JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–7
https://doi.org/10.1093/cybsec/tyad017
Research paper

Research paper

The concept of modern political confrontation in cyber space

Liudmyla Kormych* **and Yuliia Zavhorodnia**

Department of Political Theories, National University “Odesa Academy of Law”, 23 Fontanska Str., Odesa 65009, Ukraine

*Correspondence address. 65009, 23 Fontanska Str., Odesa, Ukraine. Tel: +38048 719 8881; E-mail: l.kormych@gmail.com

Received 12 April 2023; revised 3 July 2023; accepted 24 July 2023

Abstract

The purpose of the study is to determine the main forms of behavior of the participants of the political process in the information space of Ukraine and progressive informative countries of the world in order to achieve political goals and decisions that have a constructive or destructive function in the political system, considering social, cultural, legal, and ideological factors that affect interaction of participants during the confrontation of political processes in cyberspace. The subject of the study is the concept of modern political confrontation in cyberspace. Through the lens of a combination of international and national approaches to the development of effective ways of improvement for the further segmental possibility of use in the field of cybersecurity and cyber protection, the theoretical and practical underpinnings of political conflict in Ukraine were established. The protection of an individual’s and a citizen’s rights and freedoms was used in an approach that calls for the implementation of political conflict within the context of political interaction. The correlation of global cybersecurity in the context of the dichotomy “democratic political regime—non-democratic political regime” is revealed. It is proposed to borrow the experience of individual states regarding coordination of the increase of scientific potential and human resources in the field of the IT industry in order to achieve the highest level in the protection of the state’s critical infrastructure; improvement of the political system organization in the direction of the formation of an institutional subsystem at the modern informational level.

Key words: confrontation, cyber conflicts, information space, international information space, digitalization

Introduction

Modern forms of political interaction are being modified into a new political plane, namely cyberspace. The specification of this “territory” of interaction is that it does not contain any spatial boundaries, and the participants of the political process in their form of activity can go beyond the boundaries of regional or state influence on society.

Since the democratic form of political interaction involves different points of view, as well as different directions of state development, the specifics of the implementation of the declared principles of activity, the formation of legal protection mechanisms taking into account the emergence of new forms of crime, that is why the question of sharpening rivalry among the participants of the political process in cyberspace is becoming topical. The latest political system demonstrates the need to reformat political institutions, which should be the basis for the stable existence and development of society.

The new wave of state-political development in the direction of digitalization has already become relevant for many developed countries of the world. However, for Ukrainian society, the process of normative and institutional form of transformation begins at the current stage of the state’s development in the conditions of the coronavirus pandemic, and the most difficult in the conditions of the Russian–Ukrainian war, which clearly established a single direction of public interests and the consolidation of Ukrainian society. In the conditions of the formation of state cyber security institutes and the formation of legal norms, regarding the stabilization of political processes, a system of views is being formed on the positive and negative styles of behavior of the participants of the political process in cyberspace, the possible permissible limits of their activity and the creation of a public information base that does not harm the interests of the country.

The main achievements of Ukrainian society in the direction of the formation of a regulatory framework are the implementation of the decision of the National Security and Defense Council of Ukraine from 29th December 2016 [4], and later the adoption of the Law of Ukraine "On the Main Principles of Ensuring Cyber Security of Ukraine" [17], which became the basis for the perception of the cybernetic plane as a full-fledged system of interaction of participants in the political process. In addition, this law gives a normative assessment to the concepts of "cyber crime," "cyber attack," "critical information infrastructure," etc. That is, specific forms of the influence of danger in the cybernetic plane have been determined at the regulatory level.

Valuable forms of building a political cyber system are the authorization of state institutions, which will be the regulatory and security basis for the development of a digitalized society. In the sphere of the executive power system, such a constructive basis is the Ministry of Information Policy of Ukraine, the Ministry of Culture of Ukraine, the Ministry of Foreign Affairs of Ukraine, the National Council of Ukraine for Television and Radio Broadcasting, the State Agency of Ukraine for Film Affairs, and the State Committee for Television and Radio Broadcasting, which create the conditions for implementation political goals and tasks of political power in the country [2, 26].

In addition, coordination of the activities of executive authorities with the aim of implementing the Doctrine and guaranteeing national security in the information sphere should be carried out by the National Security and Defense Council of Ukraine, which demonstrates its important role in the system of political and legal institutions, but the range of powers limits the ability to quickly respond to information attacks, cyber conflicts, and crimes social scale that arise in the digitalized imperfect information space. Such an information platform, which has hybrid forms of perception of the political plane, shifting the blame and the absence of a rigid defensive position, which creates conditions for the use of a system of destabilization of the governing bodies and society as a whole. When researching the concept of information security in the political process, general and special methods of scientific knowledge were used: the method of system analysis, the dialectical method, the formal-logical method, and the comparative method, as well as a number of empirical methods.

In order to create a comprehensive idea of political confrontation in cyberspace, a generalization of scientific studies related to the issues of modern realities of the development of political conflicts was used. A significant component of research in the direction of political transformation of conflict activism into globalization policy [10, 23] and changes in perceptions about modern political conflicts in Ukraine [13, 15, 24, 32]. Attention is also paid to cooperation in the information security sector as an important component of influencing conflicts [36]. An approach is used that allows to demonstrate the interdependence of international policy and state policy in the fight against cyber threats from the confrontation of political processes in cyberspace.

Thus, the relevance of the question of the interaction of the participants of the political process in cyberspace in the conditions of confrontation, as a form of defending one's own position, is a very relevant and socially motivated field of research that has theoretical and practical value. In this work, attention is focused on the modern form of cyber–conflict interaction of the participants of the political process in Ukraine and the features of effective interaction in cyberspace by subjects of developed digitalized countries, in particular the USA and China.

Modern forms of conflict activity in political processes

Conflicts that a person faces during his existence are diverse. The region of development, the goal of the conflict, participants in the confrontation, methods of influencing the opponent, and many other features influence the development of conflict activity. However, the essence of the democratic political process is formed through the competitive period of electing candidates for the highest public positions in the corresponding period, during which the subject of politics either confirms the support of the population in the elections, or loses it. Therefore, political conflicts, as a form of serious opposition in political decisions, are an integral part of political activity.

The process of a political conflict can be a process of making a separate political decision, which is socially important and decisive for the further development of the country. Since a political conflict goes through three main stages, such as: pre-conflict stage, direct conflict, and conflict resolution, similarly, the process of making an important decision can proceed in three stages, firstly, the register of the draft law for discussion, secondly, voting in the readings for this law (during which the parties oppose, publicly express dissatisfaction, introduce amendments, vote by majority vote), thirdly, the adoption of a compromise decision, which will contain elements of compromise and consensus [34].

In addition, in a political conflict, it is customary to distinguish the fourth stage of the development of the conflict, as the post-conflict syndrome [1]. The peculiarity of this stage is the observation of the parties to the conflict, since the settlement of the conflict can be completed taking into account the interests of one of the parties more than the other, and therefore, the so-called personal resentment arises, which requires continued monitoring of the parties to the conflict. Also, after the end of the conflict, and not the settlement, new threats arise regarding the conflict activity of the parties to the conflict, because the parties remain dissatisfied, embitterment, which is not appeased by positive decisions, recognition of the truth in political views.

Post syndrome can begin to manifest itself during the adoption of new decisions and the emergence of interaction between political figures. Therefore, it is important to distinguish between procedural conflict and the process of making a political decision, because during the phenomenon of conflict, the parties not only resort to a dispute with arguments for their own position, but also oppose each other, resort to political means to discredit the opponent and his vision of choosing the vector of agreement on the issue.

S. Sitarsky rightly points out that "destabilization in the country does not occur because there are conflicts. They have always been and will remain in civil society. Tension arises as a result of untimely detection, control and regulation of the conflict process, that is, its management. By management, we mean regulation, resolution, suppression, even initiation of some conflicts in the interests of society or its individual subjects" [24].

After all, in modern political processes, the most important thing is the analysis of conflict response, the analysis of the parties' positions, the analysis of the parties' capabilities, and the possibility of applying radical methods of influence. During the study of all these aspects, it is possible to form a picture regarding the expediency of influencing such a conflict, control over its progress, or the lack of need for such measures at all, since the conflict does not contain any serious threats to the political system and the stability of social development.

It is important to understand that the development of conflicts can occur in any political processes and become public through social networks and media resources. However, its danger is that there is a minimal risk of negative impact on society. Thus, according to L. Kochubey, “the higher the level of social tension, the higher the involvement of the social subject in the campaign. To aggravate the situation, the technology of expanding the conflict zone, its globalization, is used, which is implemented by giving the conflict hypersignificance” [13].

In today’s world, social tension develops through social networks and rating periodicals that enjoy the authority of objectivity of information. Political leaders use their own information channels to highlight subjective views on political decisions or events.

Modern scientific views divide conflicts according to various signs, forms of behavior, etc. [24]. However, modern political processes, which often move into the cybernetic plane, influence each other there, during the struggle for separate political processes, therefore rethinking the relationship to conflict activity in politics.

The specifics of cyber conflicts as a transformed form of political confrontation

To create a generalized approach to political confrontation in cyberspace, the development of cybercrime in the global world from 2019 to mid-2022 in the economic equivalent of damage to society [3] was analyzed basing on the following criteria: (a) historical period, within which negative consequences of cybercrime; (b) an economic indicator of the damage caused in the world due to cybercrimes. So, the peculiarities of the development of cybercrime in the global world in: 2019—3.92 million dollars; 2020—3.86 million dollars; 2021—4.24 million dollars; 2022—1 trillion (economic forecast until the end of the year).

Digitized political rivalry is a transformed form of existing ideas about political conflict, which contains a number of differences and features. The main characteristic features of a cyber conflict, which branch it off from a political conflict, are spatial boundaries, the possibility of global development in the shortest possible time, and the absence of subject attachment to specific actions in cyberspace (as a rule, cyber attacks are carried out by competent persons at the appropriate disposal of the subjects of the conflict).

Modern state policy is focused on simplifying the bureaucratic system, saving time for any registration processes, and effective use of social guarantees. However, in addition to the positive aspects, there are a number of threats regarding cyber attacks for the disclosure of personal data, the possibility of their use and removal from databases. These are the threats facing the modern sector of information policy in order to protect and preserve personal information [6, 32]. Disclosure of personal data is one of the main dangers for political leaders that may be exposed in cyberspace, as this may include: data on family members of political subjects (wife, children, parents), which are often used in political confrontation; data on the availability of movable and immovable property of an active political figure and his family members; data on economic transactions that are of a dubious-illegal nature and amounts that exceed the official income of a person and other information that may harm the activity of a political figure.

Regarding the possibility of using or deleting any information about a political leader or political party, it is worth noting that in this case, the fact of hacking the information base/channel can play a bigger role than the information being used or deleted. After all, the possibility of creating chaos in the information system brings society into a dominant mood, and therefore is the negative factor that the opposition parties seek, that is, a change in consciousness regarding the perception of political power or a political leader.

In addition, the transformation of conflict activity into cyberspace provokes a rapid globalization of confrontation with the possibility of involving international actors who have an influence on international political processes. In the modern world, according to N. Rzhevska, “mass media are the most effective tools of informational and psychological influence on potential objects of conflict. In modern conditions, the information environment of the geopolitical conflict is formed and supported by the activities of mass media. Most often, the mass media is the main link in the information field of an international conflict. Recently, the rapid growth of temporary electronic mass media and the accelerated development of information technologies have brought the projects of creating complex information systems of the highest level closer to reality. Their task is to promote the transformation of conflicts through special manipulative methods” [23].

Of course, the role of information channels is quite relevant, because modern international conflicts are mainly realized in the media space, in the form of a struggle for awareness of national and international political processes. And therefore, an important role is played by normative processes, which are the mechanism for the implementation of public rhetoric of political leaders, the demonstration of their policy vector and the level of correspondence between words and actions. If the conflict enters the extreme phase of its development, military confrontation, then N. Rzhevska successfully notes the role of communication resources along with military equipment, which is important for society’s perception, therefore military actions are reinforced by information wars.

Foreign experience regarding the reaction to cyber conflicts in the political plane and its dependence on professional staffing in the field of the information system [9, 28], considerable attention is paid to the analysis of cyberwars as a new formation of negative influence and an essential destabilizing factor in society, it is the economy [8, 18, 22], features of the evolution of attacks that can exploit and damage individual systems and critical infrastructure [21]. Despite the length of scientific investigations in the field of political conflictology, it should be recognized that scientists have fragmentary investigated individual tools of cyber-activity in politics.

Taking into account the specifics of cyberspace, a cyber attack as a form of political cyber attack can potentially provoke an international conflict, including in a territorially defined space, since, on the one hand, in the conditions of global interaction of the information infrastructures of individual countries, it is extremely difficult to calculate the limits and consequences of such an attack, on the other hand—individual measures of the affected party may be disproportionate due to the difficulty of determining the source and the probability of an erroneous assessment of the situation. This can cause open military conflicts with the use of traditional types of weapons [20]. In addition, psychological technologies that successfully operate in the information plane should not be excluded. When in conditions of complete informational chaos, the process of forming a controlled negotiation state occurs. Information and psychological technologies can return the international conflict to a peaceful course [23].

Since, in the information society, the perception of the conflict and the negative consequences of its escalation are formed, therefore the positions of the parties are weakened and the intensity of the conflict is reduced, and the conditions are created for the stabilization of the political situation, in the form of a compromise or consensus decision. In this regard, we can note that the information struggle is carried out to influence the mass political consciousness, by means of distorting reality regarding the consequences of the confrontation of the parties. The result of a cyber conflict can be political decisions of global importance. For example, the issue of the export of Ukrainian grain from the seaports of Ukraine was interpreted as a threat of famine in African countries, with negative consequences for the whole world [29]. Therefore, in the form of a negotiation process, a compromise decision was made to maintain stability in the world. Of course, the results of a political cyber conflict have a significant impact on the process of making the most important political decisions in the world. The political elite uses the results of the confrontation as a platform for legitimizing personal decisions and realizing goals at the geopolitical level.

Therefore, the transformation of political conflicts into cyberspace is a manifestation of the modernization of the negotiation process between political leaders, the implementation of the competitiveness of the parties in the election process, and the implementation of globalization political decisions. Since the increase of democratic political regimes implies a constant influence on the political consciousness of society in order to personalize the role of political subjects in making important decisions for the development of the management system and society in general. In today's digital society, it is possible to do this in cyberspace, which has become a parallel reality of the world's existence. Therefore, cyber-conflicts become an integral form of the implementation of the democratic political process, in connection with this, there is a need for the formation of a system of response by management bodies to the danger that they can bring to society.

In this regard, the role of e-democracy is gaining relevance as an integral component of the construction of the latest ideas about political processes in the era of digitalization. Yes, according to L.I. Kormych "e-democracy is an improved model of e-governance that ensures two-way political communication and the participation of non-state actors in the decision-making process. The best way to distinguish between e-governance and e-democracy is by identifying the main stakeholder of the transformations. If digitization affects only the procedural aspect of public administration, it remains a matter of electronic governance" [15, 30]. Therefore, the transformation of ideas about conflict activity and politics through the prism of the new cyber plane should be carried out taking into account the new conditions for the formation of electronic forms of democracy, which create conditions for the formation of cyber conflicts.

International experience of political response to cyber conflicts

The development of cyber conflicts occurs in connection with the discovery of a political incident that does not have a legal continuation mechanism in the information plane. It is very difficult to ensure the reliability of information, in the absence of an effective measure of responsibility, which is regulated by law with a clear application procedure. In turn, there is a need for digital transformation as an activity aimed at finding effective mechanisms for protecting the information environment.

Modern international experience in response to cyber-conflicts, or certain forms of manifestation of cyber-struggle, is reduced to the practice of global participants, at the internal and external level, in the implementation of cyber-influence on political processes. Effective examples of influence that continue to develop are a democratic country and a totalitarian country: the USA and the People's Republic of China, respectively. Their activities are transformed into cooperation with like-minded countries and international organizations that pursue the principles of joint struggle and cooperation in the field of cyber defense.

The democratic state that contains effective mechanisms of the most powerful cyber power is the USA, which has formed the appropriate institutions and regulatory framework for regulating cyber conflicts. Back in 2003, the US National Strategy to Secure Cyberspace was published [36]. This is the period when the process of using computers and laptops in individual activities began in Ukraine, and there was no urgent need for any processes of protection or struggle. However, in the USA, the cyberspace defense strategy has become part of national security.

The National Strategy to Secure Cyberspace proclaims three strategic goals, namely: protecting US critical infrastructure from cyber attacks; minimization of losses and recovery time from cyber attacks; reducing vulnerability to cyber attacks on a national scale [27]. In April 2015, the decree "On the seizure of property of persons involved in serious illegal actions in cyberspace" was signed, its essence is to build a system of responsibility for illegal actions in cyberspace. In the USA, the legal conditions for imposing sanctions on companies and individuals involved in cyber attacks that disrupt the stable functioning of the critical infrastructure of the USA and key computer networks and systems have been created. At the same time, there is a need to apply appropriate sanctions to individuals and companies that, with the help of cyber attacks, have misappropriated funds or other assets, including trade secrets, personal data, and financial information of American companies and organizations, or used them, if they knew that they are stolen in a cyber attack by a third party.

In addition, the process of developing potential protection against any provocative attacks in the USA, or public statements in the information space is quite carefully monitored and eradicated. The practice of blocking President D. Trump's posts in the social network is a demonstration of opposition to any form of undermining stability in society. The process of rapid response to various forms of threats continues to develop. The country is accumulating scientific and human potential that is able to respond to the challenges of modern escalation of tension at the regional, state, and global levels, which demonstrates the ability to fight new challenges in cyberspace.

Another informationally progressive country at the global level is China. In today's global information space, there is sufficient freedom regarding worldviews and statements in the direction of political processes. In cyberspace, the People's Republic of China, over the last decade, is also forming its own system of actions to strengthen national information sovereignty, which creates an ambiguous form of perception in the world. So, on one hand, the USA has repeatedly emphasized the attempts to destroy the integrity of the Internet network by the influence of the PRC, since the state structures of the relevant direction are active in monitoring anti-state processes with specific content and censoring it. From another point of view, we can interpret it as the protection of state interests with a strict system of response and sanctioning.

Of course, the policy of the People's Republic of China is clear and far-sighted for the development of its own media segment, but it hardly fits within the limits of the principles of democratic countries. Another important component is the number of Internet users, which is quite large in China. For example, in 2013, the number of Internet users in the PRC and Internet users in the entire EU exceeded many times [31]. Of course, one of the priorities is the size of the population and the progressive development of China, which is happening quite quickly. In turn, Europe is experiencing an aging population and a significant decrease in the number of young people, who are the drivers of progress and the adoption of the latest developments.

According to Dubov D.V. in China, it is conditionally possible to distinguish two main areas of control. The first direction is the so-called "low level," and the second is "high level." The first level controls not technological, but regulatory and organizational methods related to censorship, that is, the admissibility of individual content, its inviolability of national interests. The second "high level" of control involves limiting the spread of so-called unwanted information, which is related to information and cybernetic technologies, in order to control the internal state of society, the influence on its consciousness. Contemporaries call this a new dimension for the manifestation of dominance in the space of the country [7].

During the study of the People's Republic of China, it becomes clear that in modern Chinese society, national interests are at a higher level than the rights and freedoms of a person and a citizen. It is possible to say that this is a negative phenomenon for the modern geopolitical worldview, but by delving into their internal political system, taking into account historical, cultural, political, and legal values, it is possible to claim that it is precisely such priorities and emphases in making political decisions that help the PRC remain a country with high economic potential, a competitive representative of the progressive countries of the world [31].

Taking into account the peculiarities of the political system depending on the political regime, methods of influence on confrontation in cyberspace, general principles regarding the formation of conditions for such influence, the People's Republic of China and the USA act oppositely regarding the value of human rights in cyberspace, their freedom, and opportunity for self-expression. At the same time, the strategy for improving the existing cyber defense system has common features, namely: increasing human potential in the information field, as the most essential condition for improvement and global impact in general.

Peculiarities of the practical implementation of cyber protection policy in Ukraine

Cooperation with partners on cybersecurity and cyber defense in the conditions of war

Since 2014, Ukraine in the modern conditions of war has quite often felt the impact on the system of protection of critical infrastructure objects, which created the need for regulatory regulation, the development of cyber protection, and the formation of relevant institutions for state regulation of security issues in the information sphere.

In the conditions of consolidation of progressive, peaceful countries of the world, conditions are being formed for a joint interstate fight against cyber conflicts in the form of cyber attacks. Thus, in August 2022, a memorandum on cooperation in the field of cyber defense was signed between Ukraine and Poland. The countries will conduct joint exercises to counter cyber attacks, because Poland, too, has repeatedly become a victim of such attacks from the side of the aggressor, as it fruitfully supports Ukraine in the fight on all fronts, and therefore there is a need to form joint effective efforts to combat the cyber influence that carries destructive nature for the participants of the Memorandum [14].

In addition, a new rapid response program for cyber attacks was announced at the Madrid NATO summit. At the same time, the alliance pledged to strengthen Ukraine's cyber defense against the backdrop of Russia's relentless attacks. After all, Russia systematically carries out cyber attacks on the energy sector, the banking system, and other objects critical to the economy of Ukraine. For example, one of the most powerful was a hacker attack on Ukrainian government websites that took place on the eve of the Russian invasion in January 2022. A message of a provocative nature was posted on the main page of these sites [12, 19].

An important role is played by the normative acts of NATO, which respond to the modern problems of the cybernetic world and demonstrate the modern problem of information threats. Thus, in 2021, the Alliance approved NATO's Comprehensive Cyber Defense Policy with the aim of ensuring a peaceful and secure cyberspace [11]. Such activity demonstrates the formation of the foundations of cyber protection, as the member countries of the Alliance feel the negative impact of cyber attacks, which are the result of political decisions and activities of management bodies. The regulatory framework for the expansion of NATO's influence on cyberspace is regulated by modern challenges and the need to protect member countries from negative influence in the information struggle. Therefore, the Alliance declares that cyberspace belongs to the sphere of responsibility and activity of NATO, also the Alliance defines cyber defense as the main one in the modern information world, and most importantly, Article 5 of the North Atlantic Treaty applies to collective defense and cyberspace in general [10].

Undoubtedly, the issue of impact on cyber conflicts is important for Ukrainian society. In addition, the majority of Ukrainian society and governing bodies are ready for close cooperation with NATO as a security institution. Therefore, the issue of Ukraine's cooperation with NATO in order to prevent and resolve conflicts in cyberspace remains important. Since 2018, Ukraine has already started building a system of defense of cyberspace against negative influences on the NATO model, which demonstrates its effective manifestation in repulsed attacks by our specialists, which number in the hundreds. Such a transformation is a manifestation of the means of necessity in the conditions that have developed in the state. However, in the practical implementation of tasks, Ukrainian specialists demonstrate education and progressiveness in the ability to respond to new challenges [33].

Constant cyber attacks and cybercrime, which adjust society to destabilizing processes in the relationship with governing bodies require constant updating in the cyber defense strategy of Ukraine [20]. The main forms of manifestation are the expansion of the arsenal of offensive cyber weapons, the use of which can cause irreparable, irreversible destructive consequences. At the same time, information and communication systems of state bodies of Ukraine and objects of critical information infrastructure are exposed to the influence of aggressor with the aim of disabling them (cyber sabotage), obtaining covert access and control, carrying out intelligence and intelligence-subversive activities. Cyber attacks are a frequently used method of influence, which also actively acts as an element of special information operations with the aim of manipulative influence on the population and discrediting Ukrainian statehood. Also, they were used during election campaigns in Ukraine and could be misinterpreted as "black PR" and election technologies. However, all these events are a complex of actions on the cyber defense system in Ukraine.

Thus, the State Service for Special Communications and Information Protection of Ukraine published statistics of cyber attacks on Ukrainian critical information infrastructure during March 15–22. According to which, during March 15–22, the Government Computer Emergency Response Team CERT-UA recorded 60 cyber attacks (of them: government and local authorities—11, financial sector—6, telecom and software—4, security and defense sector—8, commercial sector—6, energy—2, and other—22) [25].

About the Cybersecurity Strategy of Ukraine of 2021

The main challenges announced in the cybersecurity of Ukraine by the 2021 strategy are the active use of cyber means in the manifestation of international competition and individual influence at the global level, the competitive nature of the development of cyber security means in the conditions of rapid progressive changes in information and communication technologies, in particular cloud and quantum computing, 5G networks, big data, the Internet of Things, artificial intelligence, etc. [5]. The competitive nature is manifested precisely through cyber conflicts, which can be an effective element of influence, or, on the contrary, a negative consequence of an unsuccessful cyber struggle.

The new version of the Cybersecurity Strategy of Ukraine [5] regulates integration with the NATO cyber defense system as a significant element, because Ukraine's fight against cyber threats has become quite relevant in the modern informational and political space. After all, an effective political system is when the governing bodies are effective. Until 2021, the Cybersecurity Strategy of Ukraine of 2016 [16] was in effect in Ukraine, however, due to the active influence of political actors during cyber warfare, there was a need to improve and specify the problematic aspects faced by Ukrainian society.

The current threat identified in the strategy, which is actually implemented by the aggressor country on the territory of Ukraine, is "the militarization of cyberspace and the development of cyber-weapons, which makes it possible to covertly carry out cyberattacks to support hostilities and intelligence-subversive activities in cyberspace" [5]. The current Russian–Ukrainian war demonstrates the use by special services of information that citizens publish publicly in social networks [35]. In addition, for political leaders, social networks have become a platform for public communication with the population in the conditions of war and a form of reporting on the work done and planned. And videos that appear on social networks are considered as direct public appeals of authorized persons to society. Therefore, the aggressor uses any information that can help in the fight against Ukraine. In this aspect, this challenge is no longer something abstract and distant, but a real form of threat, which had a noticeable negative impact on Ukrainian society in January and February 2022 the most.

Also, important aspects of the challenges are "the impact of the COVID-19 pandemic on economic activity and social behavior, which caused a rapid transformation and organization of a significant segment of social relations in remote mode with the wide use of electronic services and information and communication systems and the introduction of new technologies, digital services and mechanisms of electronic interaction between citizens and the state, which is carried out unsystematically in terms of cyber security measures and without proper risk assessment" [5]. Of course, the socio-political problems that have arisen in the state have increased the use of information and communication systems, and accordingly, the level of danger in cyberspace has increased, because the rapid change of various sectoral forms of activity into the form of cyberspace creates threats in connection with a low protection system.

In the context of the escalation of the conflict between Russia and Ukraine, the 2021 Strategy is already losing its relevance. Because the extreme form of conflict is already developing in practical activities using all possible informational means. In addition, the attack of a country with great resources, which was preparing for this attack on Ukraine, which is in the process of formation and has only started to develop the defense sphere since 2014, is dependent on partners who provide means of struggle, but with logistical collisions. The sphere of cyberspace turned out to be more unprepared than the sphere of defense, and attacks on critical infrastructure continue and intensify against partners who support Ukraine.

In the conditions of endurance of the Ukrainian information and communication system, it is a manifestation of the courage and courage of the Ukrainian society, which does not succumb to such provocations, or simply does not react to them. In this regard, there is an opportunity for management bodies to stabilize communication systems and restore their activity. The experience of such negative processes forms the coordinated work of management bodies and society. In addition, the unification of Ukraine in the fight against cyber threats with individual countries or international security organizations is a way of exchanging experience and practical exercises in the fight against aggressors. At the same time, the negative component of cyber warfare should not be excluded, because its damage to society and the state is significant and requires considerable time to recover. And therefore, the work on improving the system of rapid response bodies needs improvement, and accordingly, the regulatory system must meet the challenges of the times, which demonstrates the need for specialists in information direction.

Conclusions

The article analyses the theoretical and practical form of cyber conflicts during confrontation in political processes with a combination of national and international approaches to the impact on information security and the security system.

The protection of cyberspace is not limited by territorial borders, therefore, international partnership in the field of cyberspace is a modern progressive branch of cooperation at the level of interstate partnership in the study of cyber crimes, as a result of political influence on the opponent. After all, individual struggle in cyber defense processes is not very effective in the global world.

However, it was noted that modern Ukrainian realities place the political and information system of protection within the limits of dependence on international partnership and assistance in the fight against the aggressor, which outlines the limitations of the modern protection system in Ukraine. Modern Ukrainian society needs specialists in the information field, high-quality educational programs and political will for the normative settlement of problematic issues, which are developing faster than the system of management bodies, which institutionally does not meet the challenges of modernity.

The relatively short-term policy of the governing bodies in Ukraine regarding the reaction to cyber rivalry, as a manifestation of political struggle, allows us to assert that the political struggle takes place in a state of transformation in modern conditions into the cyber plane. Borrowing the experience of individual states is determined to be useful for Ukraine in relation to: (a) coordination of the increase of scientific potential and human resources in the field of the IT industry in order to achieve the highest level in the protection of the state's critical infrastructure; (b) improvement of the organization of the political system in the field of formation of the institutional subsystem at the modern information level.

Conflict of interest statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author contributions

Liudmyla Kormych (Data curation [equal], Methodology [equal], Resources [equal], Supervision [equal], Writing – original draft [equal], Writing – review & editing [equal]) and Yuliia Zavhorodnia (Conceptualization [equal], Data curation [equal], Methodology [equal], Project administration [equal], Resources [equal], Writing – original draft [equal], Writing – review & editing [equal]).

References

1. Biletska YV. *Stages of Development of Political Conflicts*. Odesa: National University “Odesa Academy of Law”, 2015, 20.
2. Britchenko I, Romanchenko T, Hladkyi O. Potential of sustainable regional development in view of smart specialisation. *Ikonomicheski Izsledvania* 2019;**28**:88–109.
3. Complex Discovery. *Statistics, Data, Trends of Cyber Attacks in 2022*. 2022. https://complexdiscovery.com/an-evolving-threat-landscape-2022-cyber-attack-statistics-data-and-trends/?amazonai-language=uk (25 June 2023, date last accessed).
4. Decree of the President of Ukraine No. 47. “*Doctrine of Information Security*”. 2017. https://zakon.rada.gov.ua/laws/show/47/2017#Text (25 June 2023, date last accessed).
5. Decree of the President of Ukraine No. 447. *On the Decision of the National Security and Defense Council of Ukraine “On the Cybersecurity Strategy of Ukraine”*. 2021. https://www.president.gov.ua/documents/4472021-40013 (25 June 2023, date last accessed).
6. Derevyanko B, Nikolenko L, Turkot O. *et al.* Mediation as an alternative form of protection of shareholders’ rights in property relations. *Int J Public Law Policy* 2022;**8**:227–41.
7. Dubov DV. *Cyberspace as a New Dimension of Geopolitical Rivalry*. Kyiv: NISD, 2014, 193.
8. Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to Earth. *Int Secur* 2013;**38**:41–73. http://dx.doi.org/10.1162/ISEC_a_00136.
9. Gorwa R, Smeets M. *Cyber Conflict in Political Science: A Review of Methods and Literature*. Toronto: International Studies Association, 2019, 24.
10. Hvozd V. *Cyber Conflict and Geopolitics—a new front of the cold war*. 2018. https://bintel.org.ua/nash_archiv/arxiv-voyenni-pitannya/arxiv-gibridnia-vijna/09_05_krynica/ (25 June 2023, date last accessed).
11. Interfax-Ukraine. *The Leaders of NATO Countries Approved the Alliance’s Comprehensive Cyber Defense Policy*. 2021. https://ua.interfax.com.ua/news/general/750063.html (25 June 2023, date last accessed).
12. Kalinichenko O. NATO on cyber defense: how the alliance helps Ukraine protect itself from hacker attacks by the Russian Federation. *European Truth*. 2022. https://www.eurointegration.com.ua/articles/2022/07/6/7142651/ (25 June 2023, date last accessed).
13. Kochubey LO. Political conflicts in modern Ukraine: prevention technologies and specifics of the course. *Sci Notes* 2013;**41**:16–25.
14. Kostyukova Yu. *Poland and Ukraine Signed a Memorandum on Cooperation in the Field of Cyber Defense*. 2022. https://mind.ua/news/20245980-polshcha-ta-ukrayina-pidpisali-memorandum-pro-spivpracyu-u-sferi-kiberzahistu (25 June 2023, date last accessed).
15. Kormych LI, Kormych AI. Improvement of public administration in Ukraine in the context of digitalization: theoretical aspect. *Actual Problems Polit* 2022;**69**:5–12.
16. Law of Ukraine No. n0003525-16. “*About Cyber Security Strategy of Ukraine*”. 2016. https://zakon.rada.gov.ua/laws/show/n0003525-16#Text (25 June 2023, date last accessed).
17. Law of Ukraine No. 2163-VIII. “*On the Main Principles of Ensuring Cyber Security of Ukraine*”. 2017. https://zakon.rada.gov.ua/laws/show/2163-19#Text (25 June 2023, date last accessed).
18. Liff AP. Cyberwar: a new “absolute weapon”? The proliferation of cyberwarfare capabilities and interstate war. *J Strateg Stud* 2012;**35**:401–28.
19. Levchenko I, Losonczi P, Britchenko I. *et al.* Development of a method for targeted financing of economy sectors through capital investment in the innovative development. *East Eur J Enterp Technol* 2021;**5**:6–13.
20. Ozhevan M. Fronts and rears of great information wars: general informational needs and interests. *Entrep Ukraine* 2001;**4**:20–3.
21. Puyvelde DV, Brantly AF. *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Hoboken: Wiley, 2019, 224.
22. Rid T. Cyber war will not take place. *J Strateg Stud* 2012;**35**:5–32.
23. Rzhevska NF. Geoinformational factor as a mechanism of transformation of international conflicts. *Eur Polit Law Discourse* 2017;**4** 47–52.
24. Sitarskyi SM. Political conflict and modern Ukrainian realities. *Economy State* 2013;**8**:137–9.
25. State Service of Special Communication and Information Protection of Ukraine. *Statistics of Cyberattacks on Ukrainian Critical Information Infrastructure: March 15–22*. 2022. https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya (25 June 2023, date last accessed).
26. Tarasenko N. The doctrine of information security of Ukraine in the evaluations of experts. *Resonance Bull* 2017;**18**:3–53.
27. The White House. *The National Strategy to Secure Cyberspace*. 2003. https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf (25 June 2023, date last accessed).
28. Tor U. Cumulative deterrence’ as a new paradigm for cyber deterrence. *J Strateg Stud* 2017;**40**:92–117.
29. Voice of America. *The US Cooperates with Ukraine to Export Grain for Africa*. 2022. https://ukrainian.voanews.com/a/6613209.html (25 June 2023, date last accessed).
30. Yasynska NA, Syrmamiikh IV, Derevyanko BV. *et al.* Transformation of the metallurgical industry of Ukraine from the concept “Industry 4.0” to capitalism of stakeholder. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu* 2022;**2**:166–73.
31. Zavhorodnia Y. Features of protection of China’s national interests within cybernetic space. *Eur Polit Law Discourse* 2021;**8**:37–42. http://dx.doi.org/10.46340/eppd.2021.8.6.6.
32. Zavhorodnia YuV. Cyber conflicts as a modern threat of digitalization of society: political aspect. *Actual Problems Philos Sociol* 2022;**35**:88–92.
33. Zavhorodnia YuV. The role of NATO in the fight against cyber conflicts. *Reg Stud* 2022;**30**:67–71.
34. Zavhorodnia YuV. Transformational ideas about conflict in political processes. *Actual Problems Polit* 2022;**69**:61–4.
35. Zavhorodnia Y. *Political Conflicts as a Prerequisite for the Russian–Ukrainian War: Manipulative Features*. Riga: Baltija Publishing, 2022, 1436.
36. Zhadko VO, Kharitonenko OI, Poltavets YuS. *Hybrid War and Journalism. Problems of Information Security*. Kyiv: Publishing House of Drahomanov National University of Applied Sciences, 2018, 356.