Information War and its Main Threats to Today's Society

Monica Delgado Hernandez[*], Heidy Rodríguez Malvarez and Ruby Solana Aguilar

Informatic science University, Cuba

[*]Corresponding Author
Monica Delgado Hernandez, Informatic science University, Cuba.

Citation: Hernandez, M. D., Malvarez, H. R., Aguilar, R. S. (2024). Information War and its Main Threats to Today's Society. *J Math Techniques Comput Math, 3*(6), 01-03.

Abstract
The information war is a multifaceted phenomenon that has become increasingly prominent in the digital era. It is characterized by the strategic use of information to influence public opinion or the behavior of an objective group. In this document we discuss the information war, its main characteristics, antecedents, influence on civil society, Fake News as part of the information war, propaganda or disinformation, as well as its procedures. They employed biographical search methods, synthesis, comparison and deduction.

Keywords: Information War, Disinformation, Deception, Hoax

1. Introduction
We live in an era where everything is interconnected. News and information are capable of reaching millions of people in less than a second. But not everything that circulates on the internet is 100% real, many times the information is used for partial or total disinformation on a topic (García, 2020).

The War of Information is present in all areas of our society and can manifest itself in many ways. Our approach is given in dar conocer como la manipulation de la información puede beneficiar a una minority y podremos conocer por que fulfills the well-known saying of Jim Morrison: "Who controls the media of information, controls the minds"

2. Content
Information and disinformation have always been used as weapons to subdue willfuls and conquer consciences. In the centuries old struggle between dominators and dominated, exploiters and exploited, the battle for ideas is an integral part of that carried out with the weapons of physical violence. This is what is also called « information war ».

The audiences considered the objective of information warfare can be civilian and military populations, their own, those of enemy nations, and neutral ones.

Information Warfare (GI) is a relatively new concept on which modern warfare is based, curiously, it is an element that since antiquity has been present in wars developed by men: "information". The latter has always been raw material in every intelligence process and all its activities are related to it.

3. Background
In reality, the information war (GI) does not appear to be very novel, because most of the elements that make it up have been applied in the history of the art of war, and as part of the psychological operations, the obtaining of information of the enemy's capabilities and intentions, the denial of information about our own capabilities and intentions, disinformation, deception, and countless activities directly related to information (Riquelme, 2012)

4. What is New Then?
First, the technological advance of today has allowed processes based on information to reach levels of efficiency never seen before.

Second, each time there is greater dependence of the military and civil systems on the technology of management and information transfer.

Third, this dependency has allowed us to identify new vulnerabilities and weaknesses, which has led to the development of new technologies and procedures to exploit them and, consequently, their countermeasures.

Fourth, the interest of the political leaders of the States to develop wars that are shorter, cheaper and with less loss of human lives.

As a consequence of the previous in the actuality, as never, the information has passed to have a tagonic role in the development of the war transforming at the same time into "resource, weapon and target" being able to even decide the destiny of a conflict before that war activities begin.

The advantage of new technologies to achieve the "superiority of information in support of the national military strategy, affecting the information and information systems of the adversary while reinforcing and protecting the information and information systems of one's own", is what has been called War of Information (Badillo, 2019) .

We can consider as a concept of War of Information: The use and management of information with the objective of obtaining a competitive advantage over an opponent.

GI activities are of offensive and defensive character:
GI's offensive activities have as their objective, both in peacetime and in war, information and information systems for civil and military use and their purpose is:
• Obtain information from the adversary without them realizing it.
• Alter or damage the information obtained and stored by the adversary with the purpose of deceiving him and making him rely on the information that he uses despite being false.
• Disinform the adversary by providing their search media with totally false information or part of true information carefully selected to achieve a specific purpose or transmitting false information in order to fulfill their objectives of overthrowing governments, even if they are democratically elected.

We will assume that disinformation is the actions or omissions through which the facts (the truth) are hidden, distorted, decontextualized or deliberately falsified for illegitimate purposes. Disinformation is carried out by two fundamental methods:
• The denial and concealment of facts (truths).
• Pseudoinformation or disclosure of false, decontextualized, distorted or irrelevant data and facts.

When we talk about massive use of disinformation, we are referring to that which is carried out by or in the interest of oligarchic groups of power, taking advantage of the power provided to them by the mass media, to the detriment of one of its three universally accepted functions: inform.

The massive use of disinformation, as a tool for the oligarchy to achieve its interests of domination, on a national or global scale, constitutes a threat to peace and a problem of international and national security.

The main arguments that sustain this investigation are the flagrant use of disinformation that is increasing and with increasingly dangerous consequences:

1. Justify and promote wars of aggression, ethnic genocides and other forms of massive violence.
2. Confuse and frighten the population with non-existent or magnified threats and risks, in what constitutes a form of terrorism.
3. Defame, demonize, attack and destabilize progressive leaders, parties, organizations, organizations and governments or those that do not respond to the interests of oligarchies.
4. Prevent knowledge of the truth about revolutionary or progressive processes or projects, and about the attacks that are committed against them.
5. Condition, promote, justify and support coups against constitutional governments.
6. Promote or justify the permanence of socioeconomic systems, politicians and models of irrational and unsustainable consumption for human society and the planet itself.
4. Physically destroy information, information-based processes and/or information systems of the adversary. This activity is quite broad since it includes everything from erasing a disk to destroying a command and control center.
5. Denial of the elements or services required to operate information-based processes and/or information systems.

The proliferation of digital tools allows the acquisition, processing and diffusion of images and sound, making it possible to modify and even create fictitious situations with a psychological effect on the objective groups that may be sufficient to generate subversion and insurgency in the population as alteration of the morale of the troops on the battlefield.

Not only the alteration of reality can be used in activities of psychological operations, subversion or insurgency. The possibilities offered by, for example, the Internet make it possible to transmit directly and simultaneously to millions of people information that governments would like to avoid. For this reason, one of the main strategies of some countries is action through Internet networks, especially when radio and television stations are interfered with.

In the modern war of information, the main battleground is in the science of the intangible. It is much more important to know what each information hides than its own contents. The contents are available to everyone, what they hide is not. It is not secret information that gives advantage, as has been traditional in wars, but rather the mastery of intangible resources that wins or loses the war.

For example, disinformation is not only in 'fake news', but in millions of messages that society digests and that moves its states of opinion, behavior, and reactions that are transformed into political, electoral, financial and financial results. economical. Knowing how to decode and analyze this 'big data' of millions of messages, is what provides the best information to design strategies for the future.

A false news or hoax is a message or news transmitted by information and communication technologies (TIC) with false or misleading and attractive content. It is normally distributed in a chain by its successive recipients due to its shocking content that seems to come from a serious and reliable source, or because the same message asks to be forwarded (Pennycook & Rand, 2021) . People who create hoaxes usually aim to melt or manipulate public opinion in society.

Basically, hoaxes or fake news can be warnings about incurable

viruses; fallacies about countries, people, institutions or companies, religious-themed messages; chains of solidarity; lucky chains; methods to become a millionaire; gifts from large companies; urban legends; etc.

5. Guidelines for Recognizing Fake News on the Internet

Some of the guidelines to recognize if certain information is fake news or not, are:
• Most of them are anonymous, they don't cite sources (because they lack the same ones) and they are not signed to avoid legal repercussions.
• They have no publication date and are written in the most temporary way possible so that they remain circulating on the Internet for as long as possible.
• Contains a hook to capture the attention of the internet user. Your success will reside in how morbid, monetary, fear-generating your hooko is and above all in the way it fits into the context of the environment.

To win the information war you must always be one step ahead. The social outbreaks that the press consider spontaneous are designed so that they only perish and hide the true objectives and strategy of those who do it. If they are not detected with advance, then it is too late. The spark has turned on. You have lost the initiative.

The information war can consist of:
• Collect tactical information,
• Confirm the veracity of the information itself,
• The distribution of propaganda or disinformation to demoralize the enemy and the public,
• Undermine the quality of enemy force information and;

• Deny opportunities to gather information to enemy forces.

6. Conclusions

The War of Information has become an omnipresent and disruptive phenomenon in contemporary society. Through the manipulation and distortion of information on digital platforms, a profound influence is exerted on public opinion and social behavior, exacerbating political polarization and undermining trust in institutions. This represents a significant threat to debilitate transparency and informed decision-making, as well as posing threats to national security and being used as a weapon in international conflicts and acts of hybrid warfare. The increasing dependence on digital technology increases vulnerabilities to manipulation and cyber attacks, underscoring the urgent need to improve digital literacy, strengthen cyber security and regulate digital platforms. Addressing these threats will require a multidimensional and collaborative response at a global level to protect the integrity of information and strengthen defenses against malicious manipulation in cyberspace [1-4].

References

1. Badillo, A. (2019). The society of disinformation: Propaganda, "fake news" and the new geopolitics of information. Working Paper, 8, 2019-14.
2. García, J. (2020). The grand manipulation: How disinformation turned Spain into a coronavirus paradise. *The Sphere of Books.*
3. Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in cognitive sciences, 25*(5), 388-402.
4. Riquelme, E. J. (2012). The influence of the information war in a theater of operations.