

Chapter 5

Special Forces Operations against Threat Systems based on Political and Information Warfare*

DOI: <https://doi.org/10.25062/9786287818408.05>

Oscar Mauricio Bernal Vallarino
Ilmar Ubiratan Salgado Luzia

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Political and information warfare are not new phenomena, but they have been better identified and defined in the 20th century, where they have gained relevance as means used by state and non-state actors. Their main advantage is the ability to influence operational environments, counter adversaries, and achieve objectives without a formal declaration of war. In this context, various countries around the world have developed Special Forces doctrines to operate in areas where special warfare and information operations are widely used to gain the support of populations, train friendly forces, and weaken the enemy. This chapter analyzes the role of the Colombian Special Forces, as defined by their doctrine and capabilities, within a strategy for operating in an environment where political and information warfare are present.

Keywords: strategy; information warfare; special warfare; political warfare; special operations.

* 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.

Oscar Mauricio Bernal Vallarino

Lieutenant Colonel in the Colombian National Army Special Forces. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Military Resources Administration, National Army Arms and Services College. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Bachelor's in Business Administration, Universidad Politécnico Grancolombiano. Email: oscar.bernalva@buzonejercito.mil.co

Ilmar Ubiratan Salgado Luzia

Retired Lieutenant Colonel of the Brazilian Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Graduate degrees in Military Operations, Escola de Aperfeiçoamento de Oficiais; Military Sciences, Army Command and Staff College; and Intelligence, Army Intelligence College. Bachelor of Military Sciences, Academia Militar das Agulhas Negras, Resende, Brazil.

<https://orcid.org/0000-0002-7680-916X> - Email: ubiratan.ilm@eb.mil.br

APA Citation: Bernal Vallarino, O. M., & Salgado Luzia, I. U. (2025). Special Forces Operations against Threat Systems based on Political and Information Warfare. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 105-128). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818408.05>

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

The genuine interest in the war helped open besieged roads. In this regard, it must be established that many of the world's borders have been drawn through major armed conflicts over territorial disputes, a fact rooted in nationalism, which, through irrational discourses, massifies the individual and places the common good above the individual.

Colombia has been subjected for more than half a century to excessive violence inflicted by Marxist insurgent groups, who have consolidated their position in the country based on a radical discourse. Consequently, the country has been stigmatized by a world-renowned internal conflict.

Decades have passed, and social dynamics and technologies have evolved, while the conflict and its actors have adapted to the conditions of the new millennium. In this context, the significance of the informational dimension has grown, as digital technologies have created new tools to influence opinions and employ them in warfare.

To understand this phenomenon and apply it to Colombia's reality, it is important to revisit the concepts of *political warfare*, developed by American defense doctrine during the Cold War, and *information warfare*, a term that appeared in that doctrine in the 1990s.

This chapter analyzes whether illegal armed groups and their supporters have developed political warfare and information warfare in Colombia, primarily in the last decade.

Thus, it seeks to answer this guiding question: What are the challenges and opportunities for the Special Forces Division (DIVFE) of the Colombian National Army in the face of threat systems based on political warfare and information warfare?

To accomplish this objective, the chapter is divided into three sections with specific objectives: to examine the use of political warfare and information warfare by threats; to correlate the new requirements of threat systems based on political warfare and information warfare using DIVFE; and to analyze the operational and strategic scope of DIVFE in the face of threat systems based on political warfare and information warfare.

Use of Political Warfare and Information Warfare by Threats

This section analyzes the use of political warfare and information warfare strategies in response to threats. To do so, it is important to understand that the concept of political warfare is broader and encompasses a range of actions, including those carried out in the context of information warfare. In other words, information warfare is a concept within the spectrum of political warfare.

Political Warfare

The more one investigates the concept of political warfare, the more difficult it becomes to define a dividing line between politics and war. In the 19th century, Clausewitz argued that war constituted the continuation of politics by other means. In the mid-20th century, the American diplomat George Kennan defined political warfare as the practice of Clausewitz's military doctrine in times of peace.

In more detail, Kennan argued in 1948 that political warfare could be defined as the use of all means at a nation's disposal, except war, to achieve its national objectives. From this reflection, the term came to be used to describe the American strategy applied during the Cold War to counter the advance of communism worldwide. Strategies range from overt actions, such as economic measures, political alliances, and "white" propaganda, to covert actions, such as clandestine support for friendly groups abroad, "black" psychological warfare, and the promotion of popular resistance in hostile States (N. Rodríguez, 2019). Later, in a 1985 article, Kennan stated: "Excessive secrecy, duplicity, and clandestine actions are simply not our cup of tea, since such operations conflict with our own traditional norms and compromise our diplomacy in other areas" (Lucas & Mistry, 2009, p. 45).

Such a reflection on the rise of U.S. foreign policy between 1946 and 1950 raises ethical questions and potential diplomatic disadvantages in applying the

term Kennan proposed. However, the concept and its applicability became so effective that the American diplomat's subsequent analyses were disregarded (Lucas & Mistry, 2009).

From Kennan's definition, it is clear that political warfare has always existed, as all countries have sought, in one way or another, to shape other States' policies toward positions favorable to their objectives (Lucas & Mistry, 2009). Throughout history, countless examples of overt, covert, or mixed actions can be found. From the Trojan horse to cyberattacks, history offers countless examples of interference in different forms (N. Rodríguez, 2019).

A detailed analysis of the nature of covert actions reveals that they serve to prevent a military escalation that could have disastrous consequences. The countries that practice them have decided that it is better to adopt the assumptions of political realism and take proactive measures. Political realism has made political warfare the ideal instrument for waging war, with unorthodox strategies, without direct confrontation (N. Rodríguez, 2019).

George Kennan inspired the American program to contain Soviet expansionism with his concept of political warfare. The program proposed economic and political measures to counter the Soviet sphere, including the enhancement of timely, affirmative operations in psychological and economic warfare to support and encourage unrest and subversion in countries that possessed strategic satellites. The government delegated responsibility for carrying out covert actions to the U.S. Central Intelligence Agency (CIA) (N. Rodríguez, 2019).

Since then, the CIA has perfected the tactics and techniques of political warfare. For example, its campaign in Chile lasted more than a decade, during which covert actions funded political parties and media propaganda, in addition to openly promoting military coups. In other cases, such as the coup in Iran or the numerous operations in Syria, they have carried out similar activities. It is difficult to find an international event of significance in which the CIA has not participated in some capacity. Its actions demonstrate that implementing political warfare is not simple, as public diplomacy must be synchronized with covert and clandestine operations (those conducted without informing Congress). Political warfare disseminates white, gray, and black propaganda, creates alliances with dissidents, and promotes subversive actions (N. Rodríguez, 2019).

China has been another clear example of the use of a political warfare strategy. For China, political warfare, which it calls *unrestricted warfare*, is an all-encompassing form of war fundamental to its security strategy and foreign

policy. Thus, this strategy represents for the Chinese an alternative to violent warfare, which seeks to influence the emotions, motives, objective reasoning, and behavior of governments, organizations, individuals, and groups in a manner more favorable to their own political, military, and economic objectives. China's political warfare goes beyond the traditional united front. Its strategy seeks liaison work and the development of coalitions to support the People's Republic of China and "disintegrate" enemies. This includes the *three wars*: public opinion and media warfare, psychological warfare, and legal warfare. Chinese political warfare also involves active measures, such as violence and other forms of coercive and destructive attacks (Gershaneck, 2020).

From the Chinese perspective, this is a war waged primarily for control and influence, employing coercion, corruption, and violent covert operations. The People's Republic of China prefers to win this war without ever firing a shot, but its increasingly powerful military and paramilitary forces are working in the background to support its escalating war of influence (Gershaneck, 2020).

For its part, Russia's political warfare is not focused on isolated events, but rather is at the heart of a political strategy deployed against the West to weaken its institutions and undermine the transatlantic consensus. As such, Moscow's efforts work in a mutually reinforcing manner, though not always in a clearly coordinated manner, as if it were an evolving ecosystem. This complex ecosystem consists of a network of proxy actors, media organizations, social media accounts, vested commercial interests, oligarchs, civil society groups, cybercriminals, intelligence agencies, private companies, and political actors inside and outside Russia. Some of these actors act at the direct behest of the Kremlin, while others act outside their own political agenda, but with the same ultimate goal. The system is a moving target, continually evolving in sophistication, complexity, and deliberate concealment (Polyakova & Boyer, 2018).

Paradoxically, Moscow also claims something similar: upholding its civilizing role, perceiving itself threatened and mentally preparing its people for war, it also claims to be the target of a political war waged by the West. Defined by Russians as any military or non-military action (cultural, political, economic, diplomatic, informational, or environmental) aimed at weakening an adversary and based on the use of non-governmental organizations (NGOs) and civil society organizations, support for political opponents or social movements, control of the internet and information technology, media propaganda, and cultural penetration, this U.S.-sponsored war seeks to exploit the potential for popular protest to provoke or

facilitate changes in government in Russia. Russia's perception of threat and its lower conventional military power relative to the North Atlantic Treaty Organization (NATO) allow it to justify destabilization, subversion, information operations, and military operations within its regional area of influence (Piella, 2019).

From a legal perspective, the agreements that regulate war include the Rome Statute, the Geneva Conventions, and the Universal Declaration of Human Rights. These statutes seek, in some way, to provide a legal and regulatory framework that tells States (or other actors involved in war) what they may or may not do to avoid violating human rights or international humanitarian law. When analyzing political warfare, it can be inferred that these treaties and countries' internal laws function as limits that actors base their strategies on and decide whether to respect or exceed.

In this respect, Borrero (2017) considers that, currently, war, as it is inherently conceived, tends to be misinterpreted, and its degree of acceptance is justified by its motivations. In other words, war has come to be considered necessary to defend ideologies or territories. This qualification does not rule out the possibility of an inevitable or justified war, which shows that the long debate over the concept of political war ends up being framed within a misguided just-war framework, as each of the contenders presents what they consider their reasons. For this reason, from a more ambiguous perspective, Borrero (2017) not only describes political war as a potential response to the interests of regulating a world order, but also does not prohibit it as a mechanism for strengthening disputes among States.

Likewise, the United Nations Charter has consolidated a progress derived from the mechanisms established in the law of war—hereinafter, *ius ad bellum*—that seeks to understand the reasons States give for just war and the confusion that arises from them. Thus, political war becomes an impermissible method of waging war because no mechanism has been established to regulate it.

In this context, it is essential to establish the most relevant conceptualizations of war, in which political war fits within the implements of power. Figure 1 presents a comparison of concepts and doctrines of war based on the use of state or non-state means to achieve countries' political objectives.

This comparison shows that the concepts coincide in the use of unconventional means to influence the politics of other countries. The basic difference in this comparison is that the American political warfare strategy did not include the use of criminal elements or terrorist forces to carry out actions. The concepts of hybrid warfare and unrestricted warfare do. Thus, it can be inferred that, from the perspective of means, unrestricted warfare is a type of political warfare

according to Chinese doctrine. In the case of hybrid warfare, while American doctrine excludes other instruments of national power, various theorists include them, which would make it resemble political warfare or unrestricted warfare. It is important to understand the periods and conditions in which these concepts were developed, as well as the lack of consensus surrounding them. However, the important thing in this comparison is to understand how legal and ethical limits constrain the means employed in strategies and can be altered in the determining aspects of “new” types of conflict.

Figure 1. Comparison of the Use of Means in Different Types of War



Source: Own elaboration.

It is worth noting that the previous illustration highlights four fundamental aspects of political warfare, including diplomacy, which can be used to prevent armed conflicts or, if necessary, to incite them. This was evident during the Cold War, when, despite being often defined as a non-military conflict, the opposing sides—then the U.S. and the USSR—clashed across different arenas, including the Korean Peninsula, Vietnam, and Germany.

Military operations are also highlighted, as although some even have peacekeeping objectives, they often create tension among States and risk escalating into a military confrontation that could quickly turn from a political conflict into a war.

Information Warfare

Information warfare is the contemporary, unofficial doctrine created in the 1990s, whose main premise is the use of information as a weapon in armed combat and

political confrontation, for the defense or seizure of power (Tovar, 2011). It involves using information to gain an advantage over the opponent, such as collecting tactical information, confirming the veracity of one's own information, distributing propaganda or disinformation to demoralize the public and the enemy, reducing the effectiveness of enemy intelligence, and denying information-gathering opportunities (Rojas et al., 2011). Furthermore, it can work to gain the support of groups or populations in an area of operations.

As already stated, information warfare is among the actions an actor can undertake in the context of political warfare, so it should not be understood as a separate tool but rather as a complement. However, information warfare actions are not perceived solely as a complement to military operations; they can also be executed as an independent course of action (Tovar, 2011).

Information warfare alters and attacks the enemy's epistemological systems to generate confusion in their ability to distinguish between reality and, thus, diminish the efficiency of the decision-making process and achieve the objective (Tovar, 2011). To this end, informational attacks are widely disseminated, targeting audiences with narratives aimed at weakening adversaries, primarily through radio, the press, television, and the internet. This also involves executing tactics or issuing opinions that, through media dissemination and coverage, alter adversaries' knowledge and beliefs, as well as their perceptions of reality. These actions, therefore, require coordination between civilian information service operators and the military command (Tovar, 2011).

Humans' reliance on media representations of reality thus becomes a key advantage for information aggressors in achieving their goals. In the context of information warfare, the widespread dissemination of lies, disinformation, or fake news, along with the creation of confusion and fear among the population, is both feasible and justifiable. Therefore, carrying out information operations through the media integrates nonviolent warfare strategies into daily life, blurring the line between peace and war (Tovar, 2011).

Use of Political Warfare and Information Warfare by Threats in Colombia

The transformation of the internal conflict in Colombia has caused Organized Armed Groups (OAGs) to change their strategies, adding new elements to their guerrilla

warfare. Their strategy to influence populations and audiences has sometimes included cultivating political allies abroad and disinformation campaigns. However, since political warfare, by definition, is waged solely by state actors, it is necessary to look holistically to identify the threats this strategy can pose to our country.

To carry out political warfare, States employ multiple layers of proxies—direct or indirect agents and entities—to maintain plausible deniability and strategic ambiguity (Polyakova & Boyer, 2018). In this context, OAGs, as well as criminal organizations, would not be the perpetrators but rather the agents through which a hostile State could implement its political warfare strategy.

Thus, a country could infiltrate Colombia through elites, political parties, front organizations, influencers, and groups outside the law. From then on, it could carry out actions through the elites, atomize and neutralize political and social organizations, and even bring about a change of government. Today, nothing is more suspicious than spontaneous subversive operations or media devices with a direct and unidirectional narrative, given the immense range of actors and interests involved (N. Rodríguez, 2019).

Another method is to identify social vulnerabilities by amplifying divisive social problems. In Latin America, political polarization, gender ideology, "class struggle," and ethnic and religious issues are amplified to destabilize governments and enable changes favorable to threats. In the United States, Russia's disinformation machine has focused on racial tensions, criminal justice policy, immigration of people from Latin American and Muslim countries, and class divisions (Polyakova & Boyer, 2018).

To identify which international actors are actually using political warfare against Colombia, it is enough to ask: Which countries employ diplomatic, informational, economic, and military means, with both overt and covert actions, to influence Colombia, along with supporting the actions of OAGs (overtly or covertly), possibly through other methods such as drug trafficking, smuggling, or immigration?

Effects of Political and Information Warfare on SF Operations

In Colombia, pro-government groups have sought to delegitimize the actions of the Armed Forces to weaken them and restrict their freedom of action. In this

regard, these groups and their supporters have employed discursive and political strategies to attack the triad composed of the SF, the power of strategic air strikes, and intelligence. This triad has become the primary instrument for numerous Armed Forces to confront asymmetric enemies successfully. This tool, which would have been invincible on the battlefield, is one of the Armed Forces' strengths and can be perceived by the threat as the center of gravity that must be defeated through the manipulation of propaganda and politics (Montero, 2021).

The asymmetric threat recognized that if it partially deactivated its armed component to focus on social, political, and legal pressures, it could weaken some state capabilities that might otherwise defeat it on the battlefield, while also controlling the narrative by shifting public opinion on social media (Montero, 2021). According to these narratives, legitimate intelligence actions are, in fact, acts of political persecution and privacy abuse; strategic airstrikes conducted within the framework of International Humanitarian Law (IHL) are seen as abuses of IHL itself. Likewise, the Army is gradually losing its freedom of action due to the legal war waged against it, which results in military personnel being prosecuted for abuses simply for carrying out their constitutional duties. Therefore, it is important to recognize that the political war being fought arises from the understanding of how political factors influence military activity—issues that should have been fully addressed by the National Army (Rojas, 2017).

Consequently, as has been the case since ancient times, when confronting a stronger army is impossible or when choosing not to do so, the adversary employs asymmetric strategies. It blends among populations, considers the opposing population as its center of gravity, acts outside traditional norms of warfare, exploits IHL for its own interests, and aims to achieve strategic effects through effective informational exploitation of its logical, physical, and informational actions. In other words, the threat leverages the moral, political, social, demographic, legal, economic, or military weaknesses of adversaries who are more effective in direct confrontation (Piella, 2019).

In this scenario, it must also be considered that the technological field has developed telecommunications, information technology, and audiovisual media, which have impacted the economic, political, and cultural order, especially with the milestone of the internet in communication and the interdependence of countries. This has accelerated the unification of markets, the movement of capital, and the creation of new communities that transcend existing societies and cultures (Piella, 2019).

With the development of information and communication technologies, digital social networks have revolutionized interpersonal relationships and the way we have conversations today. The ease and convenience provided by technology across a multitude of fields have allowed it to permeate the educational, business, and government spheres, in areas where Colombians' perceptions can be violated, especially because its introduction facilitated everyday activities and promoted others that were once considered impossible (M. C. Rodríguez, 2019).

Therefore, the information revolution has been compared to the Industrial Revolution, insofar as it represented a historical and social leap thanks to the massive application of technology in production processes, although now that technology is not the steam engine, but rather access to information (M. C. Rodríguez, 2019). In this respect, it is necessary to take advantage of the speed of technological change, as it offers key tools to support decision-making, protection, and lethality, while recognizing that their proper use extends to the cyber domain and the informational dimension.

Given the multidimensional nature of cybersecurity in Colombia, it is necessary to implement tools to sustain the cyber resilience process and achieve objectives and strategies grounded in a situational assessment.

Furthermore, the future will pose new challenges, as technological advances in artificial intelligence, machine learning, and automation, coupled with the growing use of big data, have set the stage for a new era of high-impact political, economic, and cyberwarfare. In the short term, it will be more difficult, if not impossible, to differentiate between real and fake audio, video, or online personalities, making it harder to distinguish between reliable and unreliable information. Malicious actors will use these technologies to attack societies more effectively and efficiently. As States like the United States, Russia, and China invest resources in developing technologies, the global competition for the next leap in political warfare will intensify. Thus, forward-looking analysis indicates that strategies need to mitigate not only current threats but also future ones, in a context where opportunities to do so are rapidly diminishing (Polyakova & Boyer, 2018).

Executing disinformation actions requires the use of key overt and covert actors. The threat may use State-run media outlets, and covert means could include social media trolls, automated accounts (bots), phishing accounts on Facebook, Twitter (now X), and Instagram, or websites (Polyakova & Boyer, 2018).

Considering the international support that illegal groups receive, from the perspective of political warfare, it can be inferred that the use of proxy structures

would characterize these groups' use to destabilize the domestic political environment. Along these lines, this political-economic phenomenon created the need to analyze, specify, and understand how political warfare worked in Latin American countries, to the point that it has even become one of the most important challenges for academics today.

To understand the impacts and roles of SF in confronting these challenges, it is crucial to examine other States that have experienced political warfare, focusing on the political, economic, and social consequences that have arisen under these governments.

Countries with dictatorial governments seek to control public opinion through media control. At the same time, they impose restrictions and censorship on informational content, such as websites, music, and films, that, in their opinion, could harm their political and strategic objectives. Thus, the coercion of personal freedoms is a tool that dictatorial governments often use in the name of a supposed greater collective good that would justify it. This can be clearly seen in the case of the Sandinista regime in Nicaragua, where the State

[...] imposed an extraordinary law that limited public freedoms; implemented a media law that censored the independent press; established social organizations that, instead of fighting for their unions, supported the policies of the Sandinista Party, even at the expense of their own needs; set up a surveillance system in neighborhoods that watched every movement of the people, and if they criticized the revolutionary government, they were accused of being contras. (Cisneros, 2014, p. 235)

This is how political warfare is often related to the limitation of personal freedoms. In many cases, such as under the Nicaraguan Sandinista regime, freedom of expression was curtailed, public liberties no longer existed, and the press was tightly controlled, even affecting people's life choices.

On the other hand, countries that practice Western-style representative democracies, which seek to guarantee individual freedoms such as freedom of expression and thought, are more vulnerable to information warfare campaigns by internal and external actors. In these countries, the State often lacks the strategies and, consequently, the tools to counter these campaigns.

Inspired by international military doctrine, primarily NATO doctrine, Colombia has developed SO capabilities to combat OAGs. Its evolution over the past few decades led to the creation of the DIVFE, which has become an SO command

tasked with training its members in direct action, irregular warfare, and intelligence gathering on battlefields and in various domains, with the responsibility of planning and executing SO inside and outside the national territory (Ejército Nacional de Colombia, 2018b). Over time, the DIVFE's operations have played a fundamental role in the State's successful response to the threat posed by OAGs in Colombia.

However, within the framework of SO, changes in domestic public opinion and international pressure; the risk of collateral damage; submission to anachronistic and restrictive customs and practices of war; anxiety about the electoral effects and political costs of operational actions; the demand to restrict their impact, scope, and duration; and the need to use force in a restrictive and limited manner are all factors that can be exploited by actors countering a Western military (Piella, 2019). The resulting lack of freedom of action to employ intelligence and carry out surgical strikes has debilitating effects on SO.

Role of the Armed Forces in Countering Adversarial Political and Information Warfare

For Americans, the instruments of national power include, in addition to the diplomatic, economic, and military dimensions, an informational component. This element helps strategic planners recognize the importance of national strategies in informing and influencing audiences across a country's external and internal environments. Apart from serving as a means to achieve narrative superiority in the informational dimension, these strategies also provide protection against informational attacks, as they generate structures specialized for this type of attack.

Clearly, the American case demonstrates that the State needs options between military intervention and complete non-intervention. To address contemporary threats, the State should be capable of waging political warfare using overt and covert measures, from economic actions, political alliances, and propaganda to covert operations, psychological warfare, and even the promotion of underground resistance in hostile States (Boot & Doran, 2013).

According to American doctrine, although the strategy for executing effective covert actions is well developed, it is important to distinguish between information and propaganda: information for allies is public diplomacy, while information for the enemy is psychological warfare (N. Rodríguez, 2019). From this, we can infer how political warfare works on the international stage. It is practiced by countries

that seek to influence others based on their justifications and, at the same time, delegitimize the adversary's political warfare.

Regarding SO, the U.S. Army has a specific school for special warfare education and training: the John F. Kennedy Special Warfare Center and School. At this institution, the training approach has changed little since its creation in 1952, consisting of selecting and educating SF personnel to organize, train, and employ a guerrilla force. At the time of its creation, low-intensity conflicts were common, and with them arose the need to develop special warfare capabilities: counterinsurgency and unconventional warfare (Department of the Army, 2014).

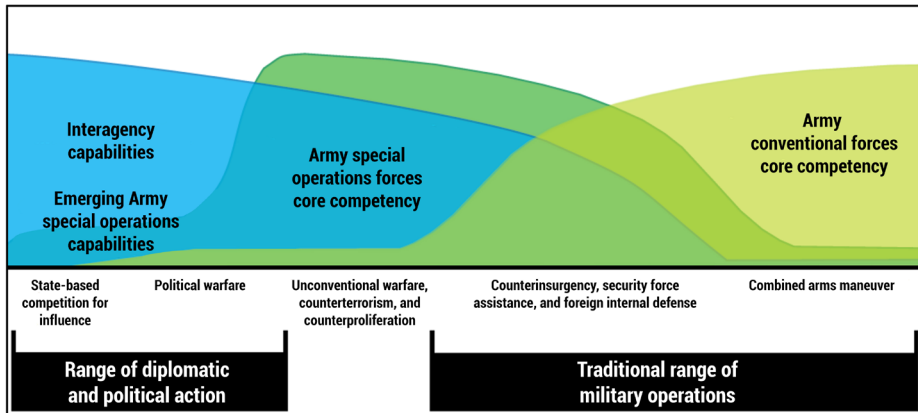
During the 1980s and 1990s, the American defense system reactivated the SF to respond to threats posed by nations in the Pacific Rim, the Caribbean, and Africa. This SF played a pivotal role in combating guerrilla movements and containing the spread of communism in Central and South America by leveraging the military capabilities of democratic regimes. To this end, SF was deployed in El Salvador to develop an effective counterinsurgency force and assist Hondurans in resisting and defeating an invasion from Nicaragua and a communist-backed insurgency. During the second half of the 1980s, American SO supported counternarcotics operations in Venezuela, Colombia, Ecuador, Peru, and Bolivia (Department of the Army, 2014).

The genesis of SF in the United States occurred when they developed the skill sets necessary for special warfare. Subsequently, special warfare capabilities were key to a revival of unconventional warfare following the terrorist attack on the Twin Towers on September 11, 2001. On that occasion, operational detachments played a central role in defeating the Afghans during Operation Enduring Freedom, in which insurgent training against the Taliban gained prominence with images of "horse soldiers." Operation Iraqi Freedom also demonstrated that a small number of SF teams, linked to training and assisting the indigenous resistance, could support large combat operations by preventing 13 Iraqi divisions from reinforcing units defending Baghdad (Department of the Army, 2014). This special war strategy via unconventional warfare, in which the United States employed SF to leverage proxy forces, can be employed both in political warfare and in support of conventional operations.

A 2015 white paper by the U.S. Special Operations Command, *Redefining the Win*, describes the conflict spectrum represented in Figure 2. Using this spectrum, the white paper presents unconventional warfare as a gray area that does not encompass political warfare or even war itself (Linnemann, 2016). From this figure, it can be concluded that "emerging capabilities" and the "core competency of Special

Operations Forces" fall within the spectrum of political warfare, along with the "range of diplomatic and political action." It also notes that political warfare lies between "competition among States for influence" and unconventional warfare actions.

Figure 2. Comparison between National and Special Operations Capabilities in Relation to the Spectrum of Conflicts



Source: Linnemann (2016).

According to the doctrine of Colombia's SO, the special warfare operations carried out by SF include unconventional warfare, assistance to security forces, counterinsurgency, preparation of the operational environment, internal defense abroad, psychological operations, and civil affairs, that is, it resembles what was described about American doctrine (Ejército Nacional de Colombia, 2018b). All of this suggests that the Colombian SF are trained to execute these types of operations, but practice shows they have not developed these capabilities, as they have focused solely on surgical strikes (Sánchez & Alexis, 2020).

Colombian SO doctrine emphasizes that foreign internal defense consists of coordinating the participation of a government's military and civilian agencies in action programs adopted by another organization or government aimed at liberating and protecting its society from subversion, anarchy, insurgency, terrorism, and other security threats. This includes supporting training for military forces from other countries, taking into account their internal threats.

In this context, the primary role of Special Operations Forces should be to train, advise, and assist the host nation's security forces in special warfare activities. According to doctrinal manuals, this implies a comprehensive approach

encompassing all instruments of national diplomatic, informational, military, and economic power. It is worth noting the legacy of American political warfare doctrine in this regard, as already established (Ejército Nacional de Colombia, 2017).

Internal defense abroad is therefore carried out through a unified effort that involves the synchronization, coordination, and integration of activities from both governmental and non-governmental entities within the operation to achieve unity of effort (Ejército Nacional de Colombia, 2017). This highlights the importance of other instruments of national power, beyond the military, in implementing this strategy. Without coordinated actions and state support, SF will not be able to carry out special warfare to improve its operations in the face of adversarial political warfare (Paddock, 1980).

SO doctrine still emphasizes the need for SF to prepare in an operational environment before acting on direct missions. That is, units must change the prevailing conditions in hostile environments to weaken the threat, obtain as much information as possible about it, and gain the support of local populations. In this respect, SF should conduct operational environment preparation as a shaping activity for future missions (Ejército Nacional de Colombia, 2017). If this capability is properly applied, SF could conduct its operations with the potential reduction of risks associated with the political warfare waged by the threat within the country. Furthermore, it would allow them to exert influence within an aggressor State to destabilize it through training, advising, and assisting local combat forces.

Special warfare tasks are not simple. On the contrary, they require units to be able to operate within a specific population, so they must address sociocultural factors by understanding the culture. To the extent that the success of any military operation or campaign depends on the application of unique capabilities designed to combat and win population-centered conflicts, sociocultural factors will be an essential part of special warfare activities (Paddock, 1980). In this respect, SO must consider the totality of physical aspects and the social and cultural environments that influence human behavior, but to do so, special operators need rigorous education and training in these areas (Ejército Nacional de Colombia, 2017).

It is important to note that successful counterinsurgency operations focus on the population because they aim to create conditions of legitimacy and credibility for the government and its programs. Likewise, public support is a fundamental objective of insurgency and must be directed as part of an integrated counterinsurgency effort (Department of the Army, 2014).

According to Colombian doctrine, the objective of unconventional warfare operations is to achieve a change in political control and the perceived legitimacy of regimes. Therefore, it is doctrinally accepted that unconventional warfare has strategic utility, as it can alter the balance of power among sovereign States. Conducting such operations entails significant political risk in both the national and international spheres and requires careful execution and oversight. The need to operate with a diverse mix of clandestine and covert means, methods, and ends underscores the critical need for excellent intelligence in the area where operations are conducted. As in all conflict scenarios, in unconventional warfare, the Military Forces must closely coordinate their activities with inter-organizational interlocutors to enable and safeguard sensitive operations (Ejército Nacional de Colombia, 2017).

Colombian doctrine presents information operations as a distinctive capability of SF, which it executes across the strategic, operational, and tactical levels of warfare. Furthermore, the doctrine notes that these operations are also a capability of the Ministry of National Defense (MDN), used as part of inter-institutional activities to achieve national objectives (Paddock, 1980). On this point, American doctrine on employing the informational instrument of national power to distinguish its objectives is echoed in Colombian documents. However, the Colombian State does not have this structured capability, as is the case with the United States and other countries that employ it, which undermines the current doctrine's foundation (Department of the Army, 2014).

Doctrinally, information operations are the primary information capability of SF, enabling them to analyze and address psychological factors in the operational environment; provide support for information and influence activities as a core competency of SF; assist other information agencies in influencing; conduct information operations activities supporting national civil authorities; support adversary disinformation efforts; deliver a significant non-lethal effect to identify high-value targets; carry out deception operations; influence and guide target acquisition; analyze target audiences within the operational environment; and examine media in the operational environment (Ejército Nacional de Colombia, 2017). This SO capability should coordinate all existing information capabilities within a force to counter adversary information warfare. In this regard, it is important to note that while NATO doctrine already includes a toolkit developed and tested in complex operational environments to address the challenges of

information warfare, it remains essential to understand, master, and apply them (Paddock, 1980).

It is evident that information operations doctrine, an essential function of SF, is not being implemented within SO in Colombia, as outlined in NATO doctrine. On the contrary, the Colombian SF engage only in surgical strikes, while the Comprehensive Action units or teams aim to influence audiences, with the limitations inherent to that specialty. This way, the DIVFE strays from the fundamental doctrinal tasks of information operations.

In this regard, the Colombian DIVFE must, together with its intelligence agencies, identify all types of disinformation operations aimed at undermining the country's security and defense. These operations may originate from any type of organization or online group whose objective is to execute a plan to destabilize the state structure. By effectively fulfilling this task, the DIVFE can also provide timely advice to higher echelons for strategic planning and policy definition.

Finally, it must be clear that the activities of the Armed Forces must be based on a series of regulations and laws, which are subject to the prescriptive norms governing the selection of targets, and that they must be directed solely against military objectives. In this regard, it must be emphasized that strict compliance with IHL, International Human Rights Law (IHRL), and international standards governing conflicts provides operations with comprehensive legitimacy.

One of the fundamental characteristics of information warfare and political warfare is that the State must mobilize all its resources—infrastructure, technology, and communications—to eliminate a threat that constantly seeks to destabilize it. In this regard, the State's dominance must be absolute, as the threat makes a continuous, tireless effort to win over its citizens' minds.

According to Montero (2021), current wars are asymmetric or hybrid, presenting different strategic, operational, and tactical challenges and requiring fighting in entirely new and complex operational environments. In this context, methodologies for selecting centers of gravity become relevant, suggesting that, in these new confrontations, the main focus should be on legitimacy or, more broadly, on some factor within the political spectrum. Therefore, it can be said that the political objective of war significantly influences the military objective, as its effects can destabilize the State. Montero (2021) states that the politics-war relationship is determined by the capacity of the Force, as evidenced in asymmetric scenarios. Clearly, one of the enemy's main weapons in this type of war is social sensitivity, which fosters social resentment through misinformation or misinterpretation of situations.

Conclusions

The survival of organizations throughout human history depends on their ability to adapt to the environments in which they operate and the efficiency of their processes. Therefore, security innovation initiatives must drive adaptation to an increasingly demanding environment (Lesaca, 2018).

In this regard, it is concluded that SF has concentrated on executing surgical strikes to disrupt and weaken OAGs. While this type of action has long been the foundation of the Armed Forces, alternative attacks generated by political warfare and information warfare demonstrate the increasing importance of special warfare within the scope of SO, with the belief that these operations can influence and alter operational environments.

Therefore, it is crucial for special operators to address highly complex issues, such as the relationships among governments, populations, and their cultures; adapting to changing circumstances; theories of victory; and the multiple aspects of the environment where strategy development occurs.

It is crucial for the DIVFE to recognize policies that support the processing of sensitive data and information, as well as the information capabilities on which the country's infrastructure relies. This way, it can meet its operational requirements and achieve its mission by correctly applying legal frameworks.

In this context, the DIVFE can no longer focus solely on the land domain within a joint force but must also support other military forces in their domains and dimensions to help them overcome operational challenges. This means that the shift must concentrate on improving the DIVFE's capability to produce multi-domain effects and to effectively and continuously integrate the entire joint force (Brown, 2018).

It is special warfare, not surgical strike operations, that characterizes SF worldwide and distinguishes them from other troops with similar capabilities, such as the Police SO or the Commando Forces. A country cannot refrain from developing these capabilities without paying the price of greater vulnerability to adversarial political warfare.

Of course, the process that would enable Colombia to improve the State's informational capacity as a tool of national power does not originate within SF but rather in its defense policy and strategy. Without this, SF will remain weakened because they lack the freedom of action needed to maximize their operations, as

NATO doctrine alone does not guarantee its application in a manner similar to that in developed countries.

In a Latin American country, individual privacy sometimes outweighs national stability. When discussing the limits on intelligence gathering while allowing the widespread use of fake news and disinformation, we need to examine how much individual freedoms can supersede society's well-being. The chance that disinformation campaigns may go unpunished because of privacy policies has caused instability that harms many people and endangers democracy in our country.

The fragility of public opinion depends on the population's low level of knowledge on the subject, which the enemy has exploited to strengthen its position. By manipulating the community's sensitivity, it creates fear and sometimes even disgust toward law enforcement, emphasizing the need to reinforce SF mechanisms against political and information warfare. Therefore, it can be said that the lack of understanding on the topic increases social sensitivity.

It is crucial to highlight the government's responsibility to develop effective systems for countering the threats posed by political and information warfare. To do this, it is necessary to promote strategic thinking throughout all government institutions, ensuring they can respond decisively to potential attacks.

Lastly, the State should also focus on identifying media attacks on security forces and potential threats, as enhancing strategic intelligence would be a highly effective tool for preventing such attacks. This improvement must rely on institutional collaboration that directly involves all agencies involved in national security.

References

- Boot, M., & Doran, M. (2013, June 28). Department of Dirty Tricks: Why the United States needs to sabotage, undermine, and expose its enemies in the Middle East. *Foreign Policy*. <https://tinyurl.com/377f5ewf>
- Borrero Mansilla, A. (2017). *Guerra, política y derecho*. Editorial Universidad El Bosque.
- Brown, R. B. (2018). La región del Indo-Asia Pacífico y el concepto de batalla multidominio. *Military Review*, (first quarter), 81–88. <https://tinyurl.com/3m36v9xc>
- Cisneros, I. (2014). *Norberto Bobbio: De la razón de Estado al gobierno democrático*. Instituto Electoral y de Participación Ciudadana del Estado de Jalisco. <https://tinyurl.com/4vtdtxd>
- Colom, G. (2019). La amenaza híbrida: mitos, leyendas y realidades. *Boletín IEE*, (13), 669–682. <https://tinyurl.com/2y57tjb3>
- Department of the Army. (2014). *Field Manual FM 3-18 Special Forces Operations*. <https://tinyurl.com/yn6h6atz>
- Ejército Nacional de Colombia. (2017). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Public]*. Imprenta Militar del Ejército. <https://tinyurl.com/2p8b7nse>
- Ejército Nacional de Colombia. (2018a, September 13). *Caballería*. <https://tinyurl.com/5e3d9yce>
- Ejército Nacional de Colombia. (2018b). *Manual de Campaña del Ejército MCE 3-18 Operaciones de Fuerzas Especiales [Restricted]*. Imprenta Ejército.
- Gershaneck, K. K. (2020). *Political warfare: Strategies for combating China's plan to "win without fighting"*. Marine Corps University Press. <https://tinyurl.com/yc49pkfr>
- Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Potomac Institute for Police Studies. <https://tinyurl.com/dyc5rmnv>
- Lesaca, J. (2018). La disrupción digital en el contexto de las guerras híbridas. *Cuadernos de Estrategia*, (197), 159–196. <https://tinyurl.com/3cxzsaw5>
- Linnemann, R. A. (2016). Unconventional Art and Modern War. *Military Review*, (May-June), 17–26. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160630_art007.pdf
- Lucas, S., & Mistry, K. (2009). Illusions of Coherence: George F. Kennan, U.S. Strategy and political warfare in the early Cold War, 1946–1950. *Diplomatic History*, 33(1), 39–66. <https://tinyurl.com/mpb8rb95>
- Montero, L. A. (2021, March 18). *De la guerra política como parte de la guerra asimétrica*. Escuela Superior de Guerra. <https://tinyurl.com/5u6h86bm>
- Paddock, A. H. (1980). *Psychological and unconventional warfare, 1941-1952: Origins of a "special warfare" capability for the United States Army* [Individual Study Project, US Army War College]. Repositorio DTIC. <https://tinyurl.com/37wsfnk>
- Polyakova, A., & Boyer, S. P. (2018). *The future of political warfare: Russia, the West, and the coming age of global digital competition*. The Brookings Institution. <https://tinyurl.com/cjsu5mvs>

- Rodríguez, M. C. (2019). *Límites legales del control parental en las redes informáticas con relación al libre desarrollo de la personalidad en niños menores de 14 años* [Bachelor's thesis, Universidad Católica de Colombia]. <https://tinyurl.com/yc7vv67s>
- Rodríguez, N. (2019, November 7). *Guerra política y teoría de las acciones encubiertas 2.0*. <https://tinyurl.com/27553jca>
- Rojas Guevara, P. J. (2017). Doctrina Damasco: eje articulador de la segunda gran reforma del Ejército Nacional de Colombia. *Revista Científica General José María Córdova*, 15(19), 95–119. <https://doi.org/10.21830/19006586.78>
- Rojas, W. A., Benavides, J. F., & Bello, J. C. (2011). Las operaciones de información en las guerras de información [Specialization capstone, Universidad Piloto de Colombia]. Repositorio Unipiloto. <https://tinyurl.com/3f7vpwer>
- Sánchez, M., & Alexis, D. (2020). Transformación de las Fuerzas Especiales de acuerdo con la doctrina internacional. *Brújula Semilleros de Investigación*, 4(7), 46–57. <https://tinyurl.com/2xb9xxes>
- Tovar, H. L. (2011). *Guerra de información: ¿El arma es el mensaje?* [Master's thesis, Universidad Central de Venezuela]. Repositorio UCV. <https://tinyurl.com/nhhxt9jxB>