INTERNATIONAL CONFERENCE RCIC'22
Redefining Community in Intercultural Context
Braşov, 5-7 May 2022

WEAPONIZED INFORMATION AND DEMOCRATIC RESILIENCE

Dan ROMAN*

* 'George Barițiu' History Institute, Romanian Academy, Cluj-Napoca, Romania

Abstract: *The virtual environment, represented mainly by social media, is being used more and more frequently and aggressively as a space for a new type of war, which uses information as a weapon. This essential change in the way war is conducted poses a considerable challenge to a democratic society, which must develop appropriate responses to the threats it faces, usually generated by an undeclared and especially invisible enemy.*

Keywords*: weaponized information; democratic resilience; hybrid war; social media*

1. INTRODUCTION

The last decades insistently revealed the manifestation of tendencies that attest significant transformation of the way wars are conducted, increasing the stake on non-military resources and capabilities. The main ways to do this are the *information warfare* (IW) – insidious, usually unassumed, conducted by various *proxies*, as well as the *economic warfare* (EW) – which uses, as a weapon, the imposing of sanctions by which it is largely limited or even blocked a state's access to the global market, weakening it considerably. However, waging a war by non-military means is far from being the prerogative of contemporaneity. Actually, 2,500 years ago, the famous Chinese general and strategist Sun Tzu noted the following, in his treatise *The art of war*[1] *(Sūn Zǐ Bīng Fǎ):* "to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting." (Sun Tzu, 2004:37).

To a greater extent, today's actors seem to align themselves with this goal. "War as politics by other means", as the Prussian general von Clausewitz called it, is no longer necessarily carried in the trenches of the battlefield, it no longer uses bullets and missiles. Today, it is conducted rather in front of the computer and in the offices of political and economic factors. It involves different strategies and aims with the purpose of controlling and dominating the opponent rather than annihilating it.

If regarding the economic war, the measures ordered and the actions are still clear and easy to identify, things get significantly more complicated when it comes to activities that are subject to propaganda, misinformation and, more recently, fake-news/ deep-fake.

What answers should be given, what countermeasures are required in such situations? The purpose of this material is to make a brief and hopefully equally edifying presentation on the concepts evoked in its title, while also revealing the relationship between them, and to show some measures and directions of action.

2. LOOKING BACK TO THE HISTORY

Throughout history, information has been a weapon since ancient times. It has been used both as a notable resource for substantiating operational decisions on the battlefield with the purpose of supplementing the knowledge of the enemy by revealing its vulnerabilities and intentions, and as a direct way of influencing it, in order to "crush its resistance without a fight", as the influential above-mentioned Chinese strategist put it.

In the second perspective, it is circumscribed to the modern concept of information operations, in which propaganda and misinformation are included, as typical actions in the course of the war. Such actions have been known since antiquity – and even since prehistory, according to P. Taylor, who notes that Neolithic murals depicting groups of people fighting each other with weapons could be "perhaps the earliest form of war propaganda" (Taylor, 2003:20).

For the ancient period, the Australian author Haroro J. Ingram, interested in terrorist propaganda, notes in a study published under the auspices of the International Center for Counter-Terrorism –

[1]In fact, the book's literal name is *Master Sun's Military Methods*.

The Hague, as a significant example, the actions of Alexander the Great who built his empire not only on the basis of his military and political genius, but he also "deployed a range of propaganda strategies including PSYOPS ('psychological operations') against enemies, narratives that framed him as one with the gods, ensuring Greek culture and even the Greeks themselves were part of the conquered societies" (Ingram, 2016:7).

A much more present narrative in war propaganda uses the feeling of fear, which seeks to 'paralyze' the opponent, who is thus determined to give up the fight. Conclusive in this direction is an example mentioned by the American professor James J. F. Forest, author of several books in the field of international security studies, who recalls the practice of the Mongol hordes that devastated Europe in the 13th century: "they deliberately spread news of the atrocities they perpetrated on cities that did not surrender." (Forest, 2001:17). Many cities fell this way.

The golden age of disinformation and propaganda, carried out as part of the war, is undoubtedly the twentieth century, with the two world conflagrations that have left their mark on contemporaneity. The development of mass media, especially the radio, facilitated, already in the First World War, the propagation of messages in order to model behaviors. Information warfare also played an essential role in World War II, with the allies' actions succeeding in tipping the balance decisively on their side.

More than ever, propaganda became the most widely used weapon during the Cold War period, supporting the ideological battle between communism and capitalism.

The magnificent triumph of the Western world did not mark also "the end of its history", as predicted by the American philosopher Francis Fukuyama in the early 1990s. Instead, after what seemed to be more of a 'short break', history continued to manifest itself in force, with new challenges, fears and answers to them.

3. THE WEAPONIZATION OF INFORMATION

Representing a way of action that has been part of the arsenal of war since ancient times, the information acquired new operational valences in the first years of the third millennium, under the auspices of an unprecedented expansion and diversification of the media. More than ever before in history, information today sustains its vital resource feature, capable of bringing about considerable change by altering the perception of targets for the intended purpose, as notedby Rand Waltzman (2015), senior information scientist at the RAND Corporation.

The new global reality, characterized by interconnectivity, social media, and real-time events, has led to the exploitation of these facilities, in a framework that reveals the aspect of instrumentalization. One of the representative facets of this situation, which marked significant development in the recent years, is the dimension highlighted by a new concept: 'the weaponization of information'.

In general terms, it refers to the act of assigning new valences to information, which is thus adapted and used as a weapon of war. Through this, an alteration of the information is made, to which the essential feature of objectivity is confiscated, necessary for correct information. According to the specialized literature (Polyakova & Boyer, 2018; Giles, 2016), the concept has evolved in close connection with Russia's actions, in the context of its support for the separatist movement in eastern Ukraine (Donbas and Luhansk), as well as the annexation of Crimea. The media coverage of these events (and not only) by the state channels in Russia revealed the subordination of the factual reality to the propaganda action, an aspect that founded the designation of these actions through the theme of 'weaponized news' (Roudakova, 2017).

In this context, 'weaponized information' means, according to a standard definition, "messages or content that is designed to affect the user's perceptions and beliefs in a way that will harm a target" (Wigmore, 2017). It is the most widely used form of 'cognitive hacking', defined as "a cyber-attack that seeks to manipulate people's perceptions by exploiting their psychological vulnerabilities" (Wigmore, 2017) (contrary to the common belief that these actions are mostly non-technical, and do not involve unauthorized access to systems or their corruption)[1].

An important contribution to the understanding of weaponized information acts on public perception is brought by the American political scientist Joseph S. Nye Jr., former chair of the National Intelligence Council and a trustee of the Center for Strategic & International Studies, a non-profit policy research organization headquartered in Washington, DC.

[1] Instead of the conventional term *cyber-attack*, which turns out to be relatively inappropriate in this context, James J. F. Forest proposes the use of *digital influence*. This action "is not about the functional integrity of a computer system"; "rather", the author points out, it aims "to use those computer systems against the target in whatever ways might benefit that attacker's objectives" (James J.F. Forest, 2001:19).

Analyzing the above-mentioned concept, the author places it in the sphere of 'sharp power' and illustrates the harmful consequences that it brings to the integrity of the information. Referring to the totalitarian regimes, Joseph S. Nye (2018) identifies Russia and China as the main actors carrying out such actions.

4. WHEN SOCIAL MEDIA GOES TO WAR

In the inventory of technological resources exploited as weaponized information, social media qualifies itself, by far, as the most used - and probably the most effective. The assessments made in this regard in the specialized literature are as clear as possible: "No technology has been weaponized at such an unprecedented global scale as social media" (*Mercy Corps*, 2019). Highlighting the implications of such actions, Catherine A. Theohary, an American specialist in National Security Policy and Information Operations, points out the following aspects:

> social media is used as a tool of information warfare - a weapon of words that influences the hearts and minds of a target audience and a weapon of mass disruption that can have effects on targets in the physical world (Theohary, 2015).

In an iconic work on the phenomenon, called *LikeWar – Weaponization of Social Media,* its authors, P. W. Singer and Emerson T. Brooking (2018), point to the fundamental change in the way war is conducted today and its consequences. They codify five fundamental principles relating to how social media is actually being weaponized: (1) 'The internet has left adolescence'; (2) 'The internet has become a battlefield'; (3) 'The battlefield changes how conflicts are fought'; (4) 'This battle changes war means' and (5) 'Were all part of this war'.

In the light of them a new paradigm is emerging: war by means of psychological influence, the path to 'supreme excellence' as Sun Tzu called it – obtaining the victory without fighting. In practice, the actions – that illustrate the manifestation of the notion of weaponization of social media - cover a wide range, highlighting the multiple possibilities of engaging in such approaches, as well as their insidious nature which makes them difficult to identify and label as such. According to Mercy Corps (2019), the well-known global non-governmental humanitarian aid organization, these manifestations can be categorized into four categories, as follows:

– *Information Operations* (IO) – 'coordinated disinformation campaigns are designed to disrupt decision making, erode social cohesion and delegitimize adversaries in the midst of interstate conflict' (Russia has carried out such actions in Syria, portraying the humanitarian organization White Helmets as a terrorist group, which has led to violent attacks against it);

– *Political Manipulation* (PM) – 'influencing news reporting, silencing dissent, undermining the integrity of democratic governance and electoral systems, and strengthening the hand of authoritarian regimes' (It is classic Russia's involvement in the US election process and the interference with Brexit);

– *Digital Hate Speech* (DGS) – 'creating opportunities for individuals and organized groups to prey on existing fears and grievances' (A tragic example is Myanmar through its violent actions against the Muslim minority);

– *Radicalization & Recruitment* – social media became 'a channel of choice for some violent extremists and militant organizations, as a means of recruitment, manipulation and coordination' (Al Quaeda has been a pioneer in this field, while these type of activities have been substantially developed later by ISIS).

Undoubtedly, it can be argued that social media has developed a fertile ground for propaganda and misinformation. By conveying fake content and conducting deceptive campaigns, the actors behind them seek to produce offline instability and violence in order to undermine democratic values and the foundations of the EU. The response to these aggressions must not be delayed.

4. SUSTAINING DEMOCRATIC RESILIENCE

The evolution of the Internet in the new space of warfare inevitably calls into question the state's ability to respond effectively to such situations.

In specialized terms, the aspects of this issue reflects the concept of resilience[2], which can be qualified, from the perspective of threats to a democratic state, as its ability to deal with them and to mitigate the crises, as Timothy D. Sisk (2017:4-5) argues in a consistent study. The author states, *ab initio,* that there is a 'complicated relationship' which is based on two essential principles, both specific to democracy: 'value resilience' and 'demand resilience'. The first refers to the so called 'in-build values' of a democratic society, which help it to act

[2] The term was originally used to refer to major changes in the environmental system. In this sense it was being associated, mainly, with the manifestation of natural disasters. In recent years, however, it has also established itself in the field of social systems, being frequently encountered in the documents of international institutions.

successfully in the challenges and crises it faces; the second claims that 'democracy is resilient because of the continuing demand for democracy'. In this context, democratic resilience designates the actions of the system

> that through its attributes of flexibility, recovery, adaptation, and innovation is capable of addressing complex challenges, and weathering and responding to the crises that affect its survival or durability, and its overall quality and performance (Sisk, 2017:4-5).

In order to properly manage the threats posed by the new dimension of war, Western states have developed significant resources in this direction, both by calibrating the actions of existing entities and by setting up new ones, dedicated exclusively to this phenomenon.

A conclusive example is provided by the US, through the Department of Defense Cyber Strategy; developed in 2018, this document introduces the concept of 'defend forward', substantiating preventive strikes in cyberspace against a foreign cyber actor (Kane, 2019:52).

Important actions has been also taken by NATO, which materialized in the establishment, in 2014, of the Strategic Communication Center of Excellence, based in Riga, Latvia. In addition, significantly and fully conclusive is the concern showed by the EU that set up, in 2015, an East European Strategic Communication Task Force with the purpose of countering Russia's misinformation campaign against it and the Member States.

Last but not least, we must mention the salutary approach of the Romanian state, which established, in May 2021, The Euro-Atlantic Center for Resilience, under the authority of the Ministry of Foreign Affairs. According to a special report prepared, in October 2021, under the auspices of the NATO Parliamentary Assembly, this new institution "is organized around three pillars: risk mitigation through anticipation and adaptation, the development of analytical tools and best practices, and cooperation in education, training and joint exercises", and it aims to facilitate "research and cooperation in the development of resilience across the Alliance" (Sanchez, 2021:15).

Through their attributions and their intended purpose, these bodies have a clear role of early warning. Acting from this perspective, they identify and label harmful manifestations carried out in the virtual space which are used in the new arsenal of war. In this context, they are, in fact, 'the first guardian of the Internet'. Ironically, their guard is determined by the very need that the freedom of this space, still largely unrestricted, is not to be exploited, and thus directed by an unseen enemy against those who hold it and can enjoy its benefits.

An absolutely necessary step forward to limit the manifestation of weaponized information in the virtual space also involves taking appropriate measures to regulate it[3]. Certainly, these must be achieved through a fair balance between freedom of expression and the preservation of the public interest, in accordance with the values of a democratic society. All of this can have some costs and will require the active participation of democratic society at large. After all, as the old saying goes, 'freedom is not for free'.

4. CONCLUSIONS

The opportunities and advantages offered by the digital age have shifted the context of the war, which today places it, to a significant extent, in the virtual space. Through its characteristics, this new form of manifestation of the war threatens the very essence of the democratic society which it aims to dispel from the shadows.

In response to these threats, Western states have begun to take significant steps to counter them effectively. Until this goal is reached, however, there seems to be enough to do.

BIBLIOGRAPHY

1. Forest, J.F. James. (2021). Political Warfare and Propaganda. An Introduction. *Journal of Advanced Military Studies*, Vol. 12, no. 1. Spring 2021. 13-33.
2. Giles, Keir. (2016). *Handbook of Russian Information Warfare*. Rome: NATO Defence/ College Research Division.
3. Ingram, J. Haroro. (2016). A Brief History of Propaganda during Conflict: Lessons for Couner-Terrorism Strategic Communications. *The International Centre for Counter-Terrorism – The Hague*. Vol. 7, no. 6. 1-47.
4. Kane, J. Nicholas. (2019). Defense against Weaponized Information: A Human Problem, Not Just A Tehnical One. *InterAgency Journal*. Vol. 10, no. 3. 46-65.
5. Nye, Joseph S. Jr. (2018). How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence. *Foreign Affairs*. 24 January.
6. Polyakova, Alina & Boyer, Spencer P. (2018). *The Future of Political Warfare; Russia, the West, and the*

[3] For example, Germany adopted in 2017 the NetzDG law "which makes social media companies with more than two million users liable for fines of up to €50 million for failure to delete 'obviously illegal' content within 24 hours of its publication" (Sanchez, 2021:13).

Coming Age of Global Digital Competition. Washington, D.C.: Brookings Institute.
7. Roudakova, N. (2017). *Losing Pravda: Ethics and The Press in Post-Truth Russia.* Cambridge: Cambridge University Press.
8. Sanchez, Linda. (2021, October). *Bolstering the Democratic Resilience of the Alliance against Desinformation and Propaganda*. Special Report (013 CDS 21 E rev.2 fin). Brussels: NATO Parliamentary Assembly.
9. Singer, P.W., Brooking, Emerson T. (2018). *LikeWar – Weaponization of Social Media.* Boston: Houghton Mifflin Harcourt.
10. Sisk, D. Timothy. (2017). *Democracy and Resilience. Conceptual Approaches and Considerations*. Stockholm: International Institute for Democracy and Electoral Assistance (IDEA).
11. Sun Tzu. (2004). *The Art of War.* Translated with introduction and notes by Lionel Gils. Leicester: Allandale Online Publishing.
12. Taylor, P. (2003). *Munitions of the Mind*: *A History of Propaganda from Ancient World to the Present Day*. Manchester: Manchester University Press.
13. Theohary, Catherine A. (2015). Information Warfare: The Role of Social Media in Conflict. *CRS Insights* [online]. Available: https://sgp.fas.org/crs/misc/IN10240.pdf [Accessed March 2022].
14. Waltzman, Rand. (2015). The Weaponization of the Information Environment. *American Foreign Policy Council Defense Technology Program Brief*. September.
15. Wigmore, Ivy. (2017). Cognitive Hacking. *Tech Target* [online]. Available: https://www.techtarget.com/whatis/definition/cognitive-hacking [Accessed March 2022].
16. ***. (2019). The Weaponization of Social Media. *Mercy Corps* [online]. Available: https://www.mercycorps.org/research-resources/weaponization-social-media [Accessed March 2022].