy to hide behind proxies, raise false flags and act on behalf of another person [27, 31]).
- an imbalance between offense and defense (a single weak point may be enough for an attacker to enter systems and networks to achieve their goals, while defenders need to guard many systems, often without adequate resources [27, 28, 31]).

An information conflict in security systems "subject-subject" at the international level "states, a group of subjects/hackers—institutions and/or

political leaders of another state" is called the process of confrontation between subjects of international relations in cyberspace, where offensive means and techniques of subjects of one state are aimed at information systems of critical infrastructure objects of another state, as a result of which it is possible to disrupt the functioning of these objects.

Table 6

Stages of information conflict at the level of the state, groups of subjects—institutions, political figures of another state

Stages	Description
The emergence of a conflict situation	Preparation of a cyber attack on critical infrastructure facilities of another state. Motivation: - disruption of functioning and destruction of critical infrastructure: power grids, production and distribution of oil and gas; logistics networks; telecommunications; financial sector; services. - a claim to a certain status. Involvement of public and private individuals/groups in the formation of a cyberattack. Bribery and blackmail of members of the government and political figures.
Latent stage	Unauthorized interference (use of malicious software); bribery of insiders; blackmail of politicians.
Active stage	Violation of integrity (manipulation of data or introduction of data to influence the political and economic activities of the government). Violation of availability (refusal to service critical infrastructure objects). Violation of confidentiality (removal of personal data of members of the government, political figures. Espionage)
The stage of ending the conflict	If the active stage has taken place, then a violation of the regular mode of operation of the critical infrastructure object. In the opposite case: the use of the legal field at the international level, and involvement of a third party (state or group of states) in the negotiations.

The increase in the number of information conflicts at the international level is especially intensified during the period of armed conflicts between states. Thus, cyberattacks on the Ukrainian government and the military sector increased by 196% in the first three days of the Russian Federation's war against Ukraine [18].

3. Conclusions

Summarizing the above, we have the following results:

1. The study of information conflicts from the point of view of information and cyber security is relevant and important since the relationships between participants in the virtual space are completely different.
2. When analyzing information conflicts in cyberspace, the following key issues should be considered:
   - the problem of attribution (anonymity of the created cyber attack, it is difficult to distinguish different types of actors, including states, non-state groups, and individual hackers; the reward is a high level of information protection).
   - the advantage of offense over defense (cyberspace encourages offensive strategies as opposed to defensive ones; attackers act without warning, looking for vulnerabilities, while cyber defense monitoring must be real-time and constant).
   - unlimited territory.
   - globality.
3. Effective prevention of cyber conflicts and their resolution requires public-private cooperation (involvement of security experts, IT technologies, members of the government, and scientists).
4. The creation of mathematical models in the process of analyzing information conflicts in cyber security systems will become an adequate tool for knowledge, description, and modeling of real phenomena in this field.
5. The theory of information conflicts in information and cyber security systems has an innovative character, strengthening the creation and development of new technologies for ensuring the integrity, availability, and confidentiality of information.

4. References

[1] V. V. Yaremenko, et. al., New Glossary of Ukrainian Language in Three Volumes, Aconite, 1 (2007).

[2] M. Piren, Conflictology: Textbook. MAUP, Kyiv, (2007).

[3] A. Girnyk, V. Rezanenko, The Concept of "Conflict" in Western Culture and in the Culture of Traditional Societies of the Far East. Scientific Notes of NaUKMA, 136 (2012) 37–42.

[4] M. Vladymyrenko, et al., Analysis of Implementation Results of the Distributed Access Control System. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (2019). doi: 10.1109/picst47496.2019.9061376

[5] Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25. doi: 10.1109/UkrMiCo52950.2021.9716700

[6] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

[7] S. Shevchenko, et. al., Study of Applied Aspects Ofconflict Theory in Security Systems, Cybersecur. Educ. Sci. Technol. 2(18) (2022) 150-162. doi:10.28925/2663-4023.2022.18.150162

[8] G. Gallo, Conflict Theory, Complexity and Systems Approach, Systs. Res. Behav. Sci. 30(2) (2013) 156–175. doi:10.1002/sres.2132

[9] A. Lotka, Elements of Physical Biology, Nature 116, 461 (1925). doi:10.1038/116461b0 1925

[10] D. Trubetskov, Phenomenon of Lotka-Volterra Mathematical Model and Similar Models, Izvestiya VUZ, Appl. Nonlinear Dyn. 19(2) (2011), 69–88. doi:10.18500/0869-6632-2011-19-2-69-88

[11] A. Bratus', A. Novozhilov, A. Platonov, Dynamic Systems and Models of Biology, Draft, (2019).

[12] I. Kononovich, D. Mayevskiy, R. Podobniy, Models of System of the Cibersecurity Providing with Delay of Reaction on Incidents, Inf. Math. Methods Simul. 5(4), (2015) 339–346.

[13] S. Gorman, et. al., A Predator Prey Approach to the Network Structure of Cyberspace, (2004).

[14] S. Yevseiev, et. al., Development of a Method for Assessing the Security of Cyber-Physical Systems Based on the Lotka–Volterra Model, Eastern-European Journal of Enterprise Technologies, 5(9) (113) (2021). doi:10.15587/1729-4061.2021.241638

[15] V. Koshmanenko, Spectral Theory of Dynamic Conflict Systems, Naukova Dumka, Kyiv, (2016).

[16] V. Koshmanenko, I. Samoilenko, Model of a Dynamic System of a Conflict Triad, Nonlinear Oscillations, 14(1) (2011) 56–76. doi:10.1007/s11072-011-0141-5

[17] D. Lupton, Digital Sociology (2015) Taylor and Francis. doi: 10.4324/9781315776880-1

[18] A. Nicola, Towards Digital Organized Crime and Digital Sociology of Organized Crime. Trends. Organ. Crim. (2022). doi:10.1007/s12117-022-09457-y.

[19] Check Point Software's 2023 Cyber Security Report, Cyber Security Report.

[20] Malware, AV-TEST URL.

[21] S. Shevchenko, et. al., Insiders and Insider Information: Essence, Threats, Activities and Legal Responsibility, Cybersecur. Educ. Sci. Technol. 3(15) (2022) 175–185. doi:10.28925/2663-4023.2022.15.175185

[22] 2022 Ponemon Cost of Insider Threats Global Report, Proofpoint US.

[23] E. Cole, S. Ring. Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft, Elsevier/Syngress, Amsterdam, (2005).

[24] J. Hunker, C. Probst. Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques, J. of Wirel. Mob. Netws. Ubiquitous Comp. Dependable Appls. 2(1) (2011) 4–27. doi:10.22667/JOWUA.2011.03.31.004

[25] S. Castro, Towards the Development of a Rationalist Cyber Conflict Theory, Cyber Def. Rev. 6(1) (2021) 35–62.

[26] B. Buckland, F. Schreier, T. Winkler. Democratic Governance Challenges of Cyber Security. DCAF Horizon 2015 Working Paper, 1 (2015).

[27] D. Sherengovskij, The Concept and Essence of International Conflict in the Science of International Relations, Actual Problems of Politics, Phoenix, Odesa, 43 (2011) 98–108.
[28] M. Wohlfeld, J. Jasper, Cyberattacks and Cyber Conflict: Where Is Conflict Resolution? University of Malta. Centre for the Study and Practice of Conflict Resolution, (2018) 5–17.
[29] J. Healey, The Five Futures of Cyber Conflict and Cooperation. Georgetown J. Int. Affs. (2011) 110–117.
[30] M. Intriligator, Research on Conflict Theory: Analytic Approaches and Areas of Application, J. Confl. Resolut. 26(2) (1982) 307–327. doi:10.1177/002200278202600200 6
[31] B. Valeriano, R. Maness, What Do We Know About Cyber Conflict? Scope, Impact, and Restraint in Cyberspace.
[32] R. Inversini, Cyber Peace: And How It Can Be Achieved, The Ethics of Cybersecurity, Int. Libr. of Eths. Law Technol. 21 (2020) 259–276. doi:10.1007/978-3-030-29053-5_13
[33] R. Kazansky, The Conflict Theory as a Pillar of Security Science, Secur. Sci. J. 1(2) (2020). doi:10.37458/ssj.1.2.3
[34] H. Lin, Cyber Conflict and International Humanitarian Law, Int. Rev. Red Cross, 94(886) (2012) 515–531. doi:10.1017/S1816383112000811
[35] M. Christen, et. al., A Review of Value-Conflicts in Cybersecurity, ORBIT J. 1(1) (2017) 1–19. doi:10.29297/ORBIT.V1I1.28
[36] I. Alakbarova, Problems Created by Cyberconflicts and Methods to Solve Them, Probls. Inf. Soc. 2 (2015) 29–33. doi:10.25045/jpis.v06.i2.04