

THE IMPACT OF DIGITAL PROPAGANDA ON MODERN CONFLICTS

Marian HOGEA

“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania

marianhogeal@gmail.com

Abstract: *In the context of globalization and the spread of communication networks, digital propaganda has become a central tool for actors involved in conflict, facilitating the dissemination of misinformation and creating narratives that can destabilize both crisis situations and international relations. The methodology applied includes a quantitative and qualitative analysis of data collected from social media platforms, case studies of recent regional conflicts and a systematic literature review. The results highlight a significant correlation between the intensity of digital propaganda campaigns and changes in public perceptions of conflict, as well as strategic adaptations by military and security institutions. In today's conflicts, disinformation and information manipulation can accelerate historically escalated disputes, altering both their internal dynamics and the external relations of the states involved.*

Keywords: information warfare, digital propaganda, disinformation, artificial intelligence, deepfake

1. Introduction

In recent decades, technological developments have radically transformed the way information is communicated and perceived globally. In the context of modern conflicts, digital propaganda has become an essential strategic tool, capable of influencing public opinion, polarizing societies and shaping political and military decisions. This new paradigm of information warfare raises fundamental questions about the nature of contemporary conflicts, where traditional borders are blurring and the battlefield is expanding into cyberspace. In an era where information flows rapidly and without barriers, state and non-state actors have developed sophisticated techniques to exploit the vulnerabilities of digital systems and modern societies. This phenomenon not only redefines conflict dynamics, but also

calls into question the effectiveness of traditional defence and crisis management mechanisms.

2. Historical Foundations of Information Warfare

The concept of “information warfare” [1] is not a new term, but has its origins deeply rooted in history, evolving with human civilization. Over time, the strategies and techniques used in this type of conflict have undergone significant changes, influenced by technological development and socio-political complexity.

Propaganda, as a method of information warfare, became widespread, especially during the two world wars. In the First World War, the belligerent states discovered the value of propaganda for mobilizing the population and demonizing the opponent. “The British pioneered this

through the War Propaganda Office (Wellington House)” [2], which used posters, pamphlets and pamphlets highlighting enemy atrocities to boost public support and demoralize enemy troops.

In the Second World War, propaganda became an even more refined art, intensified by technological means such as radio and cinematography. “Nazi Germany, through Joseph Goebbels” [3], developed one of the most effective and dangerous propaganda instruments of the era, based on emotional manipulation, the use of stereotypes and strict control of information available to the public. The Allies responded with their own information campaigns and psychological operations, such as the BBC radio broadcasts, designed to offer hope and erode the morale of German troops and the civilian population.

The Cold War period also marked a defining moment in the history of information warfare, due to the intensification of the psychological operations conducted by the two rival superpowers: the United States and the Soviet Union. The ideological confrontation between capitalism and communism was amplified by the systematic use of propaganda, disinformation and media manipulation. The term “psychological warfare” [4] found a clear expression in this era, and was developed as a strategic discipline, underpinned by in-depth sociological and psychological research.

The United States of America initiated major operations through radio stations such as “Voice of America and Radio Free Europe” [5], which broadcast political and cultural messages to countries under Soviet influence. In turn, the Soviets responded through “Radio Moscow” [6] and other media channels aimed at convincing audiences in the West and non-aligned countries of the superiority of the socialist model. Both the USA and the USSR used espionage, infiltration and psychological sabotage to weaken the position of the

adversary and attract international public sympathy.

In the 20th century and into the early 21st century, traditional information warfare techniques diversified and became increasingly complex. Classic techniques such as censorship, deliberate disinformation, visual and auditory manipulation, and the use of public emotions to provoke panic or popular support continued to be used with maximum effectiveness.

Disinformation methods were significantly improved during the Cold War, with the Soviet Union becoming an expert in creating conspiracy theories, orchestrated by the KGB, and the best known is the theory that “the HIV virus was created in American laboratories as a biological weapon” [7]. This type of psychological operations aimed to destabilize the opposing society and generate a fundamental distrust of the government and institutions.

On the other hand, traditional information warfare has continuously adapted to the evolution of the technological environment. Television became an extremely powerful tool, exploited intensively especially during the conflicts in Vietnam and the Gulf War, where live images had a major impact on the public’s perception of the war and on the internal politics of the states involved.

3. The Digital Transformation of Information Warfare

The accelerated technological development in the last decades of the 20th century led to the emergence of the Internet, also a defining event that inaugurated a new stage in the evolution of information warfare, fundamentally transforming the way in which information is managed, transmitted and manipulated. Originally conceived as a decentralized network intended to ensure continuity of communication in the event of a nuclear conflict, the internet has rapidly developed into a vital global infrastructure for the free and immediate flow of

information.

In the late 1980s and early 1990s, the accessibility of the Internet to the general public facilitated the emergence of a new information paradigm, characterized by instant communication, the elimination of geographical barriers, and the rapid and global dissemination of messages. This transformation significantly influenced the characteristics of propaganda and information warfare, allowing a free circulation of information, not directly restricted by state authorities or large media conglomerates, thus generating new opportunities, but also vulnerabilities in the field of information security.

The first notable examples of the use of the Internet for geopolitical and conflictual purposes began to appear in the 1990s, “during the Kosovo conflict (1998–1999), when both NATO and Serbia used the Internet for propaganda and psychological warfare” [8]. NATO intensified its online media campaign to gain international support, while Serbian authorities used websites to disseminate counter-narratives, trying to combat official Western accounts. A significant example of the use of virtual space in geopolitical conflicts is the “China-Taiwan tensions of 1999” [9], when cyberattacks initiated by Chinese hackers against official Taiwanese government websites were recorded. This incident is among the first documented cases of cyberwarfare and marks the beginning of a new era in which geopolitical conflicts can be extended into the digital environment, beyond the traditional boundaries of physical space.

In parallel, independent groups of hackers, sometimes with indirect support from governments, began to use the Internet to launch cyberattacks against political or ideological opponents. These early incidents highlighted the vulnerabilities of digital infrastructures and prompted the development of complex cybersecurity strategies.

The first decade of the 21st century saw the

emergence of the first open and coordinated conflicts in the online environment, known today as cyberwars. A significant example is the 2007 cyberattack on Estonia, considered the first major cyberattack against a sovereign state. Following tensions with Russia, Estonia was subjected to massive DDoS (Distributed Denial of Service) attacks, which temporarily paralyzed government institutions, banks and the media. The incident highlighted the ability of a state or state-backed actors to use the digital environment as a veritable battlefield.

Another turning point was the “2010 Stuxnet cyberattack” [10], designed to target Iran’s nuclear program. Stuxnet was the first advanced malware that not only compromised computer systems but also caused actual physical damage to Iranian nuclear facilities. The attack was attributed to state actors (notably the US and Israel), marking a crucial moment in the history of cyberwarfare and clearly demonstrating that cyberspace had become a new front for geopolitical conflict. Thus, the transition to the digital era of information warfare has been marked by rapid and significant developments, redefining the nature of conflicts and opening up new dimensions in the field of international security.

4. The New Battlefield: Social Media and the Future of Information Warfare

The Internet has not only profoundly transformed the way in which information is disseminated and manipulated, but has also provided new means by which states and non-state actors can influence, destabilize or even attack adversaries, permanently changing the rules of geopolitical confrontation. In the context of the digital age, social networks and online platforms constitute essential tools in information warfare, due to their potential to facilitate the rapid and efficient dissemination of information to global audiences. Platforms such as Facebook, Twitter, Tik Tok, Instagram and YouTube

have allowed state and non-state actors to influence public perceptions through coordinated campaigns of disinformation, propaganda and the promotion of polarizing narratives. These platforms offer advanced capabilities for precise audience segmentation and dynamic message adaptation, thus optimizing the impact on public opinion.

A prime example is the Russian interference in the 2016 US presidential election, where the use of social media allowed the amplification of social and political tensions through coordinated disinformation campaigns. Techniques used include the creation of fake accounts, the use of automated “bots” [11] and the artificial amplification of certain messages to generate divisions and confusion among the target population.

“Artificial Intelligence (AI)” [12] and algorithms play a key role in modernizing information warfare techniques, providing the ability to automate, personalize and optimize propaganda messages and disinformation campaigns. Advanced recommendation algorithms and machine learning are used to personalize and spread disinformation content, exploiting the cognitive and emotional predispositions of users. These algorithms can quickly identify audience trends, preferences, and vulnerabilities, allowing for automatic adjustment of propaganda messages to increase their effectiveness.

A relevant case study is the online campaigns carried out in the context of the COVID-19 pandemic, where social media recommendation algorithms amplified the distribution of conspiracy content and false theories, fuelling confusion and distrust in medical and scientific authorities. This algorithmic amplification has had a significant impact on public behaviour and the collective response to the global health crisis.

“Deepfakes” [13], advanced technologies that use artificial intelligence to create highly realistic fake video or audio

materials, represent one of the most complex and challenging dimensions of contemporary information warfare. The use of deepfakes raises major concerns about the authenticity of information and can have serious effects on public trust, political stability and national security.

Ethical challenges associated with the use of deepfakes include the violation of the right to privacy, compromising the reputation of public figures and their use for political manipulation or blackmail. Recent examples include manipulated videos of political leaders that have been distributed to mislead public opinion or destabilize sensitive political contexts. In addition, detecting and combating deepfakes is becoming increasingly difficult as technologies advance.

The impact of digital propaganda on international relations is becoming increasingly relevant in the current context of information and communication globalization. In modern conflicts, the rapid and precisely targeted dissemination of information, often intentionally distorted, significantly influences the dynamics of alliances and amplifies existing rivalry.

First, digital propaganda [14] significantly contributes to the formation and consolidation of international alliances by building shared narratives or by creating collectively perceived threats. States or groups of states use online disinformation to strengthen their geopolitical positions, promoting narratives that justify joint actions against a common adversary perceived as dangerous or hostile.

At the same time, digital media manipulation can lead to fractures and tensions even within traditional alliances. Strategically disseminated false or misleading information can generate distrust between allied states, negatively affecting the unity and effectiveness of joint actions. A clear example is digital interference, such as the manipulation of information or the use of fake accounts on social platforms, which can erode trust

between allies by creating suspicions about the loyalty or true intentions of international partners.

On the other hand, digital propaganda significantly accentuates existing rivalries and generates new tensions between states, amplifying conflicts and hostilities at the international level. Through digital platforms, states can conduct aggressive influence campaigns aimed at destabilizing adversaries by rapidly spreading manipulative information. Thus, historical or geopolitical rivalries can be rapidly exacerbated, transforming minor diplomatic disputes into major crises.

For example, recent hybrid conflicts demonstrate how digital propaganda can be effectively used to destabilize entire regions. Russia's digital disinformation campaigns in the context of the conflict with Ukraine have contributed to the intensification of regional tensions and have generated strong reactions from the international community. This form of propaganda not only fuels direct hostilities, but also affects the international image of the states involved, having long-term effects on their positioning in international relations.

5. Conclusions

In conclusion, the analysis of the evolution of information warfare highlights that recent technological developments have fundamentally changed the dynamics and characteristics of contemporary conflicts. Starting with the classic propagation of information through propaganda in the two world wars and continuing with the

sophistication of psychological techniques and disinformation during the Cold War, there has been a significant evolution in the methods used in geopolitical confrontations.

In recent decades, the emergence and expansion of the Internet have marked the transition to a new type of information warfare, characterized by the use of cyberspace as a strategic environment. The increased accessibility of digital platforms and social networks has radically transformed the way information is disseminated and perceived, allowing state and non-state actors to conduct coordinated propaganda and disinformation campaigns on a global scale. Advanced technologies such as artificial intelligence and algorithms have increased the effectiveness of these campaigns, thus amplifying messages and exploiting the cognitive vulnerabilities of the public.

Deepfakes, as a form of artificially generated content, represent a culmination of this evolution, raising significant ethical and security challenges. The complexity and realism of these technologies make them difficult to detect and counter, undermining public trust in the authenticity of information and the integrity of institutions.

Thus, contemporary information warfare requires the development of new strategies for defence and crisis management that take into account the fluid and decentralized nature of the digital environment, as well as the impact of emerging technologies on social and political stability.

References

- [1] <https://razboiulinformational.ro/>. Accessed May, 10, 2025.
- [2] Sanders, M. L., War Propaganda Bureau from Enciclopedia Internațională a Primului Război Mondial (1914-1918) – online. The Historical Journal. 1975. 18/1. 119-146. <https://www.cambridge.org/core/journals/historical-journal/article/his-volume-18-issue-1-front-matter/50A80E3A57948358E2741B68E169DD5F>. Accessed May, 10, 2025.
- [3] Longerich, P. Goebbels: A Biography. Editura Random House. 2015. 370-375.
- [4] Luțai, R. Uniunea Sovietică și propaganda în contextul Războiului Rece. Revista de Științe Sociale. 2011. 69-76.

- [5] Tofan, L. Ne-au ținut în viață – Radio Europa Liberă, 1970-1990. Editura Omnium. 2016. 85-112.
- [6] Winek, M.D. Radio as a Tool of the State Radio Moscow and the Early Cold War. https://digitalcommons.bucknell.edu/cgi/viewcontent.cgi?article=1050&context=chr&utm_source=chatgpt.com. 99. Accessed March, 23, 2025.
- [7] Kramer, M. Lessons from Operation Denver, the KGB's Massive AIDS Disinformation Campaign. <https://thereader.mitpress.mit.edu/operation-denver-kgb-aids-disinformation-campaign/>. Accessed March, 24, 2025.
- [8] Arquilla, J., Ronfeldt, D. The Emergence of Noopolitik: Toward an American Information Strategy. Editura RAND Corporation. 1999. 27-34.
- [9] Huang, G.C.K. China-Taiwan Computer-Based Information Warfare and Propaganda. Editura Issues & Studies. 2003. 179-210.
- [10] Zetter, K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Editura Crown Publishers. 2014. 35-100.
- [11] <https://mediacritica.md/peintele-ce-sunt-botii/>. Accessed March, 27, 2025.
- [12] Mereuță, Gh. Noile tehnologii și inteligența în conflictele militare actuale și viitoare. In: Conferința Evoluția științei militare în contextul noilor amenințări la securitatea națională și regional. Vol 1. 2020. Chișinău. December, 17, 2020. 130-145.
- [13] Mirsky, Y., Lee, W. The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys. 2020. 1-41.
- [14] David, M. Propaganda digitală și securitatea națională. Revista Intelligence. January, 11, 2018. <https://intelligence.sri.ro/propaganda-digitala-si-securitatea-nationala/>. Accessed May, 10, 2025.