

Chapter 8

Strategic Impact of Disinformation Operations and the Effective Response of the Military Forces in the 21st Century*

DOI: <https://doi.org/10.25062/9786287818408.08>

Humberto Andrés Niño Vergara
Miguel Antonio González Martínez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Disinformation is a resource used at different times to undermine political and administrative stability in a society. At the operational and tactical levels, it aims to hinder military processes, especially the conduct of operations, and to push Military Intelligence to invest more effort in processing information for decision-making. The methods used include spreading out-of-context information, fake news, and targeting computer assets through cyber operations. Due to its varied effects, it must be analyzed based on its impact at each level of the Military Forces to develop an effective strategy. Ultimately, the Military Forces need doctrinal foundations supported by an organizational structure capable of managing disinformation according to its impact at each level.

Keywords: disinformation; doctrine; Colombian National Army; Special Forces; new wars.

* This chapter results from the research project "Nature of Contemporary Warfare. Challenges and Opportunities for Special Forces and Intelligence" conducted by the Army Department of Escuela Superior de Guerra. It is part of the research strand "Nature of War, Terrorism, New Threats" of the Centro de Gravedad research group, which is categorized as A under code COL0104976. The views expressed are those of the authors and do not necessarily reflect those of the participating institutions.

Humberto Andrés Niño Vergara

Lieutenant Colonel in the Colombian National Army. Master's degree in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Bachelor's in Business Administration, Universidad Militar Nueva Granada, Colombia. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: humberto.nino@buzonejercito.mil.co

Miguel Antonio González Martínez

PhD candidate in Strategic, Security, and Defense Studies, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Master's in History, Universidad Nacional de Colombia. Bachelor's in International Relations and Political Studies, Universidad Militar Nueva Granada, Colombia. Professor and researcher, Army Department, Escuela Superior de Guerra "General Rafael Reyes Prieto," and professor of the International Relations and Political Studies Program (FAEDIS), Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0002-6034-912X> - Email: miguel.gonzalez@esdeg.edu.co

APA Citation: Niño Vergara, H. A., & González Martínez, M. A. (2025). Strategic Impact of Disinformation Operations and the Effective Response of the Military Forces in the 21st Century. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 171-188). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818408.08>

COMMANDOS: CHALLENGES FACING SPECIAL FORCES AND INTELLIGENCE IN CONTEMPORARY WARFARE

Print ISBN: 978-628-7818-39-2

Digital ISBN: 978-628-7818-40-8

DOI: <https://doi.org/10.25062/9786287818408>

Security and Defense Collection

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introduction

Disinformation has emerged as a significant phenomenon in contemporary conflicts, impacting the social and political structures. These actions promote the achievement of political objectives and create a space for the convergence of various factors that threaten state power, the monopoly of force, government stability, and the rule of law.

This chapter analyzes three fundamental aspects that structure the common thread of this work. First, the concept and theory of disinformation operations, along with their strategic impact at the international level. Second, the role of the Military Forces in addressing disinformation operations is analyzed, either to prevent their emergence or mitigate their strategic impact. Finally, the operational foundations for the Special Forces (SF) in addressing disinformation operations are examined.

Throughout this chapter, doctrinal concepts will be explored that enable the SF in Colombia to understand the context in which illegal armed groups launch disinformation operations, thereby facilitating an official, legitimate, effective, and timely response. This seeks to determine the responsibility or role that the SF should play in maintaining constitutional order and defending the State, following the influence of other actors seeking to destabilize it.

Methodologically, a qualitative research study was conducted, using primary sources from available documents. According to Hernández Sampieri et al. (2010), there are various subjective realities, which vary in form and content among individuals, groups, and cultures. Therefore, the qualitative researcher begins with the premise that the social world is “relative” and can only be understood from the perspective of the actors being studied. In other words, the world is constructed by the researcher (Hernández et al., 2010, p. 11).

This methodological perspective fits with the theory to the extent that the chapter engages with the contemporary world of the postmodern era, whose agenda proposes demystifying the discourses (scientific, artistic, and cultural) of modernity that shaped and built present reality, while also taking a critical stance toward the scientific positivism of the 19th century. Undoubtedly, Ferdinand de Saussure's *Course in General Linguistics* (1919) marked a significant foray into linguistics, opening a new interpretive perspective on understanding cultural events and social facts. Thus, many researchers adopted structuralism as the theoretical framework for their research, influenced by the French linguist Ferdinand de Saussure's theory of the *linguistic sign*. Later, Jacques Derrida incorporated the notion of the "deconstruction" of discourses, thereby reinforcing the struggle for truth—for legitimate discourse based on the locus of enunciation from which it emerges.

With these new intertextual readings of reality, coupled with the phenomenon of globalization and its intensification with the widespread use of the internet, the path has been paved toward free interpretation in communication, and even the incorporation of neologisms such as *post-truth*, which ultimately brings to the forefront the desire to fight for truth in an increasingly volatile, complex, uncertain, and ambiguous world.

Disinformation

Disinformation refers to activities aimed at spreading false information, misleading, and even deceiving the audience. In the modern world, globalization and the rise of information and communications technologies (ICT) have amplified these activities. These technologies make it easier to access and share information, but this also makes it harder to control. Social media platforms like Facebook, Twitter—now X, TikTok, WhatsApp, and others—play a key role in this phenomenon because, in recent years, internet access has become more widespread. This allows the public to quickly share ideas, thoughts, emotions, reactions, and more, on a large scale and in real time, often without effective filters to verify the truth or determine if the sources are reliable, such as bots—computer programs that mimic human behavior. Therefore, in the context of postmodernism, a paradoxical situation is emerging: amid the information age, disinformation is growing rapidly because it exploits broad audiences across different sectors. They receive messages quickly, spread material at very low cost, and do so with ease that bypasses the need for truthfulness.

Sociologically, the spread and acceptance of disinformation can be explained by a person's need to reaffirm their identity, viewing the content as a reflection of their own thinking without considering its source or accuracy. This behavior can be reinforced by cognitive biases of the message recipient; for example, if someone favors a particular political movement, they are more likely to believe news that supports their existing beliefs without critical evaluation.

This "technological revolution" in the field of information has affected various aspects of public life, including culture, the economy, and politics. Disinformation influences all kinds of emotions, which can lead to political actions and social movements. The military is no exception to this trend, as it performs a key function of the State—its defense and security—and is always at risk of being targeted by disinformation campaigns aimed at destabilizing society and harming the government. Therefore, security forces must establish information security measures to protect official systems and counter messages that threaten the institutional order.

This scenario has led to a shift in deployment strategies toward a vision of official institutions where, specifically, information is one of the key pillars (Sierra, 2003). Like natural resources, the environment, and people, information can be seen as a strategic asset for States, since poor management of disinformation can result in high political, economic, and social costs, among others.

A precedent for the effects that disinformation can have is found in the Cold War, when the two dominant powers of the international system used every possible means to contain the advance of the opposing system, amidst the ideological struggle between capitalism and communism. At that time, the propaganda efforts of both sides from World War II already existed to justify and promote, in the eyes of the public, political and military actions within the war framework. The rise and widespread use of media, such as the press, radio, and cinema, played a pivotal role in mobilizing support against opposing sides.

In the 1950s, disinformation tactics became an official element, with specialized agencies aimed at discrediting the United States and its allies to benefit global communism. As a result, Americans developed strategies to counter the USSR's attacks, adjusting their foreign policy to address the influence of information on allied nations, the USSR's ability to sway opponents, and the use of force. This led to the creation of the Office of Strategic Defense, whose goal was to develop disinformation tactics in the country's international relations (Rodríguez, 2017).

In short, disinformation seeks to destabilize a country by damaging the recognition and reputation of official institutions through spreading messages that

incite hate and/or fear. At present, one of the nations that has most employed this strategy is Russia, whose involvement has become more pronounced based on:

- Carrying out malicious operations on social media.
- Spreading disinformation through traditional dissemination methods such as radio and television.
- Influencing public opinion to get allies who will support their stance and promote their ideas against the adversary. For this purpose, they have mainly used conferences.
- Conducting cyber operations to damage the perception of the media.
- Hacking and disclosing information (U.S. Department of State, 2022b).

Similarly, when investigating what information Russia has tried to position, the following was found:

- Russia, for example, in the conflict with Ukraine, acts driven by the perception of victimization of its adversary.
- Returning to historical events to stigmatize its opponents or highlight its past heroic actions.
- Criticizing Western culture to create uncertainty.
- Attacking popular movements and other forms of dissent as acts of influence orchestrated by its military and political enemies.
- Constructing realities that favor its position, causing confusion and demoralizing the adversary (U.S. Department of State, 2022b).

The goal is not only to safeguard information related to official data, financial networks, and platforms that support the operations of both the public and private sectors, but also to prevent other cybercrimes. Additionally, it aims to counter potential psychological warfare tactics and influence society. The internet serves as a resource for both information and disinformation, as it enables information to be filtered at high speeds, while also facilitating disinformation campaigns targeting specific audiences (Sierra, 2003).

This scenario creates an *information war* that involves actions aimed at establishing and maintaining information superiority while protecting one's own systems. Currently, this type of war features a wide range of strategies due to the technological revolution, which introduces new threats. As different groups and official entities can acquire the means to impact the reputation and stability of information, and even steal, delete, modify, or spy on it (López, 2007).

This information war promotes a concept of warfare that does not rely on traditional weapons and becomes a common form of threat in hybrid warfare. In this scenario, various economic, political, diplomatic, and other tools are used to weaken the enemy's confidence, create negative social conditions to provoke violent protests, disrupt government responses by making their systems fragile, and justify the use of force or consider it necessary (LISA Institute, 2019). Therefore, disinformation operations become a form of hybrid threat and can trigger conventional conflict. Ultimately, their goal is to influence a political opponent.

This hybrid threat is closely linked to constant war propaganda in publications that aim to mobilize people and discredit the opponent. Clearly, war propaganda, like information, has evolved with the progress of information technology (Noguera, 2013), which is why the same tactics are still used: spreading false strategies and exploiting public trust. In short, it involves using malicious operations, disinformation, and other methods to destabilize the enemy (Medina, 2022).

As we have seen, disinformation consists of strategies aimed at benefiting oneself while harming an opponent. In this context, the information provided already has a specific purpose, which is why it is distorted (Ustarroz, 2021). Other authors describe disinformation as false or manipulated information spread with malicious intent. This includes fake news and false stories (Rini, 2017).

Disinformation is often accompanied by sensationalist messages that reach a wide audience and have a significant social impact. Sometimes, it also includes images that evoke a strong psychological response, eliciting feelings of fear, hatred, rejection, approval, or exaltation, depending on the goal of the operation. This approach has been used since the era of radio, and its effectiveness led to the term 'infodemic' being coined (Arteaga, 2020). Its aim, beyond military victory, is to gain political power by exploiting the range of emotions it stirs in people. This strategy has been widely employed by the Russians, who try to leverage the spread of fake news and manipulated information to promote their worldview, weaken their enemies, achieve their goals, and justify their military actions (U.S. Department of State, 2021).

In any case, the goal of disinformation is to promote certain beliefs, political positions, images, and recognition of a political figure, or sometimes to influence an opponent's perception through the spread of information. Information warfare relies on humanity's primal instincts, which trigger a pattern of organized violence (Contreras, 2001).

The impact of these operations is strategic because they create social disruption by playing on humanity's fears. One method is to evoke disgust

against the enemy for violating human rights or breaking social norms. These disinformation campaigns even produce completely false content to stir up revulsion (U.S. Department of State, 2022a).

Furthermore, one factor that makes this kind of hybrid threat so effective is that the attackers stay anonymous, making it hard to identify the source of the threats (Arteaga, 2020). This is a key part of Russian doctrine, which relies on a psychopolitical warfare called *maskirovka*, or *маскировка* in Russian, seen as essential. This aims to deceive the enemy through concealment, simulation, and spreading fake news. Therefore, “*maskirovka* practices on a military level include [...] language manipulation [...] for instance, the word ‘offensive’ has completely disappeared from the Soviet military vocabulary and has been replaced with euphemisms like *movement*, *exit*, or *defense*” (Antoine, 2019, p. 21).

Disinformation not only affects the audience by influencing their emotions and feelings related to their social values and fears, but it is also characterized by its uncertain origin, intention, and impact, making it a powerful tool internationally. It is unclear who is providing the information, whether all the data is false or, instead, misrepresented, whether it was taken out of context of what actually happened, or whether it is being manipulated to serve a particular political interest (Arteaga, 2020).

Typically, when sharing any kind of information, the challenge is ensuring the message is received as intended and for the purpose it was originally meant. In military settings, this becomes even more critical, as uncertainty, discrepancies, or misunderstandings can impair decision-making and weaken the ability to respond effectively (Guzmán, 2019).

Two concepts initially converge on this point: fake news and malicious operations. Specifically, fake news refers to news that can be proven false, but it does not necessarily imply malicious intent, as it can also result from a poorly communicated message, an error in the source of the information, or other factors. Unlike disinformation operations, fake news is presented randomly and almost by chance, whereas disinformation is calculated against a specific group and involves conscious efforts (Paladino et al., 2021).

Besides fake news, there are six other types of disinformation: 1) satire or parody; 2) false connections to easy-to-understand content; 3) misleading content, which combines lies with truthful facts; 4) false context, which involves events presented in a way unrelated to reality; 5) imposter content, aimed at deceiving the audience to steal information or gain an advantage; and 6) manipulated content, which, as the name suggests, is designed to influence or sway viewers in favor of the disinformers (Doble Check, 2020).

One of the measures the United States has implemented to combat disinformation operations and safeguard itself from false news is to disseminate it through official media outlets, along with corresponding corrections or fact-checks, as shown on the Department of State website. In Colombia, a key initiative is the VERA campaign, promoted by Asomedios, where the country's leading radio stations broadcast brief messages aimed at debunking fake news that has gone viral across various media outlets.

But, how effective can this measure be regarding the speed at which disinformation operations achieve their goals? The truth is that this remains uncertain; nonetheless, the effort to implement strong responses to lessen the harmful effects of disinformation is valued. Besides these efforts by trained personnel to screen information before publication, it is essential to promote a civic culture to stop the spread of disinformation, along with coordinated, interagency collaboration to more effectively identify misleading content, prevent its dissemination, and counter it by debunking the deception.

Another recent example was the public health crisis caused by COVID-19. To address its impacts, various governments, international organizations, and the private sector launched campaigns to promote vaccination and combat misinformation. In this context, the European Union based its major efforts against disinformation on the belief that effective management of the public health crisis would be directly related to the number of deaths from the disease (European Commission, 2021).

Disinformation is a coordinated phenomenon that involves planning and logistics to ensure the spread of the intended message, along with the pursuit of a specific objective. Additionally, disinformation serves as a weapon used against an adversary to undermine its credibility, legitimacy, and stability, and to influence thoughts, emotions, and actions either against the enemy or in support of the person creating the disinformation strategy (Rodríguez, 2017).

Besides the strategic impact discussed so far, disinformation is a global industry operating in over 48 countries. Various actors, unaware of the ultimate goal of disinformation, contribute to this threat's chain (Levy, 2021).

Therefore, the European Commission has introduced an action plan to combat disinformation, outlining specific measures to address it. First, it is essential to enhance the ability to detect, analyze, and expose disinformation campaigns. This involves strengthening technology that can monitor, prevent, and identify the source of fake news or disinformation, as well as enabling quick responses to stop the spread of such content.

Second, it is essential to strengthen the response efforts of both the private and public sectors as a whole. Finally, and in line with the above, the private sector must be mobilized to raise public awareness about the effects of disinformation and improve the ability to adapt, learn, and discard manipulated information (European Commission, 2018).

Having analyzed the concepts related to disinformation, the challenges faced by the Military Forces in countering disinformation operations in national security and defense are outlined below. To achieve this, Colombian military doctrine is examined, and some concepts are proposed that clarify how the capabilities of the Military Forces should be directed to maintain an offensive and defensive advantage in disinformation operations.

Military Forces Strategy in the Face of Disinformation

Information warfare has created a unique intangible value within armies, rooted in power and knowledge. The primary strategy has been for armies to establish security and defense measures for their intangible assets, including programs to detect, control, and prevent the intrusion and theft of their most sensitive information (Sierra, 2003).

Based on the above, information operations are conducted to enhance the Force's ability to protect its information assets, while using disinformation as a strategy to its advantage. Actions include sabotaging the enemy's computer and technological systems to make them unusable, disrupting the flow of information, lowering their combat morale and/or their command and control systems; denying access to sensitive information; creating deception among the audience about the enemy; gathering intelligence about the enemy or planting false messages against it; influencing bystanders to promote favorable behavior for the Force; and early detection of intrusions into official computer systems (Andrade et al., 2011).

Information operations, which can help deter adversaries at no cost in warfare, are grouped into attack, defense, and electronic support (Clark, 2010). In this way, public value is provided to various sectors of society, helping to safeguard different aspects of public and private life, such as financial information.

After analyzing disinformation as a strategy against States, it is now crucial to examine the roadmap for the Military Forces in response to this escalating threat. On one hand, the forces must work to protect themselves from these operations,

and on the other, they must develop military strategies to control the spread of disinformation that could undermine their legitimacy, the legitimacy of the State overall, and the institutional order. Achieving this goal requires the involvement of all operational levels within the security force.

When we talk about the strategic level, we refer to the group of people and tangible and intangible resources available to support command decision-making. At this level, senior commanders plan the methods and resources to be provided to the combat Army, including the timing, sources, and quality standards. They also act as a conduit for establishing a direct relationship with the Central Government, promoting the achievement of national objectives by organizing institutions accordingly, and following the strategy of the President as Commander-in-Chief of the Military Forces.

At the operational level, the information, means, and resources conceived and executed at the strategic level are received and used to implement operational plans created at this level, ensuring operational effectiveness. Finally, tactical units carry out the operational plans provided by the operational level. Commanders at the tactical level utilize the personnel, means, and resources needed to conduct missions and complete tasks.

Operational Fundamentals for Special Forces against Disinformation Operations

Once the conceptual and theoretical framework of disinformation operations is analyzed, it becomes possible to establish guidelines that can demonstrate the direction in which operational foundations should be built to address disinformation.

When analyzing disinformation from a comprehensive perspective based on the functions, capabilities, and scope of the three levels of security forces, it becomes clear that at the strategic level, measures are necessary to reduce the impact of disinformation operations, especially when these threats threaten the institutional reputation and political and administrative stability. Likewise, planning for material and intangible resources is essential to train and equip personnel with the latest technologies to identify sources of information, the origin of fake news or cyberattacks, and to protect official databases and other related tactics.

At the operational level, intelligence is collected to identify and analyze the adversary across all areas, capabilities, techniques, and tactics (Guzmán, 2019), as well as to coordinate efforts for gathering information at the tactical level. In

this context, tactics are necessary to determine whether the information obtained is accurate and free from an intent to confuse or deceive the Force, or to obstruct decision-making processes.

The challenge at this stage is managing uncertainty, because, unlike at the strategic level, where efforts mainly aim to influence the institutional image or the legitimacy of the Government, disinformation now has the power to affect decision-making and operational success. Thus, receiving false or manipulated information compromises the integrity of the troops and the Force's ability to attain the desired operational results (Guzmán, 2019).

At the tactical level, human intelligence and other information-gathering techniques are essential processes that require thorough training in skills to identify information sources, evaluate their quality, and assess potential consequences. Similarly, information operations must be used as a deterrent against the enemy. In this context, disinformation creates the appropriate conditions to generate a strategic impact for a limited time, which matches the duration of institutional weaknesses, causing instability due to disinformation (Guzmán, 2019).

An example of this is military information support operations, a capability of the SF that spans all three levels of the Force. These operations aim to analyze and address psychological strategies in the operational arena, while also supporting the institution's information activities in coordination with other entities and national civilian authorities, among others (Ejército Nacional de Colombia, 2017).

To protect the Force during operations, the SF can and must support information security through technological tools and cyber capabilities, within their authority and in the performance of their duties. This condition is fundamental, as it aims to safeguard this action in defense of sovereignty and independence.

This is outlined in the United States Joint Publication ADP 3-13 on Information Operations, which states that military operations in the information domain must use electronic warfare, computer network operations, psychological operations, military deception tactics, and operational security in an integrated way. The goal is to influence the adversary's processes and decisions while safeguarding one's own functions (Department of the Army, 2023).

Furthermore, it notes that conducting any military operation requires support processes to accomplish the mission and assigned tasks. In this context, support is necessary to ensure information security, physical security, prevent or anticipate physical attacks, and develop counterintelligence operations and combat camera systems (Joint Chiefs of Staff, 2006).

From another perspective, information operations require enhancing civil-military relations and military diplomacy to, on one hand, gather accurate information and strengthen ties with the civilian population, and on the other, support intelligence functions and promote the conduct of operations with accurate information that reduces the inherent risk to military forces (Joint Chiefs of Staff, 2006).

In the case of Colombia, all these strategies must align with the Intelligence Law and other national and international regulations that govern the actions of security forces. Furthermore, information operations should become the foundation of any military operation, considering that disinformation is a subtle yet highly effective tool for adversaries to disrupt decision-making, hinder operational success, gain an advantage in the theater of operations, and influence audiences.

Therefore, there is a need for support, which involves the ability to collect, store, and manage information in real-time with accuracy and relevance. It also seeks opportunities to gather available, easily understandable, and concise information (Joint Chiefs of Staff, 2006). This information will provide the command with the necessary data for decision-making, so it requires a specific security scheme to protect the lives of troops, strategic assets, infrastructure, and other material and non-material resources of the Colombian State, thereby defending sovereignty, independence, territorial integrity, and the constitutional order.

Specifically, combat cameras are a vital part of the Military Forces because they address a series of psychological operations that challenge the actions of institutions to uphold the rule of law and national order. They serve as a tool to showcase the Force's efforts, including its support for civilians, its response to various disaster risks and emergencies, the execution of military operations to establish stable peace, and the dismantling of criminal networks that threaten communities.

Furthermore, through combat cameras, the nation witnesses the Force's intervention, the use of techniques and tactics protected by national and international regulations, as well as the principles and values characteristic of military culture. In this regard, mechanisms are put in place to safeguard the institutional image and serve as legal protection against allegations of actions by the security forces.

Regarding fake news or content manipulation, it is crucial to have a department or unit that, from a strategic level at the headquarters of the security forces and even from the General Command of the Military Forces (CGFM), directly provides accurate and factual information to the media. This helps protect institutional legitimacy and supports the defense of the constitutional order and social values.

However, the relationship is cyclical and interdependent, since a good image and reputation are necessary for the media—mainly from the private sector and sometimes independent of any government or public authority—to trust the content directly broadcast by the Military Forces.

Similarly, it is essential to establish how to handle crisis situations that threaten the credibility of the Military Forces. Such situations may directly impact institutions or lead to the spread of false or malicious messages that cause fear and uncertainty about national security and defense. An example might be an attack by an illegal group or an invasion by another country. This type of content should also be incorporated into the operational concept of the SF, which is designed to counter disinformation operations.

Conclusions

Disinformation targets various levels of the Military Forces by disrupting their processes, hindering decision-making, and damaging the institutional image. These attacks include delivering, publishing, or using false information to portray the adversary, which hampers operational planning and the integrity of Force members. Likewise, the legitimacy of official databases, institutions, and political and administrative stability is undermined.

Because of this, each level of the Force has specific tasks related to its capabilities to counter disinformation. Primarily, there is a focus on enhancing the skills of the Intelligence branch, both in gathering information for military operations and in identifying illegal groups and their methods. Additionally, cyber defense mechanisms must be strengthened, and initiatives should be created to protect the institutional image in support of strategic communications.

Faced with this, ICTs have created audiences that receive and send messages at an incredible pace. These audiences, sometimes because they are unaware of the published topics, may develop political loyalty naturally or in response to certain stimuli. This can lead to a clash between factions, questions about the legitimacy of institutions, and other behaviors that impact the political and administrative stability of governments.

In this context, SF units capable of defending against cyberattacks are essential to protect information vital for decision-making and the development of military operations. Similarly, they must safeguard audiovisual data that could be taken out of context to carry out disinformation campaigns against law enforcement.

From another perspective, special operations are needed to identify the source or origin of false or misleading news intended to disrupt the nation's political and administrative stability.

In any case, the primary source of disinformation spreads or publishes it with the goal of influencing the adversary and garnering political support that rejects the opponent's beliefs, positions, and/or actions. The media that use these tactics rely on manipulating the masses, targeting their belief systems and undermining their social values to provoke an ideal violent response.

This phenomenon causes events that destabilize the political and administrative system, enabling the source of disinformation to achieve its political goals. The impact can be so significant that it may even lead to the collapse of an institution, entity, or government. Clearly, this level of instability puts States at risk.

In this respect, these challenges create a new area of expertise for the defense and security sector, which must develop strategies to manage the strategic impact of disinformation operations and prevent their occurrence. To achieve this, they must enhance their technological systems, improve the Force's capabilities in manipulating technological tools and information, and adopt technologies that enable them to respond as effectively as possible.

Initially, the SF must be established with operational foundations to safeguard sensitive information of state entities. Similarly, they must verify the accuracy of information by creating content that opposes disinformation operations, for which they must continuously give the media opportunities to collect firsthand information. Additionally, they must develop strategies to prevent and contain the spread of incomplete, false, and malicious information.

As a complement to analyzing armies that have engaged in conflicts with other countries—such as the United States, which has developed a functional doctrine and implemented support capabilities for various military operations—distinct tasks must be created for the Colombian SF. These tasks should aim to maximize physical attacks on the enemy's morale, enabling better synchronization of disinformation operations planning.

References

- Andrade, W., Martínez, J. F., & Pineda, J. C. (2011). *Las operaciones de información en las guerras de información* [Specialization capstone, Universidad Piloto de Colombia]. Repositorio UNIPILOTO. <https://tinyurl.com/3f7vpwer>
- Antoine, F. (2019). Desinformación y "maskirovka" en la guerra psicopolítica soviética: el caso afgano. *Política Revista de Ciencia Política*, (December), 129–137. <https://tinyurl.com/d8wxjc43>
- Arteaga, M. (2020a). El conflicto híbrido, una contribución para la incertidumbre. In Academia de Guerra del Ejército de Chile (Ed.), *El conflicto híbrido y sus efectos en la conducción operacional y táctica* (pp. 19–43). Centro de Estudios Estratégicos CEEAG. <https://tinyurl.com/2rbbvrfx>
- Clark, B. (2010). Las operaciones de información como elemento disuasivo para el conflicto armado. *Military Review*, (September–October), 2–11. <https://tinyurl.com/3nt9b794>
- Contreras, F. (2001). La muerte del soldado: hacia la deshumanización de las tecnologías de guerra. In F. Contreras & F. Sierra, *Culturas de guerra: Medios de información y violencia simbólica* (pp. 275–308). Cátedra.
- Department of the Army. (2023). *ADP 3-13 Information*. <https://tinyurl.com/4bjc5n52>
- Doble Check. (2020). Fake news y otras 6 formas de desinformación [Video]. *YouTube*. https://www.youtube.com/watch?v=ZllaBk_8J2o
- Ejército Nacional de Colombia. (2017). *Manual Fundamental de Referencia del Ejército MFRE 3-05 Operaciones Especiales [Public]*. Imprenta Ejército. <https://tinyurl.com/32dbw83e>
- European Commission. (2018). *The 2022 Code of Practice on Disinformation*. <https://tinyurl.com/4evc6mhe>
- European Commission. (2021). *Fighting disinformation*. https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en
- Guzmán, A. (2019). La desinformación estratégica como recurso disuasivo durante la crisis. *Revista Ensayos Militares*, 5(2), 99–114. <https://tinyurl.com/44vvcmt>
- Hernández Sampieri, R., Fernández, C., & Baptista, L. (2010). *Metodología de la investigación* (5th ed.). McGraw-Hill.
- Levy, G. (2021, August 10). *La creciente industria de la desinformación*. <https://tinyurl.com/y3dts9av>
- LISA Institute. (2019, May 20). *Qué es la guerra híbrida y cómo nos afectan las amenazas híbridas*. <https://tinyurl.com/258439er>
- López, C. (2007). La guerra informática. *Boletín del Centro Naval*, (817), 219–224. <https://tinyurl.com/bdcrauey>
- Medina, A. (2022, January 28). ¿Qué es la guerra híbrida? La estrategia de Rusia contra Ucrania. *El Debate*. <https://tinyurl.com/mtv564bt>

- Noguera, A. (2013). *Propaganda de guerra, una estrategia adaptada al conflicto colombiano: Análisis de la propaganda de guerra empleada por Uribe y Santos para combatir los grupos guerrilleros* [Bachelor's thesis, Pontificia Universidad Javeriana]. Repositorio PUJ. <https://tinyurl.com/mzvtn43>
- Paladino, A., Villalba, M., & Miguel, M. (2021). Entrevista a Martín Alfredo Becerra: Desinformación, fake news y posverdad. *Palabra Clave*, 10(2), e133. <https://doi.org/10.24215/18539912e133>
- Rini, R. (2017). Fake news and partisan epistemology. *Kennedy Institute of Ethics Journal*, 27(S2), 43–64. <https://doi.org/10.1353/ken.2017.0025>
- Rodríguez, A. (2017). Fundamentos del concepto de desinformación como práctica manipuladora en la comunicación política y las relaciones internacionales. *Historia y Comunicación Social*, 23(1), 231–244. <https://tinyurl.com/ykxyu2yz>
- Sierra, F. (2003). La guerra en la era de la información: propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación. *Sphera Publica*, (3), 253–268. <https://tinyurl.com/4bk6c97h>
- U. S. Department of State. (2021, June 7). The extraordinary scope and breadth of Russian propaganda and disinformation [*Global Engagement Center Counter-Disinformation Dispatches*, No. 10]. <https://tinyurl.com/3239wjvr>
- U. S. Department of State. (2022a, January 13). Exploiting primal fears [*Global Engagement Center Counter-Disinformation Dispatches*, No. 13]. <https://tinyurl.com/2mysnc4w>
- U. S. Department of State. (2022b, January 20). *Las cinco principales narrativas de desinformación en las que insiste Rusia*. <https://tinyurl.com/navpzd67>
- Ustarroz, M. (2021). *Del fenómeno de la desinformación: Marco conceptual y análisis comparativo del marco legal en la Unión Europea* [Master's thesis, Universidad de Barcelona]. Repositorio UB. <https://tinyurl.com/zbdcyunr>