ARTIFICIAL INTELLIGENCE AND/OR CYBERTHREATS IN HYBRID WARFARE

Kharytonov Yevhen
Doctor of Law, Professor, Corresponding Member of the National Academy of Legal Sciences of Ukraine, Head of the Department of Civil Law of the National University, "Odesa Law Academy"
ORCID ID: 0000-0001-5521-0839

Kharytonova Olena
Doctor of Law, Professor, Corresponding Member of the National Academy of Legal Sciences of Ukraine, Head of the Department of Intellectual Property and Patent Justice of the National University "Odessa Law Academy
ORCID ID: 0000-0002-9681-9605

Tolmachevska Yuliia
Ph.D., Executive Editor of the scientific journal "Lex Sportiva", Private Lawyer
ORCID ID: 0000-0002-7964-8875

Preliminary remarks

The realities of modern times are the gradual but relentless involvement of an increasing number of countries in hybrid wars, which threaten to turn into a World War. This danger is further exacerbated by the "virtualization" of society, the emergence and growth of the power of cyber weapons, in particular, due to the use of artificial intelligence technologies in hybrid cyber warfare.

When considering this problem, first of all, we must define the concept of hybrid warfare.

"Hybrid warfare" in the modern world

Analyzing the phenomenon of hybrid war in the context of 154ussian aggression against Ukraine, the researchers characterize it, first of all, "as a new conflict and as a form of global confrontation," and emphasize that "the concept of hybrid war has proven to be theoretically and practically the most suitable for determining the specifics of the actions of the 154ussian federation, which, combining military, quasi-military, diplomatic, informational, and economic means, not disdaining nuclear blackmail, consistently tries to achieve its own political goals in Ukraine and other parts of the world that are not fully understood by the international community (Yavorska, & Yizhak, 2017)."

It should be emphasized that the concept of hybrid war encompasses not only modern forms of warfare, types of future wars, or names of specific mixed-type conflicts, but is a new type of global confrontation in the current destabilized international security environment.

Since the general term "hybrid war" covers a number of diverse actions and behaviors, there is a need to structure the corresponding concept. Moreover, this term is used, first of all, to denote war in the traditional sense, but a war that is complicated, "burdened" with additional elements, components, the use of non-traditional means, methods, etc. For example, the definition of hybrid war proposed in The Military Balance in 2015, covers (1) the use of military and non-military means in a comprehensive campaign aimed at achieving the effect of surprise, seizing the initiative and obtaining psychological and physical advantages through diplomatic means; (2) conducting complex and rapid information, electronic and technological operations; (3) carrying out both covert and overt military and intelligence actions; (4) exerting economic pressure (The Military

Balance, 2015). This definition was later recognized by some authors as the most successful (Gumenyuk, 2022).

Thus, although "military war" is prominent, the term "war" in a broad sense is also used in areas that do not involve any use of military weapons, for example, "informational, economic, political war." In each case, we can talk about certain characteristic methods of action in the mentioned areas, however, in the traditional sense, they are, according to some authors, only components of a "military" war (Yavorska, & Yizhak, 2017).

In our opinion, the main flaw of this approach is that by denying the appropriateness of recognizing certain types of war and tying them to the idea (requirement) of "functionally transforming traditionally non-military means of force into weapons and combining them on this basis with actual military methods," we lose the possibility of their independent analysis in cases where the aggressor avoids "recognition of a state of war" (and even "armed conflict"), does not use "actually military methods," etc., but achieves the goal in another way (political, economic, legal, mental-religious, diplomatic, cultural, etc. pressure).

Actually, this is exactly what 155ussia did during the years 1991-2013. Moreover, even after 2014, it managed to avoid declaring war and achieve its goals using non-military means of force without combining them with actual military methods.

Therefore, the currently established approach to determining the relationship between the concepts of "war" and "hybrid war" requires revision, taking into account the following methodological principles of the study.

First of all, it is advisable to distinguish between the categories of "hybrid military war" and "hybrid war – a general phenomenon."

In the first case, we are talking about the "hybridity" of war as an armed conflict – a construct that arose on a traditional basis and is now undergoing transformations due to the use of new methods, forms, and means of military action.

In the second case, we mean the "hybridity" of war in a broad sense – as a social conflict, confrontation of states, communities, societies, civilizations. War in this sense also includes "military war" (armed conflict), but can occur without the use of traditional weapons at all, but with the use of other means of influence (coercion) of subordinating one side of the conflict to its other side.

The criteria for their distinction are: goal, motivation (expectation), environment, means (methods), result. Of these, the most important for pragmatic classifications, in our opinion, are the environment (sphere) where the confrontation takes place, and the means (tools, methods) of the confrontation (war).

Taking into account these criteria, the following types of hybrid warfare can be distinguished (which can intersect and interpenetrate. The list is indicative):

1. Military (to avoid the word "war", it is often replaced with euphemisms such as "liberation campaign", "fraternal aid", "international duty", "introduction of a limited contingent", "SMO (Special military operation)", etc.)
1. Informational
2. Economical
3. Legal
4. Ideological
5. Cultural
6. Psychological

7. Historical
8. Diplomatic
9. Cyber /Technology

In further characterizing hybrid war, we will rely on the statement of K. von Clausewitz, which he made in his work dedicated to "war-armed conflict", but which also applies, in our opinion, to the phenomenon of war in general: it is, first of all, "an act of violence aimed at forcing the enemy to fulfill our will (Clausewitz, 2018)."

Based on this understanding of the essence of war, we will further consider the features of the modern understanding of it and hybrid war, having previously noted that in our country, studies of this category were especially popular in the first years after the start of 156ussian armed aggression in Ukraine (Danyk, Malyarchuk, & Briggs, 2017; Magda, 2015; Magda, 2014; Pocheptsov, 2015; Puvelde, 2015; Svitova, 2017; Taranenko, 2016; Yavorska, 2016;), with a decrease in interest during the ATO (Anti-terrorist operation) and JFO (Joint Forces Operation) (Syrotenko, 2020; Sokolov, 2021; Bratko, Zaharchuk, & Zolka, 2021; Osiichuk, & Shepotylo, 2020; Tkachuk, Shynkarenko, Tokovenko, Svorak, & Lavoryk, 2021).

Currently, the task of taking into account the positions of specialists in this field is facilitated by the appearance of a number of works of a survey nature. In particular, such a work is the research of Zh. Pavlenko and A. Antonov in 2023 "Hybrid War": Analysis of Definitions of the Concept" (Pavlenko, & Antonov, 2022). The authors rightly note that scientific works on the issue are carried out mostly within the framework of military and political sciences, although these studies require, first of all, a deep and thorough philosophical, in particular logical-methodological, understanding in order to construct the concept of "hybrid war".

Agreeing with this thesis, we note at the same time that the authors use popular, but in our opinion erroneous, ideas about the relationship between genus and species when characterizing these concepts, when they write: "It is impossible to understand the concept of "hybrid war" without its generic concept – "war". At the same time, the latter is considered by them as a phenomenon "the essential features of which are considered to be organized armed struggle between states, social classes, etc.; a conflict carried out by force of arms, both between countries and between parties within a country; a period of armed hostilities or active military operations carried out by land, sea or air". In addition, they interpret war as primarily a physical, material phenomenon (Pavlenko, & Antonov, 2022).

In fact, "hybrid war" here is a generic concept for the concept of "war – armed conflict". As E. Magda notes, "war is not only direct combat operations, but also the competition of economies, ways of life and thinking of rulers, the competition of systems of state administration, the clash of potentials and the confrontation of ideologies" (Magda, 2015). The main feature of such a war is its "hybridity: it is simultaneously an informational, economic, reputational, and semantic war. Everyone who has influence on the population must work on it: actors, singers, writers, directors. Military actions only set the background for a larger-scale war in the human mind (Pocheptsov, 2015)."

RNGW (Russian Next Generation War) = a version of the hybrid warfare concept.

There is an opinion that the concept of hybrid warfare belongs to russian general Gerasimov (Khorunzhy, 2022).

This is not true, although it should be recognized that it was in Ukraine that russia brought hybrid warfare to an absolute level (Magda, 2015).

In fact, the priorities in the field of creating a modern concept of hybrid war belong to the USA. Instead, the russian achievement, in fact, consists in the modernization by V. Gerasimov of the ancient russian theory of unconventional wars (and in fact - "wars without rules"). The founder of this theory, Isserson, wrote in the book "New Forms of Struggle", back in 1940: " *War is not declared at all. It simply begins with the armed forces deployed in advance*." An important role was also played by the provisions of the works of Messner (a military theorist from the White emigration, whom analysts call Putin's favorite strategist) regarding the wars of the future: "*In past wars, the capture of territory was considered important. In the future, the capture of souls in the state with which one is at war will be considered the most important*." Believing that traditional methods of warfare had already been exhausted, he substantiated a number of important conclusions: "*Once upon a time, wars were fought in two-dimensional space — on the surface of the sea and land. Then a third dimension appeared — war in the air. Now the most important thing is the fourth dimension — the psyche of the warring parties*." The Americans lost the war in Vietnam precisely in their heads. *"Politics is the art of uniting people. The most important task in insurgent warfare is to unite one's own people and attract to one's side part of the people of the state with which the war is being waged*," he noted (Pocheptsov, 2015).

Referring to the fact that the "rules of war" have changed now, since non-military tools are becoming more effective than military ones, Gerasimov substantiated the thesis that political, economic, informational, and humanitarian methods are now gaining importance, activating the protest potential of the population. Covert military means are added to them. (In passing, we note the correctness of the remark that "russia has never used the term "hybrid" in its strategic documents and doctrines. Moreover, the idea was promoted in russia that it was not russia, but the West that was waging a hybrid war against it, and this was precisely the Western concept. In the presentation of the russian vision of hybridity in early 2013 by V. Gerasimov, it was not about russia's actions, but contained a conspiratorial russian version of the "Arab Spring" and the task was set to find methods of counteraction. Therefore, russia developed its own methods of hybrid war, which were soon used against Ukraine (Dolzhenko, 2018).

As Herbert noted McMaster: "To fend off domestic opposition and restore Russia's greatness, Putin has resurrected the country's nationalist mission, portraying his people as fearless and crafting a foreign policy designed to intimidate neighbors and shake Western democracies (McMaster, 2023)."

Putin's ambitions pushed him and the country he led into a war for "lost greatness", for the sake of which it was worth fighting numerous opponents - according to his estimates, the entire free world. At the same time, the battle "for greatness" for russia was associated with the problem of survival, since, as H. McMaster notes, "it was not strong enough to directly compete with the United States and its allies in Europe and Asia, inferior to them in all major economic indicators. Russia's vulnerabilities were also corruption (according to the "Corruption Perception Index" - 135th place in the world), adverse demographic trends. But in accordance with their KGB habits, Putin and Patrushev are not interested in building russia, but in undermining other states. ...he develops complex strategies aimed at achieving goals located almost on the border, the crossing of which is capable of provoking a concerted response either from the target state or, say, its NATO allies (McMaster, 2023)."

The provisions of V. Gerasimov's 2013 article with its emphases are based on such ideological principles: "the very "rules of war" have changed," "the role of non-military methods

of achieving political and strategic goals has increased, which in some cases significantly exceed the power of weapons in their effectiveness."

As mentioned, the "Gerasimov concept" also had as its source the achievements of the Americans, who, in their search for means of combating international terrorism, drew attention to the expediency of emphasizing "non-military operations" (Operations Other Than War) in close interaction with non-state actors and the media environment. This radically changed the approaches to military strategy - the primary targets of strikes were now selected based on the subsequent "necessary" information "resonance" of such actions. Therefore, the first target of the war became the enemy's information infrastructure: the enemy society received specially prepared information. This concept received a new stage of development after the tragic events of September 11, 2001, when the main enemy became dispersed, horizontal networks of terrorist groups without a rigid vertical of control "sponsor country - group leader - field commanders - militants". To combat such an enemy, a tool was needed that would take into account the new information reality of the "Internet 2.0" world. Thus, a new concept of information and psychological confrontation appeared called Network-Centric Confrontation (Network-Centric Warfare – NCW).

The Russian military-political leadership was delighted with the idea, and to eliminate the problems with its practical implementation, they found a simple solution: instead of traditional military units, use "hybrid", unidentified troops. While the enemy is trying to understand what the source of the threat is, until he comes to his senses, the operation ends with the information "effect" that is formed by the aggressor. The borrowed idea was "rechristened" as "network warfare". The Chief of the russian General Staff, General V. Gerasimov, gave lectures to the Academy of Military Sciences, which were called "Gerasimov Doctrine 1.0 and 2.0". Later, the hybrid toolkit was called "asymmetric actions"). On March 2, 2019, General Gerasimov presented a continuation of his previous speech to the members of the Academy of Military Sciences, which took into account practical lessons and conclusions (Zhovtenko, 2022).

According to McMaster, the combination of these and similar statements, combining disinformation and denial of responsibility with the use of destructive technologies, with which russia attacks the strengths of target states and plays on their weaknesses, planning to use economic dependence on energy supplies supplied by russia, bravado, recognition of the expediency of using advanced, unconventional, conventional and nuclear military means, and made up the "Gerasimov doctrine", also known as "Putin's method", "Russian next-generation warfare" (RNGW), and "hybrid warfare".

The creation of russia's "own" hybrid war doctrine was a search and testing of means to achieve the desired global result. "Simply put, russia's geopolitical goal in resolving the global hybrid conflict was realized as follows: to destroy the existing world order by means of hybrid war in order to restore the world order of the Cold War period and take its usual place in it ... it is necessary to understand and accept that the new hybrid world (dis)order that is being built before our eyes is not some "transit state", it is a new reality that cannot be extrapolated to the realities of the past. ... in this new hybrid reality there may simply not be a worthy place for russia", because it "itself becomes very vulnerable to the tools and mechanisms, methods and methodologies of hybrid war if they are used against it (Gorbulin, 2017)".

Having noted the appropriation of the concept of hybrid war by russian politicians and military personnel, we agree with the position of G. Pocheptsov that in fact the concept of hybrid war in its modern (military) understanding was introduced by F. Hoffmann, who formulated

several important postulates: 1) "*Hybrid wars are not new, but they are [always] different*." 2) "*Hybrid wars combine the lethal nature of state conflicts with the fanatical and protracted fervor of irregular warfare*." 3) in such wars the interaction of cognitive and virtual spaces must be taken into account (Hoffman, 2009).

Hybrid warfare favors those who can manipulate mass consciousness. The attacking party must justify its actions to both its own people and the people it targets. And it is quite difficult for the attacked party to respond to such an undeclared war (Pocheptsov, 2015).

It is necessary to agree with the opinion that hybrid warfare has become an achievement of modern times precisely because many of the tasks required for it can be performed at the expense of the information component. The stronger the development of the information component becomes, the easier it will be to perform these tasks.

At the same time, such factors as the formation of an information society and the development of information technologies are of great importance, which determines the "routineness" of cyberwar. As David Sanger notes, "one would like to think that cyberwar is somehow different from other conflicts, as if it unfolds somewhere in the clouds, separate from what is happening on the ground. When states created air forces, they reasoned in the same way: air battles are one thing, and firefights in the trenches are another. It was not until World War II that the concept of a "single combat space" was established, encompassing air, land, and sea. In some countries of the world, cyberspace is already being added to this. It's just harder to notice (Sanger, 2022)."

Suddenly, there were practically no countries left that would not be convinced of the correctness of this observation in one way or another. This became especially noticeable after the russian aggression against Ukraine. Moreover, "in the battle for the territory of Ukraine and the souls of its inhabitants, traditional war and cyberwar did not simply complement each other. They, like a Mobius strip, reflect the conflict of the 21st century, smoothly flowing from surface to surface again and again. Putin demonstrated to the world how effective this strategy of "hybrid war…" is (Sanger, 2022).

We already considered the legal problems of information hybrid warfare in 2016-2018 (Kharytonov, Kharytonova, Tolmachevska, Fasii, & Tkalych, 2017; Kharytonov, & Kharytonova, 2017; Kharytonov, & Kharytonova, 2019), but a lot of time has passed since then and a lot has changed.

First of all, it should be emphasized once again that currently "information warfare" is a generic term for all types of confrontation in the information sphere - both traditional and modern, taking place in cyberspace.

Due to these qualities, the term "information warfare" has about ten meanings. Let us limit ourselves here to mentioning only the understanding of it as a form of confrontation between subjects ... which involves informational influence on the population using the media, computer networks, etc. with the aim of forming the appropriate public opinion, undermining the morale of both the entire society and its individual institutions (Popova, & Lipkan, 2016).

Against this background, the concept of "cyberwar" is defined briefly: it is a type of information warfare in cyberspace. A component of cyberwar is a "cyber threat" - "a destabilizing factor of negative impact on the object of information security by using the technological capabilities of cyberspace, aimed at violating the confidentiality, integrity, authorship, observability and accessibility of information; the threat of using destructive information and psychological influences on the consciousness and mental state of the population (Popova, & Lipkan, 2016)." (The most common

threat is a cyberattack - or - an attack on an information and telecommunications system - a targeted impact on vulnerable elements of such a system in order to violate the accessibility, integrity and confidentiality of information, block the work and disable the system or its elements; a form of struggle in telecommunications systems (Popova, & Lipkan, 2016)).

As follows from this understanding of cyber threats, an integral part of their characteristics are the categories of " cyber weapons " and "cyberspace."

Cyberweapons are understood as "a type of information weapon, the main elements of which are information and information technologies, methods and means of information influence and protection of freedom, intended for waging information warfare in cyberspace.

Cyberspace, even at the level of elementary characteristics, has several meanings: 1. An electronic information environment formed by an organized set of interconnected information, telecommunication and information-telecommunication systems according to common principles and rules. 2. An environment for the existence and dissemination of information created by cyber infrastructure. 3. An environment created by information systems combined into local or global computer networks or implemented on individual computers and other devices. 4. An imaginary environment in which digital information circulates using computer networks (Popova, & Lipkan, 2016)."

The aforementioned concepts are quite clearly related to the concept of "cyberspace", which serves as both the background and a qualifying characteristic of cyberwarfare, cyberthreats, etc.

Artificial Intelligence as a Cyberweapon

Cyberweapons in the modern world are becoming one of the main tools of hybrid warfare. Back in 2010, Myroslav Popovych, in the preface to Volodymyr Horbulin's book "Without the Right to Repent," emphasized that: "future conflicts require, first of all, high-precision weapons and a developed information technology system (Gorbulin, 2010)."

According to David E. Sanger, "Cyberweapons are so cheap to produce and so easy to conceal that the temptation is irresistible (Sanger, 2022)." Therefore, while "a decade ago only three or four countries had effective cyberweapons, now there are more than thirty. The curve of cyberweapon production over the past decade generally resembles the takeoff trajectory of a fighter jet. The new weapon has already been used many times, even if the results have been mixed… The modern armed forces of any country cannot function without a cyber arsenal, just as after 1918 it was impossible to imagine an army without airplanes. Today, as then, it is impossible to predict how much this invention will change the use of state power (Sanger, 2022)."

At the same time, a reminder-warning becomes a reality: "We all live in fear that our dependence on digital technologies will be turned against us by other states, which over the past decade have found new ways to continue the old confrontation. We already know that in the face of cyber weapons, as in the face of nuclear weapons, everyone is equal. And we have every reason to worry that in a few years these weapons, together with artificial intelligence, will act so quickly that people will not have time to either realize the threat or prevent it - so the attacks will occur and lead to an escalation of the conflict (Sanger, 2022)."

Let us note this circumstance, which causes a higher level of threat – one that can go beyond human control: the combination of cyberweapons with artificial intelligence. This is the main hybrid threat, and therefore requires an adequate (hybrid) response, in particular, through legal measures.

At the same time, we note that while the creation or improvement of cyberweapons is by definition a non-public matter, and the regulation of relations related to it is a secret, the development of artificial intelligence in itself seems to be a more peaceful pursuit, and

achievements often become material for discussion in the media (albeit mainly in a journalistic and popular form).

At the same time, artificial intelligence can be used as a cyber weapon (or as an element of a cyber weapon) not only in information hybrid warfare, but also in “military” hybrid warfare (for example, to conceal information important for the investigation of war crimes or to steal information regarding the planning of military actions, logistics, etc.).

In particular, as the BBC found out, evidence of potential human rights violations may be lost due to their removal by social networks, which use artificial intelligence to remove videos containing scenes of violence from their platforms.

Meta and YouTube claim that this is to protect users from harmful content. Instead, social networks insist that videos from war zones can remain online if they are of public interest. However, when the BBC tried to upload footage of the killing of civilians in Ukraine, it was removed.

Artificial intelligence is programmed to automatically remove harmful and violent content. However, when it comes to moderating videos from countries where there is a war, the machine simply cannot determine whether the footage is evidence of human rights abuses. "The AI was programmed so that the moment the machine sees something that seems difficult or traumatic, it immediately removes it," Rusbridger explains to the BBC. The Meta Council, of which he is a member, was created by Mark Zuckerberg. It is a kind of independent "supreme court" of the company that owns Facebook and Instagram.

Therefore, archiving materials from social media often falls on the shoulders of ordinary people or volunteers, which complicates possible prosecution for war crimes in the future (Goodman, & Koreniuk, 2023).

At the same time, AI can not only delete information, but also create it, distorting the essence of events or creating events that did not exist (Wang, 2024).

Leaving this problem for a special study, let us move on to considering the problems of using AI in “military” warfare.

Artificial Intelligence in the "War of War": The Collision of Defense and Aggression Goals

The use of artificial intelligence in "military warfare" is complicated, among other things, by the existence of a conflict of public and private interests, the resolution of which requires "hybrid" legal support in this case as well.

The material by Daryna Boyko and Ivan Horodysky from the Dniestryansky Center “Artificial Intelligence in Defense: Regulatory Challenges” is specifically devoted to the analysis of problems in this area, prepared in January 2024 with the support of the European Union and the International Renaissance Foundation as part of the joint initiative “European Renaissance of Ukraine” (Boyko, & Horodyskyi, 2024). According to its authors, the main problem in this area is Ukraine’s use of AI technologies for recognizing people using images from social networks and the Internet (Boyko, & Horodyskyi, 2024), automated data analysis using natural language processing technology, etc., developed by well-known foreign companies that were previously criticized due to “security and human rights issues”. Despite the fact that the use of the aforementioned AI technologies gives obvious positive results during the armed confrontation with Russia, a significant challenge for their use in Ukraine is considered to be the problem of ensuring the protection of human rights (Boyko, & Horodyskyi, 2024).

In general, the use of AI technologies (even for purely military purposes) has caused concern among international organizations, such as OpenDemocracy, which in March 1922 (that is, at a time when the fate of Ukraine was literally hanging in the balance) was concerned that the Ukrainian military had received technological means capable of helping them deter the aggressor (Meechem, & Gak, 2022). Representatives of civil society in Ukraine reacted to this "concern", expressing concerns that the further use of technologies prohibited in some EU states could slow down or jeopardize the process of Ukraine's accession to the EU (Lyudva, & Avdeeva, 2023). The existence of a problem of control over the use of AI has also been noted by foreign and domestic legal scholars (Kostenko, Jaynes, Zhuravlev, Dniprov, & Usenko, 2023).

Considering the aforementioned risks for the further use in Ukraine of technologies similar to Clearview AI, Palantir, etc., the authors of the article "Artificial Intelligence in Defense: Regulatory Challenges" emphasize that the protection of human rights when using AI technologies is the main problem for Ukrainian regulators in the context of war, and they see its solution in distinguishing between two scenarios of AI development - "peaceful" and "military" - and developing appropriate rules for each of them (Boyko, & Horodyskyi, 2024).

Such a proposal seems logical to us, since there are normal situations and there are abnormal ones: the rules that apply to normal relationships do not apply to abnormal situations.

But it should be noted here that the problem of regulating the use of AI in Ukraine is exacerbated by the need to take into account not only the specifics of "peaceful" and "military" algorithms, but also European integration processes. In this regard, in October 2023, the Ministry of Digital Transformation published a Roadmap for the Regulation of Artificial Intelligence in Ukraine , which is seen as a confirmation of the government's intentions to gradually implement the EU AI Act, which pays significant attention to the protection of human rights in the implementation and application of AI.

In the first phase of regulation, which, according to the Roadmap, will last until 2025/2026, the government will try to "not regulate" the AI industry, while preparing businesses for legally binding regulation. However, during a full-scale war, regulation of AI in projects related to military needs is not envisaged.

"We need to use the zoning principle: what should be the regulation of AI during war and after victory. During war, we plan to develop a legislative framework that will not hinder the use of AI innovations and technologies for victory. But after the war, AI regulation should help Ukraine continue to strengthen democracy," A Anna Bulakh, head of AI ethics and partnerships at Respeecher and member of the AI committee at the Ministry of Digital Affairs, told Delo.UA.

We think this decision is entirely justified. At the same time, we note that discussions are emerging among Ukrainian AI experts regarding the use of defensive AI after the end of the war. However, these issues will require additional discussions and the development of separate standards.

We should also note that the authors of the previously mentioned analytical material "Artificial Intelligence in Defense: Regulatory Challenges", despite noting the fact that artificial intelligence proved its effectiveness during the russian-Ukrainian war, insist on taking into account the risks of AI, believing that these risks cannot be subject only to industry-wide "self-regulation", in particular when it comes to the use of AI technologies beyond repelling Russian aggression.

In their opinion, the following measures, in particular, can eliminate risks and ensure the "fair and accountable" use of AI technologies in the "peaceful" sphere:

- Amendments to current legislation, elimination of regulatory gaps in the use of AI technologies for defense purposes, in order to ensure guarantees for the protection of human rights

and freedoms. Experts from the Digital Security Laboratory propose to amend the laws "On Personal Data Protection", "On National Police", as well as the Criminal and Criminal Procedure Codes for this purpose.

- Prioritizing the introduction of regulation (instead of self-regulation) in the development and use of AI technologies used for defense purposes. The risk of interference with democratic rights and freedoms is a major argument in favor of proactive action.
- Control by responsible persons or the court over the use of these technologies.
- Publicity of the process of regulating the use of these technologies: constant discussions and debates to achieve a balance of interests between the authorities, civil society and AI development companies.

Finally, the authors of the cited material emphasize once again that the main task for Ukrainian regulation of the scope of application of defense AI technologies should be to ensure the protection of human rights that may be affected by such application, especially if these technologies are used not on the battlefield. This should be the core idea in creating legal regulation of AI technologies, along with ensuring the economic development of the industry (Boyko, & Horodyskyi, 2024).

In conclusion, we return to the questions again: is it necessary to distinguish between "military" and "non-military" applications of "defense" AI? And what is "defense AI": "intended for defense" or one that was once "developed for defense" but has lost its purpose and is used "not on the battlefield." Then, why is it "defense"?

The thesis regarding the main task for Ukrainian regulation of the scope of application of defense AI technologies is most doubtful. The most important question here is the following: is the main task to ensure the protection of human rights or to ensure the survival of the country in a war of an existential nature, as experts often mention. Because if we do not take into account the second, then the first problem will simply disappear, because bloody experience shows that it is naive to expect the russian occupiers to ensure the protection of human rights.

In this regard, we optimistically note the rational approach reflected in the "White Book" developed by the Ministry of Digital Transformation (Ministry of Digital Transformation of Ukraine, 2024). Introducing it, Deputy Prime Minister, Minister of Digital Transformation Mykhailo Fedorov, noted that the White Book describes in detail Ukraine's approach to regulating AI and drew attention to the fact that it takes into account the challenges of our reality, and therefore the defense sphere remains outside of regulation: "We must not limit such AI products, but on the contrary - introduce more innovations that help fight the enemy. We also understand that for the development of Ukraine, maximum deregulation and reduction of bureaucracy are necessary in order to get rid of obstacles to the implementation of technologies. At the same time, the danger of the rapid development of artificial intelligence and its potential impact on human rights is now recognized by the whole world. To maintain balance, we have developed an approach that addresses the challenges without introducing mandatory regulation in the next 2–3 years." He also noted that "Ukraine is betting on flexibility and adaptability. We are giving business time and tools to prepare for future national legislation. The White Paper provides for specific tools, some of which businesses can use now. They will allow us to prepare for entering the EU market, where the relevant regulation will soon be approved. The next stage is to harmonize our legislation with EU legislation. This is not only necessary for European integration, but will also allow us to more actively attract investments to the Ukrainian market. In particular, due to identical legal regimes (Ministry of Digital Transformation of Ukraine, 2024)."

Comparing EU legislation on AI and Ukraine's position on this issue, Forbes notes that according to a Kantar survey Ukraine, published in the White Paper, 45% of Ukrainians believe that Ukraine should adopt a law on the regulation of artificial intelligence. The European Union, which was the first in the world to take up the regulation of AI: in March 2024, the European Parliament adopted the AI Act, was chosen as an example to follow. However, as stated in the White Paper, Ukraine is not yet on this path at the first stage, but at the second stage it will adopt a law - an analogue of the European AI Act (Nesenyuk, 2024).

Summing up this fragment of our intelligence, we note that the discussion in the field of interest to us will obviously continue, and various solutions are possible. Therefore, we will next consider general/international trends in regulating the use of cyber weapons.

The problem of international regulation of the use of cyber weapons

Above, we discussed the problems of regulating the use of cyberweapons by the "domestic" legislation of the country, which establishes the rules for the use of AI by subjects of civil relations in a particular state.

However, even more important is the establishment of rules for the use of cyber weapons by participants in an armed conflict (of course, provided that they comply with these rules). As David Sanger noted: “In the cyber era, we have not yet found a balance of power with the main adversaries (which was a guarantee of mutual destruction in the nuclear age) and, probably, we will not find it. Cyber weapons are completely different from nuclear weapons, and so far the consequences of their use are relatively insignificant. However, to think in this way is to assume that we understand the destructive power of the technologies we have created and can cope with them. As history shows, this is an extremely risky belief.” (Sanger, 2022) And he adds: “During the Cold War, we learned, albeit not easily, to live with the awareness that the nuclear weapons of the Soviet Union and China are aimed at us. There was no perfect defense. Similarly, we will have to get used to living in a world of constant cyber conflicts (Sanger, 2022).”

Considering that the aforementioned work by David Sanger, in our opinion, is currently not only the most interesting and meaningful study of the use of cyberweapons in the modern world, but also the most constructive collection of author's proposals for resolving the problems of using such weapons, we will further consider the possibility of implementing them in the practice of overcoming challenges in the cyber sector of hybrid warfare.

It should be noted that D. Sanger states that there are significant difficulties in reaching interstate agreements on deterring cyber threats. He mentions the approach of the US Cyber Command , which involved almost daily raids into the enemy's rear in order to detect threats before they reach American computer networks - "to transfer combat operations to enemy territory", and notes that this is an attempt to use the experience of conducting anti-terrorist operations.

“But the problem is that if other countries adopt the same strategy, and they certainly will, then the likelihood of cyberattacks escalating into conventional warfare or even something worse will increase dramatically,” he believes, and then suggests recognizing the absurdity of going on the offensive without proper defense (removing vulnerabilities in networks). Given how complex the Internet is, the government cannot regulate the activities of banks, telecommunications and gas companies, Google and Facebook in the field of their own cybersecurity. All systems are fundamentally different from each other. However, it is time to look at everything realistically. The government will not help protect American institutions, except perhaps the most important

power grids, voting systems, water and sewage systems, the financial system and nuclear weapons (Sanger, 2022).

Since the capabilities of the governments of other states, in particular Ukraine, also do not overcome this bar, resolving the problem at the "extra-state" level becomes of particular importance.

We deliberately use the term “non-state” here, realizing its incorrectness, but wanting to emphasize an important dominant of the concept of David Sanger, who believes that “Classical arms control agreements will not work: they take years to negotiate, and the ratification process is even longer. Given the lightning pace of technological change in cyberspace, such agreements would become obsolete before they even enter into force.” Therefore, he suggests turning to other ways to achieve the goal, and each has significant drawbacks.

In his opinion, the most interesting way is the Digital Geneva Convention (Digital Geneva Convention - an initiative of 34 large IT companies that proposed to conclude a convention on developing common rules of conduct in cyberspace), in which companies, not countries, are currently leading. A significant role is played by Microsoft President Brad Smith, who seeks to create a model of cyber agreement between companies that would be based on conventions that regulated traditional warfare and were improved over a hundred years.

However, David Sanger believes that “the analogy with cyberspace is difficult to draw. The Geneva Conventions apply in times of war. If we hope to create a similar set of rules for the cyber dimension, then we must define peacetime standards. And these standards should apply to companies as well as to countries, because Google, Microsoft, Facebook, Cisco create the cyberspace in which global cyber conflicts unfold.”

Next, we will briefly consider what solutions are proposed in this project. digital Geneva Convention (Prognimak, 2017), also using the qualified commentary of Professor Heidi Heidi Tworek) (in an adapted version of her article for Wired).

What Heidi Twork thinks, Microsoft, apparently, wants to demonstrate the ability to learn from examples from history and that is why it refers to the Geneva Conventions. The G7 countries also spoke out in favor of the need to approve universal norms of behavior in cyberspace at the state level. The decision to combat legal online nihilism is commendable, but the same history proves that international agreements alone will not protect against cybercrime. We will have the greatest chance of success if market participants voluntarily introduce certain standards for the industry.

Microsoft has outlined “three key components of international cooperation to prevent online warfare:”

1) States that support the Digital Geneva Convention must refuse to conduct and sanction cyberattacks;

2) states will sign a Technology Agreement, which will approve the basis of behavior to protect citizens on the Internet;

3) the investigation of attacks and the identification of subjects violating the agreements will be entrusted to a neutral non-governmental organization, which, however, will not have the authority to enforce the rules.

"All of these components are necessary for consumers to trust technology," Microsoft is convinced.

In addition to the Geneva Conventions on the Conduct of War, the International Telegraph Union (ITU) also served as a model for telecommunications regulation, which began operating in the 1860s and was responsible for electrical telegraph communication between countries. With the

development of radio, satellite communications, television and the Internet, new agencies emerged to regulate the rules of communication.

Heidi Tvorek, having studied the impact of regulatory experience, singled out 2 main facts: 1) countries managed to agree on and adhere to only technical standards, but not content regulation standards; 2) voluntary agreements of IT companies are vital for the successful protection of citizens, and experience shows that this is possible… (that commercial radio companies, when acting together, can significantly influence international agreements) (Tworek, 2017).

Today it is difficult to imagine how the radio network and telecommunications in general would have developed if the scheme proposed by the Europeans had been adopted at the international level. But the approved parameters allowed radio communications to develop freely, and the airwaves became an indispensable companion in the lives of millions of people around the world.

Governments already have a long tradition of agreeing on technological requirements and standards that facilitate the integration and spread of communications infrastructure. By 1901, the ITU had approved telegraph code standards for over 2 million terms in different languages. However, when it comes to more abstract concepts such as freedom of expression and the free dissemination of information, it is more difficult for states to reach agreement. International agreements reached in Atlantic City (USA) in 1947 still exempt communication transmitters from the obligation to broadcast messages classified as threatening national security, public order or public morals. This means that any data can be censored if it is deemed dangerous, according to the above characteristics.

To be successful, a digital international convention must focus on technological aspects, establish real tools to prevent criminal interference in the operation of systems. If the document deals with vague concepts that are defined in each country in their own way, such a project will be ineffective. Just as 90 years ago, industry representatives proposed that the government establish standards for the use of communications, today IT companies must join forces to define digital security standards.

Of the points proposed by Microsoft, the Technology Agreement is the one that resonates most with the general public. Trust in the project's authors is essential for society to take the initiative seriously. A recent Pew study Research has found that Americans believe the corporate IT sector is more competent at protecting personal data and countering foreign hackers than government agencies. So, international security standards from companies will have user support, but an initiative from law enforcement or government officials will fail. Therefore, for success, leading companies must participate in the creation of the future Technology Agreement (Tworek, 2017).

Based on the above principles, in the spring of 2018, about thirty companies, including Microsoft, Facebook, and Intel, agreed to “core principles.” In particular, the signatories pledged not to help any government, not even the US government, carry out attacks against “innocent civilians and businesses anywhere in the world.” The companies also promised to help any country that falls victim to such attacks, regardless of whether they are carried out with “criminal or geopolitical” intentions.

“The case has been opened,” D. Sanger noted, “but this is not enough, because no Chinese, Russian or Iranian company signed the initial agreement,” he further notes. Similarly, some giants of the technology world, including Google and Amazon, are still torn between the desire to cooperate with the US Armed Forces and the reluctance to outrage their customers. The wording of the agreement left room for maneuver: the companies could join attacks against terrorist groups or governments that oppress their citizens. There was also no mention of support for democracy

or human rights, which means that if Apple eventually joins the agreement, it will not be punished for its decision to give in to Beijing and store data about Chinese users on servers located in China (Sanger, 2022)."

Brad Smith emphasizes, "we need to enact laws that require respect for certain principles around the world. In particular, governments must refrain from attacking critical infrastructure in peacetime as well as in times of war, and even when it is unclear what time we are living in[49][1]."

According to David Sanger, "… over time, these principles have made the world more humane. … Now, as after the invention of the airplane and the atomic bomb, it would be appropriate to think more broadly about where to look for safety.

It is clear that this is not an endless cyber arms race, where victories over enemies are fleeting, but the ultimate goal is to overcome the defenses of another country or disable its enterprises. We must remember that we created these technologies to enrich our society and our lives, not to have another way to plunge the enemy into darkness. The good news is that we created these technologies, so we can control them, if we only focus on how to cope with the risks. It has worked in other dimensions, so it can work in cyberspace," he encourages (Sanger, 2022).

Conclusions

Addressing the use of AI in hybrid warfare cannot be effective without addressing cybersecurity issues in general (at least as long as we consider AI as "technologies" and not "entities").

From these positions, we will formulate the conclusions for our section.

The use of AI and cyberattacks in hybrid wars calls into question the viability of the idea of self-governance of the IT sphere at the current stage of its development. Perhaps this will become a reality after artificial intelligence becomes stronger than human intelligence and forms its ideal virtual world.

Until then, we should note the injustice of the accusations about the ineffectiveness of legal regulation of social networks. As V. Gorbulin noted, "With what some people think are "ridiculous" countermeasures, these steps of Ukraine bring quite tangible losses to the aggressor, forcing him to lose his rhythm, to be distracted by more and more new inconveniences. The ban on social networks is a great example. Undoubtedly, with certain technical skills, one can try to circumvent the ban (by the way, bypass mechanisms are often provided by structures close to the FSS (Federal Security Service)). But it is important, for example, to note that immediately after the ban on Yandex's work in Ukraine, its shares fell by 3.3%. And this is unpaid taxes to the Russian budget, and therefore — a little less money for the Russian defense industry or financing separatists. Not to mention the sharp reduction in the target audience for latent " brainwashing" (Horbulin, 2017).

Assessing the situation in this area from these perspectives, we note that solving the problem of cyber threats (including those related to the use of AI) requires taking into account two aspects: legislative and law enforcement.

As for the first of them, there are already Laws of Ukraine "On the Protection of Information in Information and Communication Systems" (Verkhovna Rada of Ukraine, 1994), "On the Basic Principles of Ensuring Cybersecurity in Ukraine." In addition, cybersecurity experts, noting some progress in the state's attitude towards cybersecurity (a cybersecurity strategy has been developed , there is a coordination center under the National Security and Defense Council, etc.), speak of the need to adopt a law on the responsibility of hackers, who now feel safe (Belogorsky, 2016).

The full-scale war in Ukraine, violations of all norms of international law, have led to the fact that international norms simply ceased to apply. As an example, the International Committee of the Red Cross (ICRC) has published rules for civilian hackers involved in conflicts for the first time. The watchdog warns that since Russia's invasion of Ukraine, an unprecedented number of people have joined patriotic cyber groups. The new rules include a ban on attacks on hospitals, the uncontrolled spread of hacking tools, and threats that terrorize the civilian population. The Ukrainian IT Army, which has 160,000 members on Telegram, has also attacked state services such as railways and banks.

Its spokesman told BBC News that they had not yet decided whether to apply ICRC rules. The group already prohibits attacks on medical targets – but the impact on civilians is inevitable because "following the rules could put one side at a disadvantage".

Meanwhile, a representative of the group Anonymous Sudan, which in recent months has begun attacking technology companies and government agencies it sees as critical of Sudan or Islam, told BBC News that the new rules were "unsustainable and that their violation in the interests of the group is inevitable."

And one of the senior members of the Anonymous group told BBC News that they had "always worked on the basis of several principles, including the rules outlined by the ICRC," but had now lost faith in the organization and would not abide by its new rules (Tidy, n.d.) [54].[1]

In the current situation, as noted by Yegor Aushev, CEO of CyberUnit Technologies, Ukraine should become a center of resistance, as it gained vast experience during the war and should use it not only to increase its cyber resilience, but also to build world-renowned expertise.

Since the beginning of the war, our state has suffered numerous cyberattacks aimed at infrastructure entities of various types of ownership - state, corporate, private, etc. Last year, CERT-UA processed 2,543 cyberincidents - this is 15.9% more than in 2022, when the Russian invasion of Ukraine was accompanied by a huge number of attacks. Most of all, hostile hackers attacked the government and government organizations, local authorities, and the security and defense sector. Numerous cyberattacks on financial institutions, critical infrastructure, the energy sector, and telecommunications have become the norm and continue to harm the state and private business.

Ukraine recognizes cybersecurity threats as an important aspect of national security. The introduction of effective mechanisms for protection against cyberattacks, increasing people's cyber awareness, and effective coordination of all cybersecurity actors are priorities.

According to Aushev, protection is needed not only at the local level, but also at the global level, where it is necessary to create global joint response groups at the interstate level, since the confrontation in cyberspace now goes beyond national borders. Countries with developed cyberwarfare programs, such as Russia, North Korea and Iran, can finance and use hacker groups as a tool to influence their strategic goals, as well as to steal funds and personal data, blackmail, etc.

In this context of global confrontation, Ukraine has every chance of becoming a center of resistance that will unite Western countries into a cyber coalition to confront threats in cyberspace, by developing joint effective cyber deterrence tools and changing the world's cyber defense policy. And the only thing that is needed for this is the awareness of the importance of all participants in the process and the unification around its drivers, which today are representatives of the Ukrainian professional community, the state and business (Ukraine should become a center of resistance: How to use the uniqueness of our experience in overcoming cyberattacks, 2024).

REFERENCES

1. Belogorsky, N. (2016). Silicon mountains and valleys. *New Time Countries*, (48), 56–58.
2. Boyko, D., & Horodyskyi, I. (2024, January 12). Artificial intelligence in the defense sector: Regulatory challenges. *DC.org.ua*. Retrieved from https://dc.org.ua/news/shtuchnyy-intelekt-u-sferi-oborony-vyklyky-regulyuvannya
3. Bratko, A., Zaharchuk, D., & Zolka, V. (2021). Hybrid warfare – a threat to the national security of the state. *Revista de Estudios en Seguridad Internacional*, 7(1), 147–160. Retrieved from http://www.seguridadinternacional.es/revista/
4. Clausewitz, C. v. (2018). The nature of war (R. Gerasimov, Trans.). Kharkiv: Vivat.
5. Danyk, Y., Malyarchuk, T., & Briggs, C. (2017). Hybrid war: Hi-tech, information, and cyber conflicts. *Connections: QJ, 16,* 5–27. Retrieved from http://connections-qj.org/ru/article/gibridnaya-voyna-hay-tek-informacionnye-i-kiberkonflikty
6. Dolzhenko, O. O. (2018). Conceptual principles and conceptual and categorical definition of "hybrid war" in the context of threats to the national security of Ukraine. *Gileya: Scientific Bulletin*, 128, 315–317.
7. Goodman, J., & Koreniuk, M. (2023, June 1). *How social media is deleting evidence of Russian war crimes in Ukraine: BBC investigation*. BBC News. https://www.bbc.com/news/how-social-media-is-removing-evidence-of-russian-war-crimes-in-ukraine
8. Gorbulin, V. P. (2010). *Without the right to repent*. Kharkiv: Folio.
9. Gorbulin, V. P. (2017). Hybrid world: Ukrainian front: Monograph (pp. 9–10). Kharkiv: Folio.
10. Gumenyuk, V. (2022). Russia's hybrid war against Ukraine as a threat to universal collective security. In *Deoccupation. Legal front: Materials of the International Expert Round Table (Kyiv, March 18, 2022)* (pp. 23–25). State University of Trade and Economics, Ukrainian Association of Comparative Law, Ukrainian Association of International Law, Association for the Reintegration of Crimea; Compiled and Scientific Editor O. V. Kresin. Kyiv: State University of Trade and Economics.
11. Hoffman, F. G. (2009). Hybrid warfare and challenges. Joint Force Quarterly, 52.
12. Horbulin, V. (2017, June 24–30). "Values" society and "hybrid world": The crisis of the protection model. *Dzerkalo Tyzhnia*, (24).
13. International Institute for Strategic Studies. (2015). *The Military Balance 2015*. https://archive.org/details/militarybalance20000unse_d0k7
14. Kharytonov, E. O., & Kharytonova, O. I. (2017). Problems of legal regulation in the IT sphere in the conditions of information war. In *Problems of restoring the constitutional order in Ukraine: Materials of the international scientific and practical conference* (pp. 159–163). Kyiv: Tavrichesky National University
15. Kharytonov, E. O., & Kharytonova, O. I. (2019). Problems of compensation for property damage in the field of information technology use. In *Memories of a person, a scientist, a civilian* (pp. 275–287). Kyiv: ArtEk.
16. Kharytonov, E., Kharytonova, O., Tolmachevska, Y., Fasii, B., & Tkalych, M. (2017). Information security and means of its legal support. *Amazonia Investiga*, 8(19), 255–265
17. Khorunzhy, G. (2022). Russia's war against Ukraine: Russian propaganda as a component of the "hybrid war." Ukrainian Scientific Journal "Education of the Region". Retrieved from https://uu.edu.ua/articles/russias-war-against-ukraine-russian-propaganda-as-a-component-of-the-hybrid-war/
18. Kostenko, O., Jaynes, T., Zhuravlev, D., Dniprov, O., & Usenko, Y. (2023). Problems of using autonomous military AI against Russia's military aggression against Ukraine. *Baltic Journal of Legal and Social Sciences*, 4, 131–145. https://doi.org/10.30525/2592-8813-2022-4-16
19. Lyudva, A., & Avdeeva, T. (2023, October 9). How "clear" is the legality of Clearview AI in Ukraine? *Digital Security Laboratory*. Retrieved from https://www.dslua.org
20. Magda, E. (2014). Hybridna war: The essence and structure of the phenomenon. *International Relations, Part "Political Sciences"*, 4. Retrieved from http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489/2220
21. Magda, E. (2015). *Hybrid war: Survive and win*. Kharkiv: Viva
22. McMaster, H. (2023). *Battlefields: The struggle for the protection of the free world* (N. Koval, Trans.). Kyiv: Our Format.
23. Meechem, D., & Gak, M. (2022, March 30). *Is facial recognition technology bringing killer robots closer to Ukraine's war? Clearview AI offers Ukraine its controversial technology to identify enemy soldiers as autonomous killing machines gain momentum.* OpenDemocracy. https://www.opendemocracy.net/en/ukrainian-military-receives-artificial-intelligence-for-facial-recognition-we-are-worried/
24. Ministry of Digital Transformation of Ukraine. (2024). *White Paper on AI Regulation in Ukraine: Vision of the Ministry of Digital Affairs. Version for Consultations*. https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf

25. Ministry of Digital Transformation of Ukraine. (2024, June 26). Regulation of artificial intelligence in Ukraine: The Ministry of Digital Transformation presents the White Book. Retrieved from https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuie-bilu-knyhu
26. Nesenyuk, A. (2024, June 27). *The Ministry of Digital Affairs proposes to adopt an analogue of the European AI Act and create a regulatory body. What else does the "White Paper" on AI regulation provide for?* Forbes Ukraine. https://forbes.ua/innovations/mintsifri-proponue-priynyati-zakon-analog-evropeyskomu-ai-act-ta-stvoriti-regulyatorniy-organ-shcho-shche-peredbachae-bila-kniga-regulyuvannya-shi-27062024-22020
27. Osiichuk, M., & Shepotylo, O. (2020). Conflict and well-being of civilians: The case of the Russian-Ukrainian hybrid war. *Economic Systems*, 44(1), 1–31. Retrieved from https://doi.org/10.1016/j.ecosys.2020.01.002
28. Pavlenko, Zh., & Antonov, A. (2022). Hybrid war: Analysis of definitions and concepts. *Bulletin National Legal University Named After Yaroslav the Wise*, 2(53), 106–119.
29. Pocheptsov, G. (2015). Hybrid war: Informational component. *Media Sapiens*. Retrieved from http://osvita.mediasapiens.ua/trends/1411978127/hybrid_war_information_warehouse/
30. Pocheptsov, G. (2015, November 1). From the history concept of hybrid wars in the USA and Russia. *Media Sapiens*. Retrieved from https://ms.detector.media/mediaanalitika/post/14619/2015-11-01-z-istorii-poniattya-gibrydnoi-viyny-v-ssha-i-rosii/
31. Popova, T. V., & Lipkan, V. A. (2016). *Strategic communications: Dictionary*. Kyiv.: FOP O. S. Lipkan.
32. Prognimak, K. (2017, May 13). *Microsoft is right: We need a digital Geneva Convention.* Imena.ua. https://www.imena.ua/blog/microsoft-digital-geneva-convention/
33. Puvelde, D. (2015). Hybrid war - does it exist at all? NATO Review. Retrieved from https://www.nato.int/docu/review/ru/articles/2015/05/07/gibridnaya-vojnasushchestvuet-li-ona-voobshche/index.html
34. Sanger, D. E. (2022). *The perfect weapon: War, sabotage, and fear in the cyber age* (p. 413). Lviv: Astrolabia Publishing House.
35. Svitova, G. (2017). *Hybrid war: Ukrainian front: Monograph* (V. P. Gorbulin, Ed.). Kharkiv: Folio
36. Syrotenko, A. M. (Ed.). (2020). *Countering "hybrid" aggression: Experience Ukraine: Monograph*. Kyiv: Ivan NUOU Chernyakhovsky. Sokolov, B. (2021, November 11). Hybrid war in action. *Day*. Retrieved from https://day.kyiv.ua/uk/article/den-planety/gibrydna-viyna-v-diyi
37. Taranenko, M. (2016). Hybrid war in Ukraine: History and modernity. *Bulletin of NTUU "KPI"*. Political Science, Sociology, Law, 3/4(31/32), 190–200. Retrieved from https://ela.kpi.ua/bitstream/123456789/25058/1/VPSP_2016-3-4_190-200.pdf
38. Tidy, J. (n.d.). *World's first rules for hackers introduced: Will Ukrainians follow them during war?* BBC News Ukraine. https://www.bbc.com/ukrainian/features-65132086
39. Tkachuk, I., Shynkarenko, R., Tokovenko, O., Svorak, S., & Lavoryk, A. (2021). Hybrid threats and the transformation of the state political institute: A neo-institutional approach. *Journal of Interdisciplinary Research*, 11/01-XVI. Retrieved from http://www.magnanimitas.cz/ADALTA/110116/papers/A_05.pdf
40. Tworek, H. (2017, May). *Microsoft is right: We need a digital Geneva Convention.* Wired. https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/
41. *Ukraine should become a center of resistance: How to use the uniqueness of our experience in overcoming cyberattacks.* (2024, March 16). https://biz.nv.ua/ukr/experts/novi-kiberataki-vid-rf-yak-reaguvati-ukrajini-ta-do-chogo-nam-vsim-gotuvatisya-50401148.html
42. Verkhovna Rada of Ukraine. (1994, July 5). *On the protection of information in information and telecommunication systems: Law of Ukraine No. 80/94-BP*. https://zakon.rada.gov.ua/laws/show/80/94-вр
43. Wang, F. (2024, May 15). *How artificial intelligence turned a Ukrainian blogger into a Russian propagandist*. BBC News. https://www.bbc.com/news/how-artificial-intelligence-turned-a-ukrainian-blogger-into-a-russian-propagandist
44. Yavorska, G. M. (2016). Hybridna war as a discursive construct. Strategic Priorities, 4(41), 41–48. Retrieved from http://ippi.org.ua/sites/default/files/yavorskaya.pdf
45. Yavorska, G. M., & Yizhak, O. I. (2017). *Phenomenon hybrid World War II hybrid war: Ukrainian front* (V. P. Gorbulin, Ed.). Kharkiv: Folio.
46. Zhovtenko, T. (2022, November 3). Hybrid war: Anatomy of instrumentation and victory. *Dif.org.ua*. Retrieved from https://dif.org.ua/article/gibridna-viyna-anatomiya-instrumentariyu-y-peremogi