

MODERN

METHODS OF CONDUCTING INFORMATION WARS

MÉTODOS MODERNOS PARA LLEVAR A CABO LA GUERRA DE LA INFORMACIÓN

Elvin Bahruz Talishinsky

E-mail: Elvin.Talishinsky@au.edu.az

ORCID: <https://orcid.org/0000-0001-5318-5537>

Department of Political and Social Sciences, Azerbaijan University.

Suggested citation (APA, seventh ed.)

Talishinsky, E. B. (2025). Modern methods of conducting information wars. *Universidad y Sociedad*, 17(S1). e5552.

ABSTRACT

This article explores the growing significance of information warfare in the digital age, analyzing its foundations, mechanisms, and implications within the broader context of political, social, and technological transformations. It traces the evolution of warfare from traditional physical confrontations to conflicts rooted in information and psychological influence, highlighting how the information and political spaces intertwine in shaping modern geopolitical dynamics. In the research it is examined key elements of information warfare, such as propaganda, disinformation, manipulation, and cyber-attacks, drawing on classical and contemporary theories, including the works of Carl von Clausewitz, Robert Cialdini, Noam Chomsky, and Zbigniew Brzezinski. It is also addressed the psychological dimensions of influence and manipulation, underscoring the role of media, digital platforms, and emotional appeals in shaping public opinion. By integrating insights from philosophy, sociology, psychology, and political science, the article presents information warfare as a critical and evolving tool of power in the 21st century.

Keywords: Confrontation of states, Information war, Manipulation, Propaganda, Cyber-attack.

RESUMEN

Este artículo explora la creciente importancia de la guerra de la información en la era digital, analizando sus fundamentos, mecanismos e implicaciones en el contexto más amplio de las transformaciones políticas, sociales y tecnológicas. Traza la evolución de la guerra desde las confrontaciones físicas tradicionales hasta los conflictos arraigados en la información y la influencia psicológica, destacando cómo los espacios informativos y políticos se entrelazan en la configuración de la dinámica geopolítica moderna. En la investigación, se examinan elementos clave de la guerra de la información, como la propaganda, la desinformación, la manipulación y los ciberataques, basándose en teorías clásicas y contemporáneas, incluyendo las obras de Carl von Clausewitz, Robert Cialdini, Noam Chomsky y Zbigniew Brzezinski. También se abordan las dimensiones psicológicas de la influencia y la manipulación, destacando el papel de los medios de comunicación, las plataformas digitales y los recursos emocionales en la formación de la opinión pública. Al integrar perspectivas de la filosofía, la sociología, la psicología y la ciencia política, el artículo presenta la guerra de la información como una herramienta de poder crucial y en constante evolución en el siglo XXI.

Palabras clave: Confrontación de estados, Guerra de información, Manipulación, Propaganda, Ciberataque.

INTRODUCTION

The transition from the 20th to the 21st century was accompanied by widespread computerization and the introduction of new technologies into various areas of public life. Today, a country striving to occupy a full-fledged place on the world political arena cannot do without the development of information and communication technologies, which serve as the basis for ensuring its status on the international stage. However, along with obvious advantages, scientific and technological progress entails new security threats for both individual states and the world community as a whole. The vulnerability of the information space is becoming increasingly obvious, which, in particular, is confirmed by the emergence of the term “information war”. When we hear the word “war”, we usually associate it with weapons, violence, and conflict. War is a confrontation between state entities that includes military action. Information warfare, although not associated with the use of weapons, is still a struggle that uses information technology.

The 18th century Prussian general and military theorist Carl von Clausewitz wrote:

War is an act of violence aimed at compelling the enemy to carry out our will... Politics indicates the purpose for which war is waged and thereby determines its character... War is not an isolated phenomenon, but grows out of a specific, very concrete situation; it is a continuation of the political relations that preceded it... Consequently, war is not only a political act, but also a genuine instrument of politics, a continuation of political relations, their implementation by other means... War in human society – the war of entire nations, and moreover, civilized nations, always flows from a political situation and is caused only by political motives... (von Clausewitz, 1989, p. 76).

Thus, war is a universal and multifaceted phenomenon; it is simultaneously a political, social, economic, cultural and psychological event, since it affects all spheres of society's life, subordinating all social, and often personal, life to its logic. The technological and technical component of war is constantly being updated, the methods of waging it are being improved, and the arsenal of weapons of physical destruction is being supplemented by “weapons” of symbolic destruction, aimed at spiritual, value-motivational spheres of activity.

Information as a weapon transcends the mere transmission of data to become an instrument of power and persuasion. In the conceptual transition from Clausewitz to modern information warfare, three essential features emerge: a) the primacy of political purpose, b) the non-linearity of the scenario—where state and non-state actors

compete simultaneously—and c) the critical importance of public perception as a “battlefield.” Therefore, information warfare is not a simple addition to the spectrum of war, but an autonomous domain in which falsehoods and the manipulation of beliefs replace conventional ammunition. This domain redefines the concept of victory: it is not measured in meters of territory, but in the “quota of credibility” that an actor manages to impose on public opinion (Donovan, 2023).

In this sense, the explosion of GANs since 2014 has allowed the creation of deepfakes with previously unattainable levels of realism (Kleemann, 2023; Walczyna & Piotrowski, 2024). Cinar (2023) analyzes how these techniques allow cybercriminals to produce fake materials to misinform citizens and weaken political institutions. Leone (2023) argues that the main danger lies not in technical quality, but in the cumulative erosion of trust: It's not one big deepfake that changes an election, but many of moderate quality that undermine the perception of truth. It has been assessed that up to 45% of online activity can be automated, aimed at spreading specific narratives. More recently, the International Panel on the Information Environment (IPIE) has noted that platform owners have decisive power over the visibility of content, increasing the risk of inadvertent bias or concerted manipulation (Milmo, 2024).

Thus, modern information warfare relies on sophisticated methods designed to manipulate public perception and destabilize social and political systems. One of its pillars is targeted disinformation campaigns, which employ techniques such as audience microsegmentation through big data analysis to identify vulnerable demographic groups and personalize messages that reinforce their prejudices. These campaigns often exploit polarizing narratives based on pre-existing divisions based on race, religion, or ideology, amplifying social conflicts to fragment collective cohesion. Furthermore, they operate in a coordinated manner across multiple platforms—from social media like Twitter and Facebook to underground forums—ensuring the persistence of the message even if some platforms block specific accounts (Łabuz & Nehring, 2024).

Another critical front is the use of cyber operations and infrastructure sabotage, which include attacks on the news supply chain through intrusions into media systems to insert false information into official sources. Also notable are techniques such as search engine manipulation through malicious SEO, positioning misleading content in the top results, and interference in electoral processes through intrusions into electronic voting systems to alter counts or generate distrust in the legitimacy of the process (Donovan, 2023). On the other hand, cognitive

warfare focuses on exploiting psychological weaknesses by designing messages that take advantage of cognitive biases, such as confirming prejudices or appealing to intense emotions (fear, anger). This approach seeks to psychologically destabilize societies, creating environments of uncertainty through the saturation of contradictory information, which induces apathy or widespread distrust (Samoilenko & Suvorova, 2023). Therefore, to counter these threats, intelligence and counterintelligence tools have been developed (Gilbert & Gilbert, 2024), such as AI-based systems to detect deepfakes by analyzing subtle artifacts in videos, although their effectiveness is still limited compared to advanced technologies such as generative adversarial networks (GANs). Furthermore, social media forensics allows for real-time analysis of dissemination patterns to identify coordinated campaigns before they reach mass audiences.

In general, these methods have significant strengths: their high scalability allows them to reach global audiences with relatively low investment, while the algorithmic multiplier effect reinforces sensationalist content, maximizing its impact. Their low physical risk allows actors to operate clandestinely, avoiding direct retaliation (Donovan, 2023). However, they have weaknesses such as emerging detection through defensive AI, which advances in closing gaps to identify bots and deepfakes. Disinformation narratives are also fragile, as their public exposure erodes the sender's credibility. Furthermore, multidimensional interference—international sanctions, diplomatic pressure, and litigation—can tarnish the legitimacy of these operations. Therefore, the ethical and legal implications related to this issue are profound: information manipulation violates human rights by undermining the right to truth and informed political participation. However, blurred legal boundaries make it difficult to criminalize in many countries, while the debate about the responsibility of platforms in the modulation and amplification of content is growing, demanding more robust regulatory frameworks (Milmo, 2024).

Given this background, the objective of this paper is to examine the growing relevance of information warfare in the digital age, analyzing its conceptual foundations, operational mechanisms, and repercussions on geopolitical and social dynamics. To this end, a qualitative approach is adopted based on an exhaustive review of classical and contemporary literature (including works by von Clausewitz, Cialdini, Chomsky, and Brzezinski), the conceptual analysis of key elements such as propaganda, disinformation, manipulation, and cyberattacks, and the interdisciplinary integration of perspectives from philosophy, sociology, psychology, and political science. This

approach is complemented by real-life case examples to illustrate current trends and challenges.

DEVELOPMENT

On information warfare: important concepts

The 21st century can rightfully be called the information age. We are witnessing a new revolution in which the attitude towards information is of particular importance. Information, in turn, influences humanity and the course of world events. Throughout human history, a huge amount of information has been accumulated, but the volume of knowledge collected recently significantly exceeds everything that was collected before. This is certainly a huge step forward. However, the most important thing is that all this information is now available to everyone, and we find ourselves in an ocean of data. For example, if earlier the main task of a person was to find the necessary information, now we are faced with the problem of how to select from this ocean of data exactly the information that is necessary to solve a specific problem. Modern society is experiencing global informatization. The dependence of civilization on the information component has made it much more vulnerable in this area. In addition, the widely accepted model of an open society has a significant impact on the situation. One of the key results of the formation of the information society was the emergence of a global information space, where a fierce struggle for information superiority has unfolded.

Before defining information warfare, it is necessary to understand the concept of information itself, which is the main resource and content of information warfare. Information, derived from the Latin "informatio", means an explanation or presentation of something. In general, it is a measure of the distribution of matter and energy in space and time, as well as a measure of changes accompanying all processes occurring in the world. Information is a general scientific concept that covers the exchange of data and signals between living beings and inanimate nature, as well as between people and devices. In other words, information is data about objects and phenomena in the environment. The parameters, properties and states of information help to reduce the degree of uncertainty and incompleteness of knowledge. In the theory of information warfare, it is important to distinguish between two concepts - information and data. Data, in turn, are considered as signs or recorded observations that for some reason are not used, but only saved. When this data begins to be used to reduce uncertainty in the future, it turns into information. Thus, it can be argued that information is data that has been updated. Information forms, along with the existing real

world, the so-called information field, which, together with information flows, forms the information space.

The information field is the totality of all information concentrated in a given volume of space-time, regardless of its forms and states, located in isolation from both the object of reflection and the subject of perception. The information flow is, in a general sense, the totality of information that moves in the information space through a communication channel. In organizational and technical terms, the structure of the information space is formed by a set of databases, information systems and technologies for their application, as well as telecommunication networks, applications and organizational units that operate on the basis of certain principles and established norms that ensure interaction between users and satisfaction of their information requests. In other words, the information space is a sphere of confrontation, where information resources serve as weapons, and the struggle is aimed at a targeted change in individual and collective consciousness. The essence of the information space, according to the well-known researcher in the field of information wars I. Panarin, is a set of information resources, systems that form, distribute, use and store information, as well as the information infrastructure (Panarin, 2003, p. 275).

The information space, being the basis for conducting an information war, is connected with the political space by a number of features, being in constant interaction and interpenetration with it. The political life of society always develops in a certain space and time. The social space is a complex network of social connections, where the existence of many social and subject objects and events is recorded, considered from the point of view of their orderliness, saturation and coverage, reflecting the real process of life of society. Fitting into the space of the biosphere and cosmic space, the social space is divided into several subspaces that make up a system, one of the important elements of which is the political space. It is formed by the entire set of social subjects influencing the system of state structure. Each of them has its place in the social structure, engaging in political activity, and becomes a subject of politics among similar subjects. Thus, the political space can be considered as one of the key concepts of the philosophy of political consciousness, denoting a part of the social space, the parameters of which determine the location, direction, depth and degree of influence of social subjects on the existing system of state structure in society.

Political space is a kind of structure according to which the political relations established in society, views on the system of state structure, bearers of state power, norms of behavior enshrined in customs, traditions and laws, as

well as the level of political culture and the system of values are reproduced. Like social space as a whole, political space has an objective character. This is expressed in the fact that throughout the existence and development of any state-organized society, there are always political subjects who have different relationships to the established system of state structure and political power. Political space, like social space, is simultaneously continuous and fragmentary. Continuity is manifested in the fact that political activity is an integral element of every state-organized society at all its historical stages. At the same time, discontinuity is expressed in the fact that the political activity of an individual political subject is limited to a certain time and ceases with its disappearance. Political space is characteristic exclusively of state-organized societies.

The structure of political space consists of specialized fields, and the specificity of political space is revealed by the dynamics of the struggle that unfolds in each of these fields (Torkunov, 1999, p. 421). By synthesizing the concept of information and political spaces, we can derive an integrative concept of information-political space - a set of subjects and objects of information-political action and interaction; information itself, intended for use by subjects of information-political interaction; information infrastructure, which ensures the possibility of implementing the exchange of information between subjects; social relations that develop in connection with the formation, transmission, dissemination and storage of information, the exchange of information within society (Manoylo et al., 2009, p. 75).

Information warfare in the structure of the information-political space is also associated with such phenomena as information threat and information risk. Information threat is a danger, the content of which consists of different information or its combinations, which can be used against a social or socio-technical object (system) in order to change its interests, needs, and orientations for the purposes of the subject of information. Information risk is a measure of information danger and real actions of the enemy, the degree of measurement of the success or danger of possible impacts. Risk depends on the nature of the impacts and the object of impacts, on the conditions of their implementation, as well as on the possibilities of protection.

Psychological Impact, Manipulation, and Methods in Information Warfare

Thus, information warfare is a key factor in the formation of the information society and has the potential to change the direction of geopolitical processes. Information warfare has existed since the very beginning of humanity and in one form or another accompanies its history: without aggressive instincts and information, humans would be

impossible. The term “information warfare” is often associated with such concepts as “psychological impact”, “manipulation”, and “information dominance”.

Psychological impact is a type of targeted influence, specially organized with the aim of changing the behavior and activities of an individual or a group of people without open coercion. Based on the goals and nature of impact, informational and psychological influence can be manipulative (subject-object) or developing (subject-subject). Manipulative influence forms temporary, unstable mental formations, and developing influence forms fundamental personal formations, primarily the value-semantic structures of personality. Psychological impact is the process by which one person or group of people influences the thoughts, feelings, and behavior of another person, with the aim of changing their perceptions, attitudes, or actions. It can be either conscious or unconscious, and can manifest itself in a variety of forms: persuasion, suggestion, manipulation, imitation, and social pressure.

“Psychological influence is a purposeful or spontaneous impact of one subject on the mental state and behavior of another subject, in which the latter experiences stable or temporary changes” (Bodalev, 2002, p. 235). Research shows that the greatest impact is exerted by the following factors:

- the authority of the source of influence,
- the emotional tone of communication,
- group pressure,
- trust and the degree of closeness between the subjects of communication.

One of the classics of Western social psychology, Robert B. Cialdini, in his fundamental work “Influence: The Psychology of Persuasion” (2001) identifies six basic principles of influence:

1. Reciprocity - people tend to return favors.
2. Commitment and Consistency - the desire to match their past actions and words.
3. Social Proof - the tendency to focus on the behavior of others.
4. Liking - people are more easily influenced by those they like.
5. Authority - the tendency to listen to those who are perceived as experts.
6. Scarcity - rare things seem more valuable.

These principles have found wide application in marketing, negotiations, interpersonal communication, and even politics. Cialdini (2001) emphasizes that influence can be both ethical and useful, and manipulative, if used to control behavior without the consent or understanding of the recipient. Psychological influence can be used both for good - for example, in training or psychotherapy, and for harm - in manipulative techniques or propaganda. Turkish psychologist Dogan Cüceloğlu in his work entitled “İnsan İnsana” draws attention to the importance of psychological influence in people's lives. According to Cüceloğlu, “one of the most important forces in communication between people is the intention and emotion behind the words, not the words themselves” (Cüceloğlu, 2016, p. 74). This approach shows that psychological influence is not only carried out on a rational level, but also on an emotional and intuitive level. Cüceloğlu also emphasizes that the basis of effective communication is mutual trust, empathy and open communication. Psychological influence in this regard can be used both positively and negatively. While positive use contributes to the development of personality, negative use can limit a person's freedom in decision-making.

Manipulation is a hidden psycholinguistic influence that requires special knowledge and is carried out in order to change the opinions, views, attitudes and goals of the person being manipulated, who, under the force of the influence exerted on him, independently expresses a desire to change them. A certain set of features follows from the definition. The signs of manipulation are understood as its essential characteristics, which make it possible to distinguish this type of influence from others (Bahruz, 2023, p. 145). Unlike overt persuasion or argumentation, manipulation relies on exploiting an individual's cognitive and emotional vulnerabilities. According to the definition given in the work of American psychologist George K. Simon, manipulation is “a form of deception in which one person uses subtle, often aggressive, methods of influence to achieve his own goals at the expense of another without revealing his true intentions” (Simon, 2010, p. 176). Simon analyzes in detail the tactics of manipulators, such as distortion of facts, blaming the victim, playing on guilt feelings, and using false logic. In his book *In Sheep's Clothing*, he identifies the characteristic traits of manipulators: they tend to use techniques such as projecting guilt, denying responsibility, exaggerating threats, withholding information, and moralizing.

Manipulation is effective largely because it operates covertly, by making the victim feel guilty, anxious, or obligated. It relies on exploiting a person's psychological weaknesses, such as the desire for recognition, fear of conflict,

or the desire to be seen as good by others. This makes it especially dangerous in family, professional, and social contexts. In a digital society, manipulation has taken on new forms. Social media algorithms, targeted advertising, and fake news create an environment in which mass manipulation has become easier and more widespread. As Tali Sharot, a neuropsychologist at University College London, points out, “manipulation is amplified in conditions of information overload, when people start to choose what they like to hear over what is true” (Sharot, 2017, p. 256). Awareness and critical thinking are key tools in combating manipulation. Exposing manipulative techniques and teaching emotional literacy help build resilience to psychological pressure.

In modern society, manipulations acquire particular significance in conditions of political instability, information warfare and media pressure. Some scholars often view manipulation as a tool of political struggle. Turkish researcher Yavuz Arslan notes in his work “Medya Manipülasyonları ve Algı Yönetimi” that Turkish media are actively used to control public opinion, especially during pre-election periods. Manipulation is manifested through selective presentation of information, emotional coloring of news and discrediting of opponents. Arslan emphasizes that manipulation can be both targeted and unintentional, which makes it difficult to detect. Manipulation is widely used in politics, advertising, the media, and even in interpersonal relationships. For example, Noam Chomsky, in his work *Manufacturing Consent*, together with Edward Herman, analyzes in detail how the media use filters—economic and ideological—to shape public opinion in the interests of the elites. Chomsky emphasizes: “Whatever does not correspond to the interests of the authorities simply does not make it onto the agenda” (Herman & Chomsky, 2008).

Like any war, information warfare has its own methods. The first method is propaganda. A number of researchers believe that information warfare is aimed primarily at the human mind. Propaganda is a systematic and purposeful activity aimed at forming certain attitudes, opinions and behavior patterns. According to the definition of Harold Lasswell, one of the founders of modern political communication: “propaganda is the management of collective opinion by the manipulation of significant symbols” (Lasswell, 1938, p. 9). The classical understanding of propaganda includes both informational and emotional impact. Jacques Ellul, a French sociologist and author of the fundamental work *Propaganda: The Formation of Men's Attitudes*, emphasizes that propaganda is not just the dissemination of ideas, but a technology for introducing these ideas into consciousness, bypassing critical thinking.

Scholars have identified several key features of propaganda:

- One-sidedness: Focusing only on favorable facts, ignoring alternative points of view.
- Appeal to emotion: Using fear, patriotism, hatred, and other emotions to enhance impact.
- Repetition: Frequent repetition of messages helps reinforce desired attitudes.
- Authority of the source: Propaganda often relies on “official” or “trusted” channels to increase credibility.

Thus, propaganda is not only a tool of authoritarian regimes, but also a mechanism operating within democratic societies through the media, education, culture and social networks.

The second method is disinformation – the dissemination of deliberately false information with the aim of influencing the opinion of the country's leadership and population. In the digital age, disinformation has become one of the main threats to society's information security. Disinformation is the deliberate dissemination of false or misleading information with the aim of manipulating public opinion, creating panic, or achieving political, economic, or military goals. Disinformation is especially dangerous on social media, where information is disseminated instantly and without due verification. According to the UNESCO report “Journalism, ‘Fake News’ & Disinformation” (Ireton & Posetti, 2018), disinformation differs from a simple error in that it is conscious, intentional and aimed at achieving a specific effect. The authors of the report emphasize that disinformation can undermine trust in state institutions, interfere with democratic elections and threaten national security. To combat disinformation, international organizations and states are taking steps to develop media literacy, create fact-checking systems and tighten control over digital platforms. However, the effectiveness of these measures directly depends on the ability of society to critically perceive information and distinguish reliable sources from manipulative ones. Thus, disinformation is not just a threat to the truth, but also a serious challenge to the stability of society, requiring a comprehensive response from the state, the media and the citizens themselves.

In addition, cyber-attacks have become a widely used method in information wars. In simple terms, this is an attempt to compromise the security of a computer system. Cyber-attacks are deliberate actions aimed at disrupting, destroying, or gaining unauthorized access to computer systems, networks, and data. In the context of digitalization and global dependence on information technology, cyber-attacks have become one of the most serious threats to national and international security. Modern cyber-attacks

can have various goals, ranging from identity theft and financial fraud to election interference, infrastructure disruption, and cyber-espionage. Examples of such attacks include ransomware (e.g. WannaCry), phishing campaigns, and attacks using malicious software (malware).

According to Edwards & Brzezinski (2009), complex computer viruses are capable of undermining the military potential of an opponent. States can support hacker attacks on certain objects for the purposes of espionage or obtaining economic information. These authors emphasized that cyber capabilities have become a powerful tool in modern statecraft. He acknowledged that complex computer viruses and cyber intrusions can seriously undermine a state's military and economic infrastructure without a single shot being fired. Such non-traditional threats challenge classical notions of warfare, as states may now sponsor cyberattacks to conduct espionage, sabotage, or economic theft, thereby blurring the lines between peace and conflict. In their book it is examined the transformation of global politics in the face of new threats, including those in cyberspace, and emphasizes that information technology can be used as a means of political pressure, espionage, and undermining the military potential of an adversary. Sophisticated distribution of computer viruses can disrupt rivals' military and industrial assets. States can order unofficial assassinations of foreign leaders and weapons scientists. They can support hacking of foreign institutions for intelligence purposes and of private commercial organizations for commercial advantage.

In his later writings, especially in the context of asymmetric threats and network-based warfare, Brzezinski pointed out that cyberspace has become a new arena of geopolitical competition, where actors ranging from nation-states to independent hacker groups can have disproportionate influence. According to a 2023 report by the European Cybersecurity Agency ENISA, the number of sophisticated cyber-attacks targeting key sectors such as health-care, energy, transport, and government has increased significantly in recent years. The document emphasizes that states and organizations must strengthen their cyber defense measures and invest in training information security specialists (European Union Agency for Cybersecurity (ENISA), 2023).

With the beginning of the new century, the nature of confrontation between countries has changed: there is a tendency to shift the focus from open force (military and economic) methods to hidden ones, including those in the information sphere. Mass media are becoming an increasingly effective instrument of foreign policy for states, capable of not only influencing public opinion, but also of shaping and manipulating it. With the advent of the 21st

century, the nature of geopolitical competition has changed significantly. Instead of relying solely on traditional instruments of power, such as military force or economic sanctions, states are increasingly using non-kinetic, covert strategies, especially in the information sphere. Mass media, social platforms, and digital content have become essential components of soft power and are now actively used to influence, shape, and even manipulate public opinion both domestically and internationally. As scholars have noted, a technetronic society appears to be moving toward pooling the individual support of millions of uncoordinated citizens, who are easily accessible to magnetic and attractive personalities that use the latest communications technologies to manipulate emotions and control minds. This shift reflects a broader strategy in which information operations and psychological influence serve as key tools in international competition, often blurring the line between peace and conflict.

CONCLUSIONS

In the twenty-first century, the nature of conflict has undergone a profound metamorphosis: no longer confined to battlefields and tanks, warfare now unfolds across the information-political spectrum. Information warfare—encompassing propaganda, targeted disinformation, psychological manipulation, and cyber-operations—has consolidated as a cornerstone of statecraft, capable of shaping perceptions, destabilizing societies and redefining strategic advantage. By blurring the line between war and peace, and between fact and falsehood, it operates through networks and algorithms as much as through traditional hierarchies. As digital interconnectivity deepens and artificial-intelligence tools grow ever more potent (from algorithmic micro-targeting to hyper-realistic deepfakes), open societies have become increasingly exposed to covert informational assaults. This vulnerability undermines trust in democratic institutions, corrodes social cohesion and can potentially escalate into kinetic or hybrid confrontations. To meet this challenge, states and civil societies must pivot from reactive detection to systemic resilience: investing in media literacy, reinforcing transparent legal and regulatory frameworks, fostering cross-sector collaboration between governments, technology platforms and independent fact-checkers, and deploying advanced counter-intelligence tools powered by AI. Only by combining strategic foresight with robust defensive capacities can democratic norms and international security be safeguarded. Ultimately, in an era where data equals power and narratives shape reality, the capacity to critically evaluate information—and to shield minds and machines from manipulation—will determine not only

the outcomes of future conflicts, but the very foundations of open, pluralistic societies.

REFERENCES

- Bahrüz, E. T. (2023). Manipulation as a form of information-psychological war. *Universidad y Sociedad*, 15(5), 143-150. <https://rus.ucf.edu.cu/index.php/rus/article/view/4060>
- Bodalev, A. A. (2002). *Personality and Communication: Selected Psychological Works*. PER SE Publishing House.
- Cialdini, R. B. (2001). *Influence: The Psychology of Persuasion* (Revised Edition). Harper Collins Publishers. <https://www.harperacademic.com/book/9780062937674/influence-new-and-expanded/>
- Cinar, B. (2023). Deepfakes in Cyber Warfare: Threats, Detection, Techniques and Countermeasures. *Asian Journal of Research in Computer Science*, 16(4), 178–193. <https://doi.org/10.9734/ajrcos/2023/v16i4381>
- Cüceloğlu, D. (2016). *Man and Behavior: Basic Concepts of Psychology*. Remzi Bookstore.
- Donovan, J. (2023, October 13). *Misinformation Is Warfare*. TIME. <https://time.com/6323387/misinformation-israel-hamas-war-essay/>
- Edwards, R., & Brzezinski, Z. (2009). *The Choice: Global Domination or Global Leadership*. Basic Books. <https://philpapers.org/rec/BRZTCG>
- European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- Gilbert, C., & Gilbert, M. A. (2024). Leveraging Artificial Intelligence (AI) by a Strategic Defense against Deepfakes and Digital Misinformation. *International Journal of Scientific Research and Modern Technology*, 3(11), 62-78. <https://doi.org/10.38124/ijrmt.v3i11.76>
- Herman, E. S., & Chomsky, N. (2008). *Manufacturing Consent: The Political Economy of the Mass Media*. The Bodley Head. https://files.libcom.org/files/2022-04/manufacturing_consent.pdf
- Ireton, C., & Posetti, J. (Eds.). (2018). *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training*. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000265552>
- Kleemann, A. (2023). Deepfakes – When We Can No Longer Believe Our Eyes and Ears: Media Manipulation in Conflict: Challenges and Responses. *SWP Comment*, 52. <https://doi.org/10.18449/2023C52>
- Łabuz, M., & Nehring, C. (2024). On the way to deep fake democracy? Deep fakes in election campaigns in 2023. *European Political Science*, 23(4), 454–473. <https://doi.org/10.1057/s41304-024-00482-9>
- Lasswell, H. (1938). *Propaganda Technique in the World War*. Peter Smith. <https://babel.hathitrust.org/cgi/pt?id=mdp.39015000379902&seq=12>
- Leone, M. (2023). The Spiral of Digital Falsehood in Deepfakes. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, 36(2), 385–405. <https://doi.org/10.1007/s11196-023-09970-5>
- Manoylo, A. V., Petrenko, A. I., & Frolov, D. P. (2009). *State Information Policy in the Conditions of Information-Psychological Warfare* (2nd ed.). Goryachaya Liniya-Telecom.
- Milmo, D. (2024, September 24). Social media owners top global survey of misinformation concerns. *The Guardian*. <https://www.theguardian.com/technology/2024/sep/24/social-media-owners-survey-misinformation-online-news>
- Panarin, I. N. (2003). *Information War and Peace*. Olma Press.
- Samoilenko, S. A., & Suvorova, I. (2023). Artificial Intelligence and Deepfakes in Strategic Deception Campaigns: The U.S. and Russian Experiences. In E. Pashentsev (Ed.), *The Palgrave Handbook of Malicious Use of AI and Psychological Security* (pp. 507–529). Springer International Publishing. https://doi.org/10.1007/978-3-031-22552-9_19
- Sharot, T. (2017). *The Influential Mind: What the Brain Reveals About Our Power to Change Others*. Henry Holt and Co. <https://us.macmillan.com/books/9781250159618/theinfluentialmind/>
- Simon, G. K. (2010). *In Sheep's Clothing: Understanding and Dealing with Manipulative People*. Parkhurst Brothers.
- Torkunov, A. V. (Ed.). (1999). *Modern International Relations*. ROSSPEN.
- von Clausewitz, C. (1989). *On War*. Princeton University Press. <https://press.princeton.edu/books/paperback/9780691018546/on-war>
- Walczyńska, T., & Piotrowski, Z. (2024). Fast fake: Easy-to-train face swap model. *Applied Sciences*, 14(5), 2149. <https://doi.org/10.3390/app14052149>