วารสารวิชาการผลประโยชน์แห่งชาติ
Thai Journal of National Interest
ISSN (Online): 3088-2729

DOI: https://doi.org/10.14456/ni.2025.19

Key methods of conducting hybrid warfare in the modern information space. Approaches to information technologies in relation to hybrid warfare

Yurii I. Kohut

E-mail: office@sidcon.com.ua
Ph.D. in Legal Sciences, Lead Auditor in Information Security Management Systems,
Director General of "SIDCON" International Consulting Company (Kyiv, Ukraine)

ABSTRACT

In the contemporary landscape of global conflicts, propaganda and disinformation have emerged as powerful tools within hybrid warfare, aimed at influencing public perception, destabilizing societies, and undermining adversaries. Propaganda can manifest in various forms, ranging from overt political messaging to subtle sociological influences disguised as private opinions. This complexity necessitates a clear understanding of the strategies and tactics employed in information warfare. Notably, the "4D" strategy—comprising denial, distortion, distraction, and dismay—provides a conceptual framework to analyze how propaganda functions and how it can be countered. Complementing this, the "4f" tactics encapsulate the common methods of fabricating news, media, experts, and events to mislead and manipulate audiences. This article aims to examine these strategies, uncover their psychological underpinnings, and explore their application in the digital age, particularly through social media platforms, which have become a significant battleground for information influence.

KEYWORDS: propaganda, disinformation, hybrid warfare, psychological warfare, information operations, 4D strategy, 4f tactics, fake news, information manipulation, social media influence

Received : 27/08/2025
Revised : 28/10/2025
Accepted: 17/12/2025

1. Formulation of the problem. Propaganda and disinformation have become central instruments in contemporary hybrid warfare, shaping public opinion, destabilizing societies, and undermining adversaries without direct military confrontation. These tools, leveraging psychological manipulation and media influence, pose serious threats to national security, democratic institutions, and social cohesion worldwide. In the context of modern conflicts, especially illustrated by recent geopolitical tensions, propaganda operates in multiple forms—political, explicit, sociological, and invisible—often blending fact and fiction to create persuasive but misleading narratives.

This article examines key frameworks used to understand and counter propaganda, focusing on the "4D" strategy—denial, distortion, distraction, and dismay—and the "4f" disinformation tactics, which include fake news, fake media, fake experts, and fake events. By analyzing the psychological mechanisms exploited by these approaches and their application through traditional and social media, the article reveals how information warfare leverages emotional appeals, cognitive biases, and network effects to manipulate target audiences.

Existing literature addresses elements of propaganda and information operations, yet this article distinguishes itself by integrating both theoretical models and practical insights from recent hybrid conflicts. Unlike broader cybersecurity or media studies perspectives, it offers a focused analysis of propaganda's operational tactics and psychological underpinnings within the evolving information environment. It also highlights the critical role of social media platforms as amplifiers of disinformation and the challenges of detecting and countering sophisticated influence campaigns.

By bridging academic theory and real-world case studies, this article provides valuable guidance for security experts, policymakers, and civil society stakeholders aiming to develop effective countermeasures against information warfare. Its comprehensive approach to understanding propaganda's multifaceted nature and its strategic deployment in hybrid conflicts makes it a significant contribution to the field of information security and psychological operations.

2. Analysis of recent research and publications. Recent scholarship on information warfare highlights the growing centrality of propaganda and disinformation in modern conflicts. Authors such as Thomas Rid (Rid, 2016) and Christopher Paul (Paul, 2011) emphasize that hybrid warfare increasingly relies on manipulating perceptions rather than direct military engagement. Studies in Journal of Information Warfare and International Security demonstrate how state and non-state actors employ information operations to destabilize adversaries and weaken social cohesion.

At the same time, research by NATO StratCom (NATO StratCom, 2021), the European External Action Service (European External Action Service, 2022), and various cybersecurity institutes has mapped specific disinformation campaigns, particularly in the context of the Russia–Ukraine conflict.

These analyses reveal the use of coordinated inauthentic behavior, fake media outlets, and digital amplification strategies that blend fact and fiction. The findings underscore the role of social media platforms as accelerators of propaganda, complicating efforts to trace origins and assess impact. However, while much of the literature addresses either strategic frameworks or technical detection, fewer works provide integrated analyses combining psychological mechanisms with practical countermeasures. This article seeks to bridge that gap by connecting theoretical models, such as the "4D" and "4f" frameworks, with recent empirical evidence. In doing so, it contributes to a more holistic understanding of how disinformation operates within the broader spectrum of hybrid warfare.

3. The purpose of the article. The purpose of this article is to analyze the role of propaganda and disinformation as key instruments of contemporary hybrid warfare. It examines psychological mechanisms and operational tactics, including the "4D" strategy (denial, distortion, distraction, dismay) and the "4f" tactics (fake news, fake media, fake experts, fake events). By bridging theoretical models with real-world case studies, the article highlights how information operations exploit cognitive biases and social media amplification. Ultimately, it aims to provide policymakers, security experts, and civil society with practical insights for developing effective countermeasures against information warfare.

4. Presenting main material. Modern hybrid warfare is not just a new stage in the development of the art of war and the use of modern hybrid technologies for destruction and domination; it takes place in a fundamentally new civilizational, cultural, and social environment (Ruschenko & Pavlenko, 2015), and therefore it is advisable to focus on the consideration of the basic methods associated with conducting hybrid warfare in the modern information space and the approaches to information technologies applied by the aggressor state in hybrid warfare. The development of science and technics, information, and communication technologies opens up virtually unlimited possibilities of hidden non-violent manipulative influence on a person, society, and the state. It is important to understand that hybrid warfare is not only a military conflict but also a war of ideological constructors.

The vast majority of experts on hybrid warfare agree that the leading component of hybrid warfare is information warfare. Thus, the constant development of the mass communication system leads to the erasure of borders and wide opportunities for manipulative influence on the consciousness of the population of the rival state with the imposition of its own ideas of the aggressor state (Feskov, 2016). Throughout the hybrid warfare, importance is paid to the information struggle, where the main actors are the media and the Internet. At the same time, the elements of information warfare include: obtaining intelligence information, disinformation, psychological operations, cyber-attacks on information infrastructure, infection with computer viruses of enemy computer networks, as well as appropriate counteraction measures to protect their own information resources (Trebin, 2014).Today, in the course of hybrid warfare, the scope and tasks of international information warfare are significantly expanded, specialized organized formations of information and psychological struggle are created, and even cyber forces are created, capable of coordinating and centrally conducting information operations and campaigns (Lisetsky et al., 2021). On September 2, 2016, the Czech counterintelligence service BIS reported that the Russian special services were waging an information warfare in the Czech Republic, trying to create a network of puppet cells and propagandists on the territory of the Czech Republic, which the Russian Federation could use to destabilize the country (Razumkov Centre, 2016). In its annual report, BIS indicated that Russia seeks to influence the Czech media by covering the role of the Russian Federation in the Ukrainian and Syrian conflicts. And on November 29, 2016, the head of German intelligence, BND, Bruno Kahl, said that hackers and trolls from Russia influenced the US elections; their target was the German elections in 2017. In particular, he noted that “Europe is in the focus of such subversive actions, and Germany, especially” (Razumkov Centre, 2016). It should be noted that the term “information warfare” was used one of the first by Thomas P. Rona in the analytical report for the Boeing Company on “Weapons Systems and Information Warfare” in 1976 (Feskov, 2016). From that moment on, the understanding *that information can be a weapon* begins to be formulated. An avalanche-like flow of information (and disinformation) can harm any state (up to a coup d’etat and overthrow of the power).The most well-known definition of information wars is: “This is a type of conflict in which the tasks of the opposing parties are to protect their own information and information systems, manipulate the enemy’s information or distort it, as well as limit the ability of the opposing party to access and process information” (Aslam et al., 2020).

Also, most often, ***information warfare is understood as an interstate confrontation in the information sphere, which is conducted with the use of information weapons and means of information and psychological influence.*** Such a confrontation can occur both in wartime and in peacetime. In this case, the object of influence becomes another state, and the influence is carried out on the population of this state and on world public opinion. The world has seen many examples of information wars. Now, against the background of Russia’s military operations in Ukraine, Russia is actively conducting an information war aimed at the population of Ukraine, primarily in the occupied territories.

The purpose of information warfare is to manage the process of changing people’s consciousness, their worldview, and their attitude toward society and the state (Loishyn et al., 2021). At the same time, the negative result of the information war is the loss of the target state’s own will by the population and its sovereignty by the state. This has always been the goal of any conqueror, but now the same can be achieved in a “soft” way (even the term “soft power” has introduced by the American political scientist, Joseph S. Nye, Jr. But "soft" tools in some cases can be more dangerous than "hard" ones because the victim of soft coercion may not be aware of the deception and may see a negative result for himself only when it is no longer possible to change events. At the same time, such information weapons have a massive capacity for destruction.

There are two leading directions of influence for information weapons (Loishyn et al., 2021):

1) influence on the enemy's information tools and systems. The first direction is also called "***cyber warfare***," when the technical equipment and software systems of the enemy state are subjected to cyber-attacks.

2) ***influence on people's consciousness***. The second direction is the old methods of propaganda and agitation, counter-propaganda and counter-propaganda, which have recently been greatly improved in terms of sophistication and mass influence on people's minds.

At the present stage, information warfare appears in the form of a network-centric war, the task of which is the so-called ***identity***, that is, the complete destruction of the national-state-civil identity of the rival country. Identification consists of convincing the majority of the people of their country, or even a part of the enemy's people, of the enemy's evil intentions regarding their actions (Doroshkevich, 2015). The object of such information warfare is mass and individual consciousness. It should be noted that information influence can be carried out both against the background of information noise and in conditions of an information vacuum (Doroshkevich, 2015).

The basic tools of hybrid warfare include various information means (Zdioruk & Palinchak, 2022):

- tools for military-political disorientation of the enemy. Thus, the development of global communication networks, as well as digital media technologies, allows cyberspace to carry out a negative information and psychological impact on the personnel of the State Defense Forces to undermine the moral and psychological state, which, in turn, affects the achieved level of state defense capability (Sirotenko, 2020).
- misinformation about one's own information resources;
- actions aimed at damaging or blocking data transmission channels in order to disorient and disorganize;
- creating an atmosphere of tension in the society of the target state from the constant expectation of strikes and a massive offensive along the entire front line;

- influence on the mass consciousness of the population of the rival state in order to demoralize and spread panic.

The key methods forp conducting information and psychological warfare and carrying out destructive information influences include: propaganda, spreading rumors, provocations, disinformation, manipulation, suggestion, physical blocking of communication and telecommunications systems, psychological and psychotropic pressure, diversification of public consciousness (public opinion), intimidation, etc. (Giegerich, 2016). For example, the purpose of propaganda by the aggressor state is to incite social hostility, escalate social conflicts, and escalate disputes in the society of the target state.

Disinformation (or misinformation) is one of the ways to manipulate information. This is misleading someone by providing incomplete or unnecessary information or distorting some of the information or context. The goal of such influence is always the same – the opponent must act as it is necessary for the manipulator (Hrynchenko & Molodetska -Hrynchuk, 2018). The action of the object to which disinformation is directed may consist in making the right decision for the manipulator or in refusing to make a decision that is unprofitable for the manipulator.

Disorientation and falsification are types of misinformation that can mislead a person**.**

Disinformation and manipulation of information is achieved through (Vassileva & Zwilling, 2018):

- *biased presentation of facts*—biased coverage of facts or other information about events using specially selected truthful data. Mainly with the help of this method, specially formed information is fed in a dosed manner, to an ever-increasing voltage;
- *misinformation "from the opposite"*—occurs by providing truthful information in a distorted form or in a situation where it is perceived by the object of influence as untrue. As a result, there is a situation when the object of influence actually knows truthful information about the intentions or specific actions of the opposite party, but perceives it inadequately, is not ready to resist negative influence;
- *terminological "mining"*—consists in distorting the primary correct essence of fundamentally important, basic terms and interpretations of a general ideological and operational-applied nature;
- *"Gray" disinformation* involves the use of the synthesis of truthful information with disinformation;
- *"Black" misinformation* is the use of mostly false information.

Diversification of public opinion aims to disperse the attention of the ruling elite of the state to various artificially emphasized problems and, thereby, distract it from solving the priority tasks of socio-political and economic development in order to ensure the normal functioning of society and the state Aslam et al., 2020).

- ***Forms of diversification of public opinion are*** (Gorban, 2015): destabilization of the situation in the state or its individual regions;
- intensification of the campaign against the political course of the ruling elite of the state and its individual leaders by various international institutions;
- initiating anti-dumping campaigns and other scandalous lawsuits;
- application of international sanctions for other reasons.

Psychological pressure is also a common method of influencing people's minds. Its use provides for blackmail, threats of persecution, repression, murder, etc., bringing to the object information about real or far-fetched threats and dangers, committing terrorist acts, and sabotage (Giegerich, 2016). A common form of psychological pressure is ***telephone terrorism***, that is, calls with information about the alleged mining of public places, railway stations, fraudulent actions against citizens of a rival state in order to cause these citizens dissatisfaction with the actions of the authorities and management of this state, and so on.

The key technologies of psychological pressure include (Zdioruk & Palinchak, 2022) : fraud, bluffing, political games and hoaxes, manipulative actions, provocations, psychological and covert operations, political games and advertising campaigns, disinformation, rumors, etc.

The spread of rumors also acts as a special technology of information warfare. Thus, the lack of information is immediately compensated by rumors: the vacuum of information in official sources leads to the instant emergence of rumors in unofficial information channels.

At the same time, ***the most common method of information and psychological warfare is propaganda*** (lat. propaganda, literally "subject to dissemination (faith)," from Lat. propago, "I spread"), which involves spreading among the masses and explaining to the population any beliefs, ideas, teachings, knowledge, and appeals to the feelings of the mass audience, repeating the same type of attitudes constantly and repeatedly (Nikolic, 2018; Fisenko, 2016). In other words, propaganda is a form of communication aimed at spreading in society a worldview, theory, statement, facts, arguments, rumors, and other information to influence public opinion in favor of a certain common cause or public position (Krikun & Baulina, 2022). Propaganda can be classified according to the source and nature of the message and have a certain color and direction depending on the sources of information and purpose

(Hrynchenko,2018).

To counteract negative propaganda and manipulation, you need to understand how the processes of structureless management in society take place, know the methods of processing information to search for and select reliable data, and know methods of countering negative forms of information influence on society.

Thus, **the main methods of propaganda include**: the formation in the mass consciousness of the image of the victim by the person involved, who is actually a criminal; shifting responsibility and attributing their own crimes to the opponent; ignoring the facts; and branding all those who do not agree with the propaganda (Vassileva & Zwilling, 2018). Thus, propaganda is an effective means of manipulating human consciousness.

Methods of enemy propaganda are outright lies, distortion of facts, insinuations, slander, information sabotage, provocations, distortion of historical events, etc. (Razumkov Centre, 2016).

For the first time, the role of propaganda was analyzed by the American political scientist Harold Dwight Lasswell, who defined it as a special type of information and psychological weapon that affects the moral (mental) state of the enemy (Hryshchuk & Tagarev, 2018).

Among the principal goals of propaganda, Harold Dwight Lasswell defines (Nikolic, 2018):

- inciting hatred towards the enemy;
- maintain friendly relations with allies;
- maintaining good relations with neutral countries and, if possible, trying to cooperate with them;
- demoralizing the enemy.

Scientists distinguish between ***vertical*** (the classic version of propaganda: the information flow goes from top to bottom with a passive reaction of the audience) and ***horizontal*** (implemented in a certain social group and does not go from above; in this situation, all participants are equal, there is no leader among them, and therefore information is perceived with maximum trust) ***propaganda*** (Vassileva & Zwilling, 2018). Modern propaganda is horizontal; it "mimics either science, education, or the opinion of a particular person, but for some reason it is broadcast to millions" (Pocheptsov, 2016). That is, the reference to propaganda has been fundamentally erased from propaganda today.

Propaganda can also be "political," "explicit" (promoted on behalf of the state and imposing a certain ideology), "sociological," or "invisible" (presented under the guise of private opinions and aimed at forming a certain worldview and values) (Hetmanchuk & Zazulyak,2019).

Theorists and practitioners of countering propaganda distinguish the so-called "4D" strategy: dismissing, distorting, distracting, and dismaying (denial, distortion, disorientation, and intimidation), as well as the ***formula of the disinformation campaign "4f-tactics,"*** which marks: fake news, fake media, fake experts, and fake events (fake news, fake media, fake experts, and fake events) (Krikun& Baulina2022). The essence of the "4D strategy" is to use the features of communication psychology in social groups. In its original form, this strategy was outlined by Ben Nimmo, a co-researcher of the Central Institute for European Policy, in a publication on the Institute's resources and reprinted by many other sites in translations (StopFake, 2025).

The "4D strategy" of propaganda contains the following links (Hrynchenko & Molodetska -Hrynchuk, 2018):

1) ***The rejection of the charge*** is the first link in the strategy. This approach of the aggressor state to negative reports or comments is to refute them either by denying statements on the ground (among consumers of information) or by slandering the person who voices them (the source of information), questioning his authority and the significance of the information itself.

2) ***Information distortion*** consists of the fact that the content of information can change in the process of its transmission through various channels from the source to the consumer. The degree of distortion is directly proportional to the number of channels and transmission links through which the message passes: the more participants gain access to this or that information and transmit it to other people, the more the final version of the information differs from the original one. This is the most common phenomenon in modern mass media. It is caused by a number of closely related reasons, ranging from a decrease in the quality of an information product due to a decrease in funding while reducing the time for preparing news content in the face of fierce competition from manufacturers to increased censorship by state bodies (Hetmanchuk & Zazulyak ,2019).

The reasons for information distortion may be as follows (Hrynchenko & Molodetska-Hrynchuk,2018):

- translation problems and polysemy create the possibility of different interpretations of the same message;
- differences in the level of education, intellectual development, and professionalism;
- non completeness of information due to restricted access to it or deliberate submission not in full, which leads to speculation and the addition of unverified facts and assumptions;
- insufficient level of qualification of the employee presenting information;

- emotional stress;
- prejudice against the persons or phenomena referred to in the message.

3) ***Disorientation of the recipient of information***—answering a question with another, and logically incorrect question, or providing an excessive amount of information that is not relevant to the case, true or false, in order to distract attention from the essence of the issue under consideration.

4) ***Intimidation***—intimidation of the enemy by the threat of failure of his plans, spreading anxiety among the opponent's supporters, using internal contradictions and opposition within the state that is the object of aggression. Thus, in recent years, intimidation as a method of Interstate Blackmail has acquired significant proportions.

They also distinguish the so-called "4f tactics" of disinformation (Hrynchenko & Molodetska-Hrynchuk,2018):

1) ***Fake news*** is an informational hoax — the deliberate dissemination of untruths or half-truths in social media and traditional media in order to mislead a person for financial or political gain. Fake news is created, often using catchy headlines or completely fabricated published materials to increase readership and citation. The main reason for using such methods in normal circumstances is the profit from the customer of the material or from cheating clicks on the resource, with subsequent profit from the placement of advertising materials. During the election race, the use of fake news is usually widespread. And within the framework of the information war, fake news is used as a kind of "weapon" with which the opposing sides are trying to gain an advantage.

2) ***Fake media resources***: information resources created for the purpose of spreading false information on a certain topic.

Characteristic features of fake media resources are (Kyrychenko, 2023):

- registration and placement of hosting services outside the region they are supposedly focused on;
- specifying contact details that are not typical for the region;
- atypical speech expressions and alien behavioral patterns in the presentation of the material;
- availability of multiple resources that are completely similar in design, theme, and content;
- content that is not created but copied from news aggregators;
- low popularity among the population of the region.

3) ***Fake experts***, fictitious or false authoritative specialists from certain branches of human activity, whose opinion is designed to confirm the significance of certain information or rumors that are not confirmed by pointing to an official source and raise doubts. The development of information technologies has significantly simplified the process of falsifying official identity documents, and social networks have accelerated the process of "legalizing" fake experts.

4) ***Fake events*** are the creation and imposition of a new interpretation of past events on the public or the partial substitution of a sequence of events. The latter process is based on such a concept as ***"memory conformism,"*** the property of memories of past events to be distorted under the influence of someone else's opinion. When a person discovers that most of the people around them describe a case that they also remember differently, they tend to agree with them. This, in particular, is facilitated by the activity of various thematic groups in social networks, where, under the influence of the social circle, a stereotype of attitudes toward key issues of the present is laid by distorting memories and changing opinions about past events (Kyrychenko,2023). It is possible to define such ***methods used in the process of propaganda during hybrid warfare*** (Tkach, 2016):

- establishing trusting relationships with the target audience (by using common and well-established statements, links to authorities, and quotes, etc.);
- creating the illusion of independent mental work (preparing and submitting materials in such a way that the audience has the feeling that they have reached the proposed conclusions completely independently; moreover, they have done serious mental work to make this decision);
- using the image of an encyclopedic author who operates with a huge amount of material and floods the enemy with information (when using full-scale texts of archival materials, interdepartmental correspondence, economic tables and calculations, and other very difficult-to-read texts, the authenticity of which is almost impossible to determine);
- "Drowning in documents"—manipulation of documentary materials, research results, purposeful selection of only those sources that "fit" into the idea, falsification of documents, impossibility of their verification, etc.;
- conscious and purposeful provision of information of intense emotional coloring in order to suppress the processes of rational thinking of the audience exposed to information attack;
- designing and describing events in the media and literature long before something like this happened in reality;

- interpretation and biased commentary on events instead of detailed information about the facts.

If until recently the Internet had a predominantly informational component, then at the present stage it is increasingly gaining strength in propaganda and propaganda influence, characterized by pronounced aggressiveness (Hryshchuk & Tagarev, 2018). Traditional mass media are increasingly working with Internet resources as sources of information and a means of influencing the consciousness of citizens. Information on the web is becoming more and more popular, socially significant, and quickly disseminated.

In the process of analyzing the essence of hybrid warfare, the term "psychological warfare" is also often used, which was first used by the British military historian, J.F.C. Fuller (John Frederick Charles Fuller) at the beginning of the twentieth century in the analysis of the first World War (Aslam et al ., 2020). Later, American researchers borrowed this term and began to use the concept of "psychological operation" or "information operation" in this context (Vassileva & Zwilling, 2018).

The Institute of National Strategic Studies of the United States and some Western experts, analyzing the components of information warfare, distinguish separately the conduct of psychological warfare, the task of which is to manipulate the masses for the purpose of (Zaporozhets, 2017):

- introducing hostile, harmful ideas and views into the public and individual consciousness;
- disorientation and misinformation of the population;
- weakening of certain beliefs and moral foundations;
- intimidation of their people by the image of the enemy;
- intimidation of the enemy with their own power, etc.

The basic tools of information warfare include (Renz, 2016):

1) hiding information;
2) misrepresentation of information;
3) quantitative increment of messages of a certain type;
4) distraction from the important and insignificant.

Each of these tools has a large number of applications and is used differently in text, video, and audio messages.

Information influences through text messages are carried out in this way (Renz, 2016):

1) keeping silence on particular matters;

2) presenting a false fact;

3) a combination of true and false facts and comments;

4) representation of random phenomena as typical and systemic;

5) shifting accents in the message by skipping, selecting manipulative headings, and highlighted quotes;

6) misleading or incorrect reference to the sources of the message (for example, veiled hints of authority — "information from reliable sources");

7) disclosure of facts obtained from unofficial and unreliable sources;

8) use of time discrepancies (using facts about past events to confirm reports about modern realities; mentioning the facts of the past with their distortion based on the fact that no one remembers the details; distorting the chronology of events);

9) silencing messages about important facts with secondary ones or creating a colorful mosaic of messages about current and irrelevant events in order to complicate the recipient's formation of priorities;

10) increase the frequency of playback of messages on the same topic;

11) use of certain irritant words with expressive positive or negative connotations: "truth," "freedom," "democracy," "patriotism," "betrayal," "fascism," "corruption," appeal to feelings and speculation on expectations: "prosperity in the house," "stability," "confidence in the future," "pride in the motherland";

12) use of models (for example, "global problems" or "protection of interests");

13) labeling (for example, "junta" or "country that did not take place");

14) hiding the lack of content or potentially dangerous content of the message behind poetic metaphors — comparisons, hyperbole, rhetorical questions, exclamation sentences, and emotionally colored vocabulary;

15) using verb forms, such as imperative verbs, to encourage direct action ("vote," "don't sleep," "decide");

16) "hypnotizing" recipients with terms, neologisms, and borrowings, the exact meaning of which is often not known not only to the general audience but also to the speakers themselves;

17) obsessive discussion over a certain period of time of a limited number (1-3) of top topics (they are called "ideas of the day," "top topics of the week," "media agenda," etc.);

18) confusion of artistic images and reality (appeal to well-known literary works, films, and works of mass media culture) or the use of mental stereotypes, national symbols, etc.

19) dominance of news of negative or tragic content; intimidation by military, environmental, and economic dangers.

Information influences, with the help of images, video, or audio recordings, are carried out in this way (Kharamurza, 2023):

1) use fragments of past records or any materials about events in another country to illustrate up-to-date news in a country that is a victim of information aggression;

2) presenting a true fragment of the record as an illustration of a manipulative comment;

3) distortion of the content by deleting some fragments;

4) overlay on the video sequence of voice acting, translation, and captions that contain text that was not actually pronounced;

5) representation of the object in a photo or video from an unfavorable angle, aimed at the appearance of disgust, neglect, subconscious antipathy, or laughter;

6) use of the prohibited "25 frames" technologies;

7) appeal to emotions through the use of scale, colors, and images.

The information challenges of hybrid warfare are quite different in nature and have both a local (short-term) dimension, for example, the information occupation of individual regions and the spread of unprecedented amounts of disinformation and propaganda, and a more abstract (long-term) dimension, such as, for example, disillusionment with the mass communication media of the international community (Barovskaya, 2016).

Specific features of information wars are (Kharamurza, 2023):

1) ***polyvector capacity*** (information operations are carried out simultaneously in several directions; the influence is directed against the population located in the conflict zone; against citizens of a hostile country located outside the zone of force influence; within the aggressor state—to justify the aggressive policy; in the international arena—to justify their actions or dissociate themselves from them; search for allies);

2) ***the imperceptible nature of information influence*** and the absence of obvious destruction;

3) ***insufficient predictability of results; delayed results over time***;

4) ***variability of information influences*** and, accordingly, difficulties in rapid response to them;

5) ***influence*** in the vast majority not on material objects but on the intelligence, emotions, and psyche of people;

6) the nature of logistics is ***atypical*** for ordinary armed conflicts (information influences are carried out through radio and television, the Internet, social networks, and communication channels in social communities).

The most important signs of the presence of information influence *today are considered* (Renz, 2016):

1) *high frequency and tendentiousness* in the coverage of certain news; lack of correct discussion of different points of view; giving preference to emotional rather than analytical ways of presenting material in the media;

2) *obsessive drawing of public attention to messages that discredit* (often with the help of falsified data) the image of the state, its political, economic, and scientific spheres, prominent representatives of the state, and facts of history;

3) *the dominance of sensational, scandalous topics in the information space*, which cause an aggravation of internal contradictions and tension in society;

4) *the presence of messages that threaten the life and health of citizens*, promote war, national and religious hostility, change of the constitutional order by force or violation of the territorial integrity of the state, totalitarianism, or Nazism;

5) *publication of identical messages of dubious content in several mass media* with the same dubious reputation at once;

6) *increasing the share of foreign mass media* and mass communication media in the information space of the state;

7) *increasing the number of domestic mass media controlled by foreign citizens* or unknown persons;

8) obsessive retransmission of TV and radio programs, films, and foreign-made music;

9) excessive and unjustified "strengthening" of the personnel of mass media, news agencies, and PR agencies by foreign specialists;

10) creating physical obstacles to the functioning of mass media, especially in the border areas of the state;

11) targeted distribution of computer viruses and special programs capable of destroying, damaging, or intercepting information in global and local computer networks.

For example, ***the process of influencing information on society in social networks occurs according to the following algorithm*** (Hrynchenko & Molodetska-Hrynchuk,2018):

1) Instagram, Facebook, etc.) highlighting one social network and *focusing on those messages* (posts) or images (in the case of Instagram, Facebook, etc.) *that represent conflict-causing information.*

2) *Identifying and specifying the focus group or target audience*. Drawing a matrix of states and vectors of shift or transformation of group activity. Simultaneously with these actions, thematic information pools are specified, the structure of verification and reliability sources is evaluated, and modifiers are segmented according to the degree of resonance for the correct sequence of "pumping.".

3) *Working out patterns of behavioral norms*. A list of expected results is constructed, a list of resonance modifiers is selected, a network of verification sources is created, and then a network of resonance control nodes for focus groups is determined.

4) *Combining information into a stream in accordance with the order of presentation*. Information is presented in the direction in which it is convenient to " promote" it in society.

5) *Finding or creating a reason (provocation)* that causes vivid public discontent.

6) *Launch pools of information that generate previous behavior patterns*. Launch trigger pools of information to transform focus groups. The passage of information through nodes is monitored, and, if necessary, correction modifiers are connected.

7) Further, it is possible to bring people to the streets through social networks.

8) *Launch modifiers for high-quality template transformation*. Control and correction of the vector of formation of activity foci.

By managing such flows of appropriately prepared information, it is possible to manage a certain segment of society, for example, radical groups or associations of citizens with protest moods, who, in a state of emotional excitement, easily and uncritically perceive such information and direct their energy to the right place for the subject of influence at the right time. Currently, at the national and interstate levels, drastic measures to counter information attacks have not yet been developed, which means that in information wars, success will be ensured by increasing the improvement of information technologies. Therefore, it is advisable to continue scientific intelligence for further study and detailed analysis of the main methods of conducting hybrid warfare in the modern information society.

5. Conclusions. The dynamics of propaganda and disinformation in hybrid warfare reveal a complex interplay of psychological manipulation, media distortion, and strategic communication. The "4D" and "4f" frameworks offer critical insight into the mechanisms by which adversaries seek to control narratives and influence both domestic and international audiences. As social media increasingly becomes the primary channel for disseminating information, the challenges of identifying and countering falsehoods grow more intricate. Effective defense against such information threats requires a multifaceted approach that combines awareness, critical analysis, and technological tools to safeguard truth and democratic resilience. Understanding the nuances of propaganda tactics is essential for policymakers, security experts, and civil society to mitigate the impact of information warfare and maintain societal stability in an era dominated by digital communication.

References

Aslam, S., Hayat, N., & Ali, A. (2020). Hybrid warfare and social media: Need and scope of digital literacy. *Indian Journal of Science and Technology, 13*(12), 1293–1299. https://doi.org/10.17485/IJST/v13i12.43

Barovskaya, A. (2016). Information challenges of hybrid warfare: Content, channels, counteraction mechanisms (Analytical supplement). *National Institute for Strategic Studies.* https://niss.gov.ua/sites/default/files/2016-06/inform_vukluku.pdf

Doroshkevich, A. (2015). Hybrid warfare in the information society. *Bulletin of the National University "Yaroslav Mudryi National Law Academy of Ukraine,"2*(25), 21–28. http://www.irbis-nbuv.gov.ua/cgi bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vnyua_2015_2_5

European External Action Service. (2022). *2022 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI).* Strategic Communications, Task Forces and Information Analysis (SG.STRAT.2), European Union. https://euhybnet.eu/wp-content/uploads/2022/11/EEAS-AnnualReport-WEB_v3.4.pdf

Feskov, I. V. (2016). Basic methods of conducting hybrid warfare in the modern information society. *Actual Political Issues, 58*, 66–76. https://dspace.onua.edu.ua/server/api/core/bitstreams/622a115c-5b8a-4cd3-8bf9-a87c614b3e66/content

Fisenko, T. (2016). Manifestations of hybrid aggression at the mass communication level. *Bulletin of the Book Chamber, 11*, 26–29.http://www.irbis-nbuv.gov.ua/cgi- bin/irbis nbuv/cgiirbis64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR _=20&S 21STN=1&S21FMT=ASP_meta&C21COM=S&2 S21P03=FILA=&2_S21STR=vkp_2016_11_10.

Giegerich, B. (2016). Hybrid warfare and the changing character of conflict. *Connections: The Quarterly Journal, 15*(2), 65–72. https://doi.org/10.11610/connections.15.2.05

Gorban, Y. (2015). Information war against Ukraine and means of its conduct. *Bulletin of the National Academy of Public Administration under the President of Ukraine, 1*, 136–141. http://www.irbis-nbuv.gov.ua/cgi- bin/irbis_nbuv/cgiirbis64.exe?I21DBN=LINK&P21DBN _=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vnadu_2015_1_21

Hetmanchuk, M., & Zazulyak, Z. (2019). The information sphere as a key factor in Russian hybrid aggression. *Bulletin of Lviv University*. https://science.lpnu.ua/sites/default/files/journalpaper/2019/jun/16905/hetmanchuk212019_0.pdf

Hrynchenko, B., & Molodetska-Hrynchuk, K. (2018). Methodological foundations of state information security in social networks under hybrid warfare. *Information & Security: An International Journal, 41*, 61–79. https://isij.eu/system/files/download-count/2023-01/4105_hryshchuk_molodetska.pdf

Hryshchuk, R., & Tagarev, T. (2018). Hybrid warfare challenges and responses: Lessons from Ukraine. *Information & Security: An International Journal, 41*, 5–8. https://doi.org/10.11610/isij.4101

Kharamurza, D. (2023). Information terrorism as a tool of hybrid warfare and a destructive factor of the media space. *Integrated Communications, 2*(16), 29–37. https://intcom kubg.edu.ua /index.php/journal/article/download/272/220/?utm_source=chatgpt.com

Krikun, V., & Baulina, T. (2022). Disinformation as a tool of hybrid warfare: Essence and consequences. *Philosophical Bulletin, Kyiv National University.* https://bulletinphilosophy-knu.kyiv.ua/index.php/journal/article/view/113

Kyrychenko, V. (2023). Ukraine's information space under hybrid warfare conditions. *Journal of Social and Applied Psychology.* https://eprints.zu.edu.ua/38824/

Lisetsky, Y., Starovoitenko, O., Semenyuk, Y., & Pavlenko, D. (2021). Hybrid warfare: Components and features. *Scientific Notes of the V. Vernadsky TNU Series: Public Administration, 32*(71/5), 63–70. https://www.pubadm.vernadskyjournals.in.ua/journals/2021/5_2021/13.pdf

Loishyn, A., Tkach, I., Havrylko, Y., Oleksiy, G., & Tkach, M. (2021). Analysis of the features of hybrid warfare. *Political Science and Security Studies Journal, 2*(1), 14–25. https://doi.org/10.5281/zenodo.4642371

NATO Strategic Communications Centre of Excellence. (2021). *Strategic Communications Hybrid Threats Toolkit*. https://stratcomcoe.org/pdfjs/?file=/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf?zoom=page-fit

Nikolic, N. (2018). Connecting conflict concepts: Hybrid warfare and Warden's rings. *Information & Security: An International Journal, 41*, 21–34. https://doi.org/10.11610/isij.4102

Paul, C. (2011). *Information operations: Doctrine and practice*. RAND Corporation. https://www.bloomsbury.com/us/information-operationsdoctrine-and-practice-9780275995911/

Razumkov Centre. (2016). Russia's "hybrid" warfare is a challenge and a threat to Europe. *National Security and Defence, 9–10*, 2–16. https://razumkov.org.ua/uploads/journal/ukr/NSD167-168_2016_ukr.pdf

Renz, B. (2016). *Russia and hybrid warfare: Going beyond the label.* Strategic Studies Institute. https://researchportal.helsinki.fi/en/publications/russia-and-hybrid-warfare-going-beyond-the-label

Rid, T. (2016). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Ruschenko, I., & Pavlenko, O. (2015). *Russo-Ukrainian hybrid warfare: A sociologist's view (Monograph)*. https://www.hups.mil.gov.ua/assets/uploads/library/vitchizna/rosiysko-ukrainska-gibridna-viyna.pdf

Sirotenko, A. (2020). *Military aspects of countering "hybrid" aggression: Experience of Ukraine* (Monograph).The National Defence University of Ukraine named after Ivan Chernyakhovsky. https://nuou.org.ua/assets/monography/mono_gibr_viin.pdf

StopFake. (2025). *Anatomy of an info war: How Russia's propaganda machine works and how to counter it.* https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine- works-and-how-to-counter-it

Trebin, M. (2014). The phenomenon of "hybrid" warfare. *Gilea: Scientific Bulletin, 87*, 366–371. http://www.irbis-nbuv.gov.ua/cgi bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=

Tkach, V. (2016). Special propaganda as an information component of Russia's hybrid warfare against Ukraine. *Strategic Priorities. Politics Series, 1*(38), 99–109. http://www.irbis-nbuv.gov.ua/cgi- bin/irbis_nbuv/cgiirbis_64.exe?I21DBN =LINK&P21DBN==UJRN&Z21ID =&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM= &2_S21P03=FILA=&2_S21STR=sppol_2016_1_12

Vassileva, B., & Zwilling, M. (2018). Hybrid warfare simulation-based learning: Challenges and opportunities. *Information & Security: An International Journal, 39*(3), 220–234. https://doi.org/10.11610/isij.3919

Zaporozhets, O. (2017). The phenomenon of hybrid warfare in modern international relations. *International Relations: Political Sciences, 16*. http://clouds.iir.edu.ua/index.php/pol_n/article/view/3344

Zdioruk, S., & Palinchak, M. (2022). *Influence of the Moscow Patriarchate on national identity in the context of Russia's war against Ukraine*(pp. 366–377).http://ud.gdip.com.ua/wp-content/uploads/2022/12/41-2022.pdf