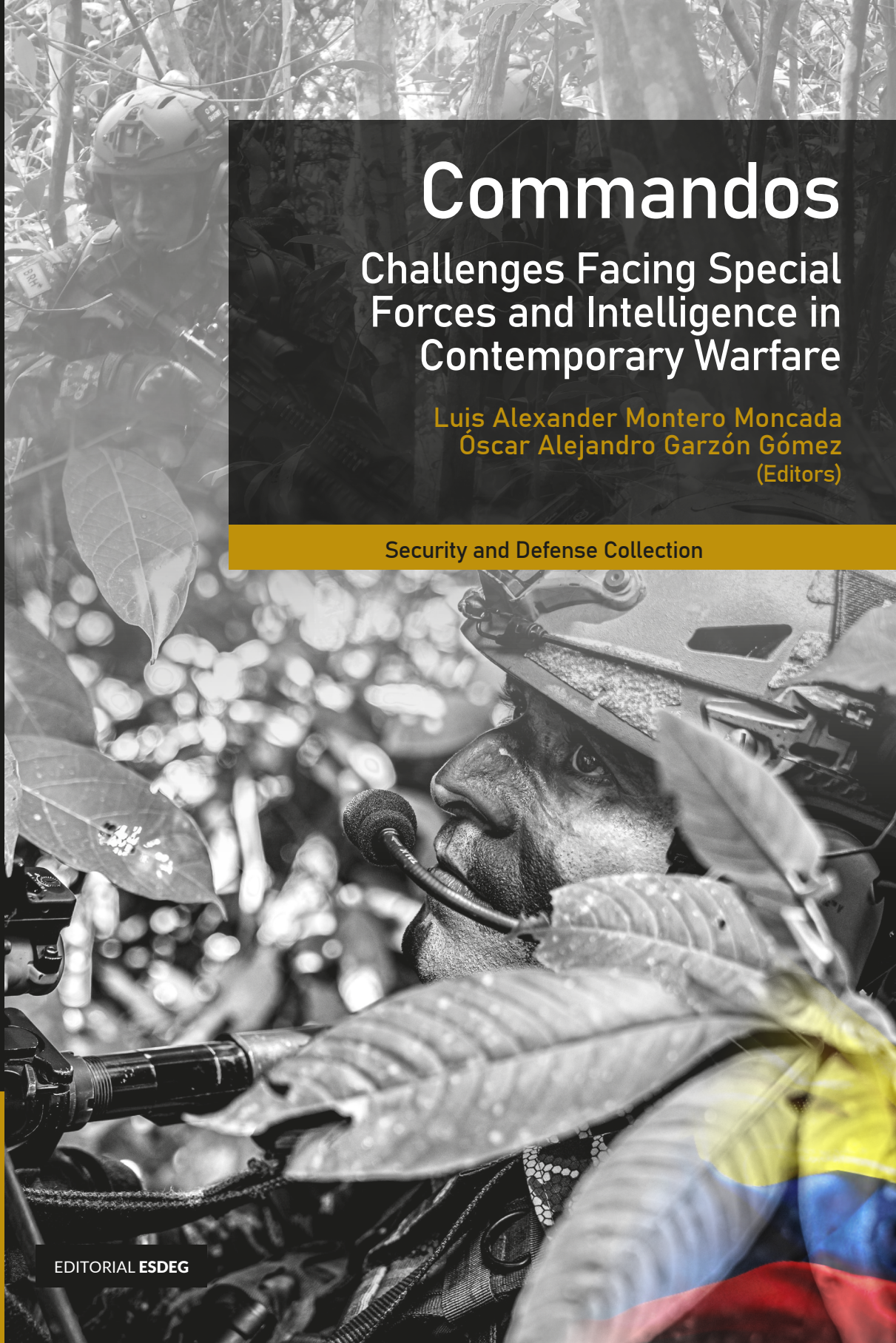


Commandos

Challenges Facing Special Forces and Intelligence in Contemporary Warfare

Luis Alexander Montero Moncada
Óscar Alejandro Garzón Gómez
(Editors)

Security and Defense Collection

EDITORIAL **ESDEG**

Commandos

Challenges Facing Special Forces and Intelligence in Contemporary Warfare

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Security and Defense Collection
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Commandos

Challenges Facing Special Forces and Intelligence in Contemporary Warfare

LUIS ALEXANDER MONTERO MONCADA

ÓSCAR ALEJANDRO GARZÓN GÓMEZ

(EDITORS)

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., 2025

Catalogación en la publicación – Escuela Superior de Guerra "General Rafael Reyes Prieto"

Commandos: challenges facing special forces and intelligence in contemporary warfare / Luis Alexander Montero Moncada, Óscar Alejandro Garzón Gómez (editors) – First edition.-- Bogotá : Sello Editorial ESDEG, 2025.

278 pages: diagrams and tables; 24 cm
Includes bibliographic references at the end of each chapter

ISBN (print): 978-628-7818-39-2
E- ISBN: 978-628-7818-40-8

(Security and Defense Collection)

1. Colombia. Army. Joint Special Operations Command. 2. Colombia. Military Forces. 3. United States. Joint Special Operations University. 4. Special forces (Military science) – Colombia. 5. Special forces (Military science) – Case studies. 6. Special operations (Military science) – Colombia. 7. Military intelligence – Colombia. 8. Asymmetric warfare. 9. Hybrid warfare. 10. Cyberspace operations (Military science). 11. Urban warfare. 12. Information warfare. 13. Colombia – Military policy. 14. Colombia – Strategic aspects i. Galindo, Jaime Alonso, Brigadier General (preface). ii. Montero Moncada, Luis Alexander (editor). iii. Garzón Gómez, Óscar Alejandro (editor). iv. Serna, Jorge (author). v. González, Miguel Antonio (author). vi. Cepeda Daza, Helver Orlando (author). vii. Reyes Pulido, Oscar Leonardo (author). viii. Torres Cabra, Álvaro Iván (author). ix. Lopes da Cunha, Guilherme (author). x. Rodríguez Rodríguez, José Nicolás (author). xi. Garzón, Oscar (author). xii. Bernal Vallarino, Oscar Mauricio (author). xiii. Salgado Luzia, Ilmar Ubiratan (author). xiv. Gutiérrez Oliveros, Jorge Rafael (author). xv. Colombia. Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG).

SCLC U262 .C65 2025 Catalog Record SIBFuP 991394724207231
SCDD 355.409861

Downloadable file in MARC at: https://tinyurl.com/esdeg991394724207231

Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare
First edition, 2025

Editors:
Luis Alexander Montero Moncada
Óscar Alejandro Garzón Gómez

Cover:
Raquel Arianne Alvarado Candela based on images provided by Luis Alexander Montero Moncada.

Security and Defense Collection

Print ISBN: 978-628-7818-39-2
Digital ISBN: 978-628-7818-40-8
DOI: https://doi.org/10.25062/9786287818408

2025 Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Office of the Deputy Director of Research
Sello Editorial ESDEG
Carrera 11 Nº. 102-50 Bogotá D.C., Colombia
www.esdeglibros.edu.co

E-book published through the Open Monograph Press platform.
Print run of 100 copies
Printed in Colombia

Translation of the book titled "Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea" resulting from research conducted at the Escuela Superior de Guerra "General Rafael Reyes Prieto."

EDITORIAL ESDEG

Table of Contents

Preface 09-10
MG Jaime Alonso Galindo

Introduction 11-12
Luis Alexander Montero Moncada

Chapter 1
Special Forces in Contemporary Warfare 13-30
Jorge Serna
Luis Alexander Montero Moncada
Miguel Antonio González

Chapter 2
In the Mind of the Strategist: Identifying the Strategy Applied to the Target Acquisition System 31-60
Helver Orlando Cepeda Daza
Oscar Leonardo Reyes Pulido

Chapter 3
Prospective Analysis of Special Forces Operations in Megacities: Colombia and Brazil 61-86
Álvaro Iván Torres Cabra
Guilherme Lopes da Cunha

Chapter 4
Contemporary Cyber Threats: Challenges for Special Operations in Colombia 87-104
José Nicolás Rodríguez Rodríguez
Oscar Garzón

Chapter 5
Special Forces Operations against Threat Systems based on Political and Information Warfare 105-128
Oscar Mauricio Bernal Vallarino
Ilmar Ubiratan Salgado Luzia

Chapter 6
Special Warfare: From Tactics to Practice 129-146
Jorge Rafael Gutiérrez Oliveros
Luis Alexander Montero Moncada

Chapter 7
Cyber Support for Colombian Army Special Forces in a Tactical Environment 147-170
Juan Guillermo Cruz Segura
Ricardo Di Genaro

Chapter 8
Strategic Impact of Disinformation Operations and the Effective Response of the Military Forces in the 21st Century 171-188
Humberto Andrés Niño Vergara
Miguel Antonio González Martínez

Chapter 9
Limits of Artificial Intelligence and Big Data Technology in Intelligence Analysis 189-208
Jaime Andrés Naranjo Ardila
Jorge Luis Mejía Rosas

Chapter 10
The Geopolitics of Organized Crime in World Order 2.0: A Case Study 209-232
Pedro Alexis Ortiz Celis
Fabio Albergaria

Chapter 11
Intelligence Operations and Gray-Zone Wars 233-258
Oscar Fernando Rubio Ramírez
Jesús María Díaz Jaimes

Chapter 12
Cyber Capabilities in Contemporary Conflicts 259-278
Juan David Zuleta
Andrés Acosta Muñoz

Preface

Major General Jaime Alonso Galindo
Former Director, Escuela Superior de Guerra "General Rafael Reyes Prieto"

Contemporary warfare presents unprecedented challenges. Today, armies face adversaries that are more dispersed than before, operating in gray zone environments marked by threats such as terrorism, cyberattacks, disinformation, destabilization operations, the use of proxies, and neutralization actions employing advanced technological or neurotoxic tools. These attacks are often untraceable to a specific source but have a significant impact and destructive capacity. Additionally, all these elements are combined with a conventional military setting that features highly advanced weapons, drastically transforming the nature of traditional warfare.

The battlefield extends beyond the five traditional domains—land, sea, air, space, and cyberspace—to include the cognitive domain, where a hyperconnected society creates ideal conditions for disinformation operations. Additionally, highly irregular actions infiltrate these traditional domains, altering how military operations are conducted. The power of satellite-based information, unmanned aerial and naval vehicles capable of launching swarm or herd attacks, depleted uranium projectiles or hypersonic missiles, and advanced battle management systems combine with traditional weapons to form an operational environment never seen before.

In this context, Special Operations and Intelligence play a leading role. These highly adaptable, flexible, interoperable, covert, and technologically advanced units, with exceptional differential capabilities and the ability to operate behind enemy lines or in the most challenging environments, are essential for confronting and defeating today's adversaries. However, it is necessary to reconsider their approach. Clearly, it is important to evaluate whether the capabilities of surgical strikes or special warfare—critical aspects of Special Forces—are sufficient to meet these challenges. Similarly, Intelligence must adapt to increasingly global environments, ensuring that tactical and operational intelligence align more closely

with strategic intelligence. The quality, complexity, and speed of information have become vital factors for success. Ultimately, it becomes evident that in today's wars, Intelligence and Special Forces must operate in a far deeper symbiosis than traditionally envisaged, nearly erasing the boundary that separates them.

This is where the significance of this book lies. This work, resulting from four years of academic reflection and research by the Army Department of Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) on Special Forces doctrine and challenges, raises some of the most current and impactful debates on the use of these units and Intelligence in today's wars. These contributions are compelling due to the specificity of the subject and the limited number of studies, from an academic perspective, on the universe of Special Operations.

Introduction

Luis Alexander Montero Moncada
Editor

This book offers a comprehensive analysis of the challenges facing Special Forces in a constantly changing world. In a global context where warfare has evolved, the book examines how Special Forces must adapt to a military environment that is not only dynamic but also shaped by technology, connectivity, and outdated doctrines.

Historically, Special Forces have been a vital part of any nation's military strategy. However, today, their importance has increased due to new technologies and warfare tactics. Modern warfare is no longer just about traditional combat; it has become a multidimensional battlefield involving cyberattacks, drones, artificial intelligence, and psychological operations. This shift has created an environment where Special Forces must operate in conditions of uncertainty and complexity, necessitating a comprehensive review of their doctrines and strategies.

One of the most prominent aspects of the book's discussion is the impact of new technologies on warfare. The incorporation of artificial intelligence and automation into military operations has changed the way missions are planned and executed. Special Forces must learn to integrate these technologies into their operations, which not only entails a change in training and education, but also in the mindset of special operators. The ability to quickly adapt to emerging technology has become a strategic imperative. Furthermore, Special Forces also face the challenge of operating in extremely changing environments. The nature of today's conflicts, which are often hybrid and asymmetric, requires these units to be flexible and able to adapt to unforeseen situations.

The hyperconnectivity of modern society presents unique challenges for Special Forces. Social media and other digital platforms have altered how information is shared and how public perceptions are shaped. In this context, Special Forces must not only carry out covert operations but also handle the challenges of information

and narrative management. Information warfare has become a vital part of any conflict, and Special Forces need to be ready to engage in this new form of warfare.

Although the book centers on the Colombian Special Forces system, its analysis holds global relevance. The challenges faced by Colombian Special Forces reflect broader international trends impacting all nations. The need for updated doctrines and innovative approaches to training and operations is a common theme in the international military community. Consequently, this book becomes a valuable resource not only for Colombia but also for any country aiming to understand and adapt to the realities of modern warfare.

Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare is more than just an analysis; it is a call to action for Special Forces to reevaluate their tactics and strategies in a rapidly evolving world. By addressing technological, operational, and social challenges, the book offers a roadmap for the modernization and adaptation of Special Forces, ensuring they stay effective and relevant in an ever-changing security landscape.

Finally, the book results from the research conducted by the Army Department of Escuela Superior de Guerra "General Rafael Reyes Prieto," as part of the project "Nature of Contemporary Warfare: Challenges and Opportunities for Special Forces and Intelligence." This research was supported and supervised by the Colombian Joint Special Operations Command (CCOES), an elite unit comprising the Special Forces of the Colombian Armed Forces and the United States Joint Special Operations University (JSOU).

Chapter 1

Special Forces in Contemporary Warfare*

DOI: https://doi.org/10.25062/9786287818408.01

Jorge Serna
Luis Alexander Montero Moncada
Miguel Antonio González
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Special Forces units are among the most vital assets of a modern army. This assessment relies not only on their high level of expertise and combat ability but also on the fact that, by their very nature, they are the most effective and suitable component for handling asymmetric and hybrid combat scenarios, which are prevalent in modern warfare. In this context, the capabilities of the Colombian Special Forces provide them with a strategic advantage in projecting power or engaging in combat operations alongside other groups or as part of international coalitions.

Keywords: international conflict; defense; Armed Forces; war; urban warfare; propaganda.

* 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. It was submitted as a graduation requirement by Major Jorge Serna for the Master's in National Security and Defense at Escuela Superior de Guerra "General Rafael Reyes Prieto." The views expressed are those of the authors and do not necessarily reflect those of the participating institutions.

Jorge Serna
Major in the Colombian National Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia.
Email: **jorge.sernaos@buzonejercito.mil.co**

Luis Alexander Montero Moncada
PhD candidate in Political Studies, Universidad Externado de Colombia, and PhD candidate in Political Studies and International Relations, Universidad Nacional de Colombia. Master's (*honoris causa*) in Strategic Intelligence, Escuela de Inteligencia "Brigadier General Ricardo Charry Solano", and Master's in Analysis of Contemporary Political, Economic, and International Issues, Sciences Po, Universidad Externado de Colombia, and Colombian Ministry of Foreign Affairs. Bachelor's in Political Science with an emphasis on International Relations, Universidad Nacional de Colombia.
https://orcid.org/0000-0003-3420-0863 - Email: **luis.montero@esdeg.edu.co**

Miguel Antonio González
PhD candidate in Strategic Studies, Security, and Defense, 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. Lecturer and researcher, Army Department, Escuela Superior de Guerra "General Rafael Reyes Prieto," and lecturer in 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: Serna, J., Montero Moncada, L. A., & González, M. A. (2025). Special Forces in Contemporary Warfare. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 13-30). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.01

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 changing nature of war has become a recurring theme in military studies. From classical authors such as Carl von Clausewitz to contemporary ones like Kaldor (2001) and Münkler (2002), researchers have concentrated on examining the mutations in conflicts and the factors—both exogenous and endogenous—that influence this process. From a chronological analytical perspective, there is consensus that the Cold War marks a milestone in accelerating changes toward *new wars,* as this period experienced an increase in phenomena such as the decline of interstate wars in favor of irregular conflicts sponsored by non-state actors, "warlords," and, consequently, the rise of asymmetric warfare.

The privatization of war violence in the hands of non-state actors (Münkler, 2002) presents new challenges for the military because it alters the theater of war operations. Irregular warfare blurs traditional battlefronts, reduces large-scale battles in favor of isolated actions, and removes the clear divide between tactical and strategic levels. Therefore, this chapter aims to analyze the role of Special Forces (SF) in hybrid and asymmetric scenarios, particularly in *new wars*. The working hypothesis is that, because of their flexible, mobile, adaptable, and self-sustaining nature, along with their high capacity to strategically influence a campaign, SF is the most effective and appropriate tool for countering the emerging threats posed by this new reality.

SF units are composed of the most select personnel, undergo demanding training, and therefore form the military elite. They are the most important strategic assets of modern States because their operational results significantly surpass the investment in each unit. SF typically operates in small groups, enabling them to maneuver in a sustained, agile, and versatile manner within the theater of operations. Furthermore, due to their rigorous training in diverse areas (hand-to-hand combat,

parachuting, diving, telecommunications, survival in various conditions, use of weapons, etc.), they are crucial in supporting missions in conventional wars and play a leading role in asymmetric and hybrid conflicts.

To develop this argument, the chapter is divided into three sections. The first, titled "Characterizing Asymmetric Warfare and Hybrid Warfare Scenarios in the Contemporary International System," explains the new global context as a result of the historical evolution of the art of war and identifies the asymmetric and hybrid elements on which SF focuses. In fact, *new wars* are being fought in an increasingly volatile, uncertain, complex, and ambiguous (VUCA) environment, where special forces must operate.

The second section, "Doctrinal Elements that Make Special Forces Ideal for Use in Asymmetric Warfare and Hybrid Warfare," aims to define, based on doctrine, these combat capabilities that distinguish SF. It emphasizes their interoperability, mission-type command, and the rigorous training that units undergo. After examining the framework of contemporary warfare and the key features that set SF apart, the final section, "The Use of Special Forces in Asymmetric Warfare and Hybrid Warfare Scenarios," offers examples of how Special Operations have been employed in recent conflicts.

Characterizing Asymmetric Warfare and Hybrid Warfare Scenarios in the Contemporary International System

In the field of security and defense studies, especially in military studies, there is a wealth of literature dedicated to interpreting the phenomenon of war. In contemporary times, William Lind's (2005) now classic proposal on *fourth-generation warfare* stands out: the evolutionary line begins with first-generation war, characterized by the consolidation of the idea of the State, rigid organization into armies, and the pursuit of the decisive battle. Second-generation war, on the other hand, is defined by the effects of the "age of revolutions," where, although inflexibility in maneuvering and battlefront actions with very large armies persisted, new concepts and doctrines were also introduced. Third-generation war involves a completely new approach, based on principles of flexibility, maneuver, elasticity, speed, and a new dimension of mission-type command, which enabled the use of army groups and corps in an agile and dynamic manner. In this regard, Aznar

(2015) complements the discussion on this generation of warfare by stating that it is based on technology, while the defining factor of the fourth generation is globalization and the return to man (p. 7).

Thus, Lind's (2005) contribution introduces new concepts about the nature of war, which are combined with post-World War II conflicts characterized by bipolarity. In this way, polemology became part of the discussion on the best ways to understand and confront wars that do not involve the clash of large armies.

The concept of *irregular warfare* is therefore linked to *protracted people's war,* a term coined doctrinally by the leader of the Chinese Revolution, Mao Tse-tung, who developed the transition from guerrilla warfare to movement warfare and later to positional warfare through this protracted strategy to seize power.

In fact, Mao already emphasized mobility as an essential factor in guerrilla warfare, so that even his response—the doctrine of counterinsurgency and later that of low-intensity conflict—should tend toward the same element. In this regard, Mao Tse-tung (1967) considered:

> The question of the initiative [and the flexibility of irregular forces] is even more vital in guerrilla warfare. For most guerrilla units operate in very difficult circumstances, fighting without a rear, with their own weak forces facing the enemy's strong forces, lacking experience (when the units are newly organized), being separated, etc. Nevertheless, it is possible to build up the initiative in guerrilla warfare, the essential condition being to seize on the enemy's three weaknesses. Taking advantage of the enemy's shortage of troops (from the viewpoint of the war as a whole), the guerrilla units can boldly use vast areas as their fields of operation. (p. 175)

This issue has also been examined from different angles. For instance, according to Miron (2019), irregular wars, as a new and common operational scenario, differ significantly from traditional wars.

> [...] unlike traditional wars, they mainly refer to the *modus operandi* used by one or all of the belligerents. This *modus operandi* is often favored by the weaker side and involves surprise attacks, guerrilla tactics, and terrorism to reach a political goal. They are often linked to non-state actors who do not have a monopoly on the legitimate use of force. (p. 459)

Although this concept is linked to guerrilla movements that emerged during the Cold War, in some cases, its theoretical importance extended beyond the

1960s and can still be seen today, such as in Colombia. When the Cold War ended, understanding the nature of war had to shift toward studying what Lind (2005) defined as fourth-generation warfare, in which

> [...] decentralization and initiative [are maintained] [...], but in other respects, the fourth generation represents the most significant change since the Peace of Westphalia. In fourth-generation warfare, the State no longer holds a monopoly on war. Globally, armed forces are now combating non-state enemies like al-Qaeda, Hamas, Hezbollah, and the FARC. In nearly every case, the State is losing. (p. 15)

The author therefore provides an analytical framework for outlining the new post-Cold War conflicts, which are much more irregular and amorphous and involve a large number of non-state actors. Lind (2005) explores the characteristics of these confrontations in greater detail and suggests that

> [...] Fourth-generation warfare is also marked by a renewed focus on cultures, not just conflicts between States. In fourth-generation warfare, invasion through immigration can be as threatening as an invasion by a national army. (p. 14)

In this regard, asymmetric warfare is understood as a set of operational practices that aim to deny the advantages and exploit the vulnerabilities of the stronger party, rather than seeking direct confrontation (Herman, 1997). However, this perspective is debated by authors such as Cabrerizo (2002) and Lind himself (2005), since asymmetry cannot be limited to a disparity in firepower that causes operational blurring; rather, it goes much further and includes highly irregular aspects within the armed component, supported by psychological, social, and even communicational factors. This fundamental error in approach also influences views like that of Verstrynge (2005), who dramatically reduces asymmetry to force disparity. For the author, "asymmetric conflicts are simply confrontations between forces of different capacity and size, and as such, they employ different strategies, with the weaker party often resorting to methods beyond the conventional" (Verstrynge, 2005, p. 72).

However, Verstrynge (2005) is correct in his specific characterization of asymmetric warfare, which helps us understand the use of armed forces as a response by the State to this type of adversary. In fact, Verstrynge's (2005) postulates suggest a flexible, highly agile, self-sustaining, and nearly invisible

response with very high combat power, without relying on traditional, heavy, and immobile formations. According to Verstrynge (2005), the characteristics of an asymmetric adversary are as follows:

a. Using techniques that differ from conventional and ineffective ones
b. A non-national or transnational base, which makes identification and location difficult
c. Freedom to choose the ground or area of operations to make it difficult for the adversary to apply its greatest power
d. The predominance of surprise
e. Prioritizing irregular actions that involve very low costs compared to the strategic effect that can be achieved
f. Having a centralized command that is complemented by decentralized and autonomous operational units, which allows for operational flexibility and a sense of control
g. Not being bound by the laws of war or international humanitarian law (IHL)
h. Emphasizing physical attacks that undermine the credibility of States
i. Involving the civilian population as much as possible
j. Designing operations in such a way as to maximize visibility and media coverage
k. Prolonging actions as long as possible to wear down the strongest adversary

Clearly, this playbook indicates that a traditional military unit cannot effectively face an asymmetric adversary, necessitating a more adaptable and decisive force. These are exactly the SF groups.

This approach is further developed by Metz and Johnson (2001), who emphasize that it is necessary to make the military power of an operation more flexible in order to ensure success. Clearly, the operational experiences of the United States, especially those in Iraq and Afghanistan, illustrate this perspective, particularly when considering how Metz and Johnson (2001) characterize the asymmetric adversary:

> Acting, organizing, and thinking differently than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative, or gain greater freedom of action. It can be political-strategic, military-strategic, operational, or a combination of these. It can entail different methods, technologies, values, organizations, time perspectives, or some combination of these. (p. 24)

At the local level, Sánchez et al. (2012) emphasize the importance of interoperability, flexibility, and sustainability for troops engaged in asymmetric warfare. According to the authors, it is crucial for States to consider factors such as combat survivability platforms and dynamic resilience that support mobility and sustainability.

Beyond military science and shifting the discussion to international relations, two concepts connected to contemporary studies of war, within the framework that Kaldor (2001) and Münkler (2002) classify as *new wars,* are essential to the analysis in this chapter. Although somewhat abstract, this definition implies a transition where States are no longer the sole controllers of the resource of war—which they held since the emergence of modern international relations starting with the Treaty of Westphalia in the seventeenth century—and are partially transferring this power to private, subnational, or even tribal actors.

The asymmetry, which refers to the disparity between combatants, is explained by the fact that the costs of war are reduced, making weapons easier to obtain. As a result, small insurgent groups can acquire weapons from the black market more easily and quickly. Furthermore, as conventional combat becomes less relevant, combatants turn to other, weaker targets such as civilians (Münkler, 2002, p. 4).

Although less precise than in military sciences, the definitions of Kaldor (2001) and Münkler (2002) also show that facing these challenges requires forces that differ from traditional ones, more aligned with the capabilities of SF. This issue worsens when actors involved in asymmetric warfare supplement it with conventional means, creating much more challenging scenarios. This combination leads to the emergence of a new concept: *hybrid warfare*.

Since the first approaches to this notion, it has been suggested that hybrid refers to combining conventional capabilities with the use of special warfare and SF units. For this reason, Robert G. Walker (1998) referenced the Fleet Marine Force Manual Warfighting FMFM-1 to highlight that "twenty-first-century wars will be characterized by an intimate blend of conventional and special actions" (p. 36).

For his part, Hoffman (2009), the precursor of the concept, stated that hybrid wars

> can be conducted by both states and a variety of nonstate actors. Hybrid threats incorporate a full range of modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder. (p. 35)

Hoffman's (2009) perspective is visionary because it paves the way for conceiving the use of SF in combined scenarios of conventional and asymmetric warfare. From his perspective, these units are more relevant than ever, an idea that was reaffirmed in the 2006 war between Hezbollah and Israel, where the Shiite militia's approach demonstrated the effectiveness of combining flexible and conventional actions.

Subsequently, Guillem Colom (2012) collected and refined Hoffman's ideas, as well as those of Wilkie and Lasica, to define hybrid warfare as

> [...] the full integration in time and space of typically conventional procedures with tactics typical of irregular warfare (from classic ambushes or propaganda, agitation, and insurgency actions to information warfare, lawfare, or cyberwarfare), the latter mixed with terrorist acts and connections to organized crime to obtain support and assistance of all kinds. (p. 80)

Here, the distinctive feature of using SF also comes to the forefront, as they are the most effective and powerful means of countering irregular warfare. The historian takes one of Hoffman's analytical elements (2009) and draws on history to assess the novelty of the hybrid. In this regard, Thomas Huber (1996)

> [...] describes the phenomenon of regular and irregular forces fighting in a coordinated manner. Huber explains compound warfare as an intellectual framework for understanding the phenomenon of conventional (regular) forces and unconventional (irregular) forces operating under unified command in order to achieve the desired end state. (García et al., 2015, p. 3)

Although there is a historical tendency to combine conventional and irregular actions, this is not enough to suggest that hybrid warfare has already been used or is common. Conversely, the modern demands of asymmetric combat mean its hybrid features require the use of SF.

Once the theoretical and conceptual foundations guiding this chapter are established, it becomes clear that the increasingly rapid flows of interactions and changes in the international system significantly impact the way contemporary wars are understood theoretically. The evolving and complex nature of threats makes it difficult for experts to define them precisely, which affects the very concept of international security and the strategies used to wage war.

In the practical field, the strategic thinking of some political leaders enables measures to be taken to counter threats that violate sovereignty or internal

political order, but this can generate domestic and international tensions. A specific example can be found in the so-called rogue States: Cuba, Iran, Nicaragua, North Korea, Syria, and Venezuela. A critical reading of this designation can be found in Chomsky (2000), who asserts that rulers maintain a wide range of strategies to achieve their objectives or interests, which generally result in the sustainability of their regimes. The geopolitical location of rogue States allows for a relatively uniform distribution of sources of tension within the current international scenario, which, combined with internal tensions—common in developing countries—that are fueled by some sectors, causes chaos and instability. The presence of illegal economies derived from drug trafficking, illegal mining, arms trafficking, and human trafficking, among many other factors, increases the destabilizing effect on the State, as they acquire significant resources to carry out terrorist actions.

Likewise, globalization has deepened in the modern international system, enabling new alliances to form within a diffuse and complex global order where new leaders challenging the power of the United States have emerged since the end of the Cold War. As a result, the world is moving toward a multipolar order, with the rising influence of China—and to some extent Russia—indicating the potential for a new theater of large-scale confrontation, including new forms of hostilities such as digital warfare. All of this presents, once again, an ideal scenario for SF.

Doctrinal Elements that Make Special Forces Ideal for Use in Asymmetric Warfare and Hybrid Warfare

SF or Elite Corps are military units trained in specialized skills, known for their agility and versatility in executing missions. They perform specific tasks and are responsible for duties that require tougher, more mechanical, intensive, and rigorous training compared to regular troops. Unlike conventional units, SF utilizes more advanced equipment that ensures maximum firepower and provides them with more comprehensive, clear, and timely intelligence about their targets.

These agile and versatile units receive more extensive training and have access to advanced technological resources compared to other forces. An SF unit is trained to perform direct or indirect close combat, sabotage, infiltration, intelligence gathering, and special reconnaissance missions. Therefore, it can be argued that SF units are the best option available to the Armed Forces for

confronting asymmetric or hybrid threats, which have the highest likelihood of success and globally undermine the security of States.

By their nature, SF units are designed to make decisive tactical contacts of strategic importance and emerge victorious as they infiltrate deep into enemy territory or highly dynamic areas, relying on their own capabilities rather than fire support or other conventional units during the operation. They require maximum surprise, agility, organizational and maneuvering flexibility, as well as self-sufficiency in logistics and power.

SF should be regarded as assets of high strategic importance for States, as their training enables them to carry out missions vital to a country's survival, integrating tactics and strategy in operations ranging from offensive actions to covert reconnaissance for information gathering. They can also operate independently or alongside conventional forces and other government agencies. These units require minimal resources, being small with targeted missions that can produce a decisive impact on superior military adversaries with surgical precision and efficiency. In essence, Special Operations are conducted to support a specific theater of operations or to target strategic or high-value objectives. As Sigüeñas warns (2018),

> […] most special operations are designed to improve the chances of success of a military campaign in an area of operations or war. Likewise, these multidisciplinary or joint operations, although they can be conducted independently, are planned and carried out as joint operations due to the requirement for multiple specialized skills on a routine basis to support and coordinate the operation. (p. 56)

Due to their fundamental characteristics, SF carries out tasks primarily aimed at new wars. In both asymmetric and hybrid warfare, SF projects its capabilities in unconventional confrontation scenarios because its flexibility and interoperability are ideal for confronting enemies that are equally flexible and diffuse, such as those that predominate in these types of warfare.

In addition, the training and capabilities of SF in counterterrorism, intelligence, and espionage in hostile theaters of operation prevent criminal acts, such as large-scale attacks, whose targets seek to impact the civilian population. Consequently, their special skills and capabilities should not be used in tasks or missions that wear them down, as conventional troops can carry out these actions. In this regard, Trejo (2018) points out that

> […] currently, Special Forces—in addition to their specific training in conventional operations—specialize in the fight against terrorism, which constitutes the main threat to developed countries. These forces have demonstrated flexibility and adaptability, but above all, ingenuity and creativity in carrying out their missions. (p. 49)

Special operations have both strategic and operational implications. Therefore, operational planning is based on specific knowledge of the target in order to exploit it more effectively, as the effort is focused entirely on rapid and accurate attacks, thereby distinguishing it from other groups that employ conventional warfare. In other words, tasks must be carried out using tactics, techniques, and procedures to plan, prepare, and execute special operations at any time and place, autonomously and self-sustainably.

In the context of military operations doctrine, it is noted that Special Operations are conducted in hostile, denied, or sensitive environments for the purpose of achieving military, political, economic, diplomatic, and/or informational objectives. Besides, these actions utilize military capabilities that do not necessitate the involvement of conventional forces and require total discretion, clandestinity, and low visibility. Thus, it is possible to affirm that SF is the asymmetric component within a state force.

This approach has involved a profound and constant change in the doctrine and structure of the Armed Forces, as it seeks to adapt this force potential to new asymmetric and hybrid scenarios. To this end, these special troops receive training to deal with domestic, subnational, tribal, ideological, terrorist, irregular, militia, convergent, international, or transnational threats.

Both asymmetric warfare and hybrid warfare are constantly evolving, so Special Operations units must keep pace with their advancement to counteract or prevent any hostile act. For this reason, the approach and work of an SF group must be entirely proactive, allowing it to continuously adjust its capabilities, doctrine, equipment, and power in response to the mutations presented by asymmetric and hybrid adversaries.

In this respect, terrorism, for instance, most often relies on surprise as a determining factor in committing violent action. States attempt to counter such acts with specialized and dominant intelligence against each of their threats, whether internal or external. However, it is through the direct action of SF groups that they can target and dismantle strategic organizations, often with highly camouflaged structures.

Consequently, States must apply the necessary doctrinal elements to confront emerging threats, among which SF holds a special place. For their part, the context of multilateral forces calls for broader training, as they must assess the enemy forces they may face, which increases their combat capabilities.

It is clear, then, that SF is of paramount importance to the Armed Forces, as well as for the development of unconventional operations by land, sea, or air, and even in cyberwarfare scenarios, during internal or external conflicts among nations. These activities include offensive raids, demolitions, reconnaissance, counter-terrorism, and search and rescue operations. As mentioned, in addition to their constant rigorous training, members of SF often have specialized skills in swimming, diving, parachuting, survival, emergency medicine, and foreign languages.

The capabilities of these units must continually improve to respond to the relentless evolution of contemporary warfare, making it possible to say that they make a difference in the environments of new wars. Historically, the SF doctrine involves characteristics such as:

- Remaining calm in high-stress situations.
- Working as part of a highly specialized team.
- Being fully prepared to face very demanding challenges.
- Facing the greatest possible danger without the possibility of immediate support and with limited resources.

At the regional level, following World War II and as part of the agreements of the Inter-American Treaty of Reciprocal Assistance, Latin American armed forces implemented a series of changes to their organizational structures and doctrine, aiming to create Special Operations Forces that could meet the challenges of the post-war era. Today, these forces, especially those in Colombia, have achieved a position of prestige in the region thanks to their decisive actions (Lauriani, 2017, p. 26).

Use of Special Forces in Asymmetric Warfare and Hybrid Warfare Scenarios

Based on the doctrinal analysis conducted so far, it can be said that SF is distinguished by its focus on strategic operations, offering greater security than any conventional, simple, surprising, or rapid operation. They thoroughly develop flexibility and adaptability, possess a high degree of autonomy, initiative in combat,

and clear innovation. These characteristics enable these units to achieve a more significant and decisive impact than much larger conventional units.

Regarding the operational approach, SF develops critical capabilities to operate in special warfare scenarios and conduct surgical strikes. The former are characterized by being carried out in permissive, uncertain, or hostile operational environments, either alone or in conjunction with other formations. The latter are precise, limited, and rapid actions aimed at capturing, defeating, controlling, or recovering a target of operational or strategic interest.

Additionally, SF units are designed to operate in operational environments and on missions that involve clear time constraints, mandatory isolation from other components, the constant need to exploit opportunities at will, mandatory decentralization in mission execution, constant initiative, and strong interdependence between special teams to synchronize or complement efforts. Only in this way can SF groups be projected toward operational success.

Precisely this concept has been applied for decades in armies such as the US and British armies, which conduct small-scale contingency operations that integrate all SF capabilities, clearly demonstrating their high value in asymmetric and hybrid warfare.

For this reason, an operational evaluation of SF groups in different contexts can show that most have achieved notable results. This is because, before executing a mission, planning and, especially, analyzing courses of action conceive scenarios with a high success rate. To this end, highly detailed information matrices are used, including all the probabilities that may arise during the mission's development, to assess the chances of success.

The communication factor, typical of asymmetric wars, is also considered in the impact of SF. Information about Special Operations that is released to the public and subsequently reaches the enemy is shared in a restricted manner to ensure the mission's efficiency and effectiveness, while also allowing for the psychological impact of the operation to be managed in accordance with the political objective. Therefore, in most cases, nothing is known about Special Operations until they are executed. Details of these actions are often withheld to prevent information from leaking to adversary organizations, which conduct criminal intelligence by analyzing data presented in the media and using it to counter SF or modify their criminal practices.

In the contemporary context of both asymmetric and hybrid wars, there are paradigmatic Special Operations that demonstrate the capabilities and constant

training of these elite units. Therefore, it is necessary to maintain their evolution and manage their interventions appropriately, as a select group can make a significant difference in a war and reduce the number of human losses, which are often unnecessary.

In various war contexts, SF groups have played a crucial role in defending the State or carrying out a specific mission by a multilateral force deployed worldwide. While it is true that not all States have military forces, they do require an allied country to protect them with its special capabilities, ensuring that there are no hostile actions or terrorist attacks from other States or organizations.

In this regard, it is worth emphasizing that the doctrinal approach of SF facilitates interoperability among States that have military or cooperation agreements, ensuring they can react to a threat in a coordinated and planned manner in the future. These peculiar characteristics of interoperability and flexibility are characteristic of asymmetric adversaries when they build their regional or even transnational networks. Thus, SF can balance this adversary status by conducting military exercises, which determine cooperation and measure the potential of SF operations in any context of contemporary war or action.

All of this not only strengthens the joint fight against the transnational threats that States face at all times, but also allows for the exchange of information and verification of areas of mutual interest, such as terrorism, drug trafficking, human trafficking, and arms trafficking. Therefore, this process of transformation and adaptation of SF to new scenarios that threaten national and comprehensive security in the contemporary 21st-century context, highly marked by asymmetry and hybridity, must continue and improve.

Thus, SF operations in most countries consist of hybrid and asymmetric (non-conventional) warfare missions, including foreign internal defense, special reconnaissance, direct action, counterterrorism, combat search and rescue, counternarcotics operations, hostage rescue, humanitarian assistance, information operations, and psychological operations. SF operations have the capacity to ensure that they will be the first on the ground or even assemble in a crisis area when a threat begins to take shape.

Conclusions

Contemporary warfare is basically characterized by two types of confrontations: asymmetric and hybrid. These wars have a highly irregular, flexible, and delocalized

component, based on agile, easily camouflaged groups with high impact power. Without a doubt, this type of adversary represents a serious challenge for conventional units, as their vast power and sheer size offer little advantage.

In response to this difficulty, SF groups are precisely the units that most closely align with the operational concepts required in asymmetric and hybrid conflicts. Their flexibility, small size, and significant firepower, combined with operational sustainability capabilities, enable them to successfully understand and combat adversary organizations in these operational environments.

In this regard, SF groups are not only one of the most important assets of the Colombian Armed Forces, but also, due to their experience, doctrine, training, and combat achievements, offer a window of opportunity for the State. It is therefore clear that this asset could contribute to the country's security and defense and become an international benchmark for professionalism, capabilities, and military power.

References

Aznar, F. (2015, November 25). *Las generaciones de guerras: Guerras de primera generación (I)* [Analysis document, No. 54]. Instituto Español de Estudios Estratégicos. https://tinyurl.com/5yca9se5

Chomsky, N. (2000). *Rogue States: The rule of force in world affairs*. Pluto Press.

Colom, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova, 10*(10), 77–90. https://doi.org/10.21830/19006586.228

García Guindo, M., Martínez, G., & González, V. (2015). *La guerra híbrida: Nociones preliminares y su repercusión en el planeamiento de los países de las organizaciones occidentales* [Working paper]. Instituto Español de Estudios Estratégicos. https://tinyurl.com/bdh8njt9

Herman, P. (1997). Asymmetric warfare: Seizing the threat. *Low Intensity Conflict & Law Enforcement, 6*(1), 23–45.

Hoffman, F. (2009). Hybrid warfare and challenges. *Joint Force Quarterly, 52*(1), 34–39. https://tinyurl.com/42ne9y2d

Kaldor, M. (2001). *Viejas y nuevas guerras*. Tusquests.

Lauriani, C. (2017). Operaciones Especiales: Una respuesta multidimensional al problema de seguridad multidimensional de Latinoamérica. *Military Review,* (second quarter), 20–30. https://tinyurl.com/5n8umnnz

Lind, W. (2005). Comprendiendo la guerra de cuarta generación. *Military Review,* (January–February), 11–17. https://tinyurl.com/y2uzpd6d

Metz, S., & Johnson, D. (2001). *Asymmetry and US Military Strategy: Definition, background and strategic concepts*. Strategic Studies Institute. https://apps.dtic.mil/sti/tr/pdf/ADA387381.pdf

Miron, M. (2019). La guerra irregular, insurgencia y cómo contrarrestarla: Una perspectiva comparativa entre los enfoques centrados en el enemigo y en la población. *Revista Científica General José María Córdova, 17*(27), 457–480. https://doi.org/10.21830/19006586.497

Münkler, H. (2002). *Viejas y nuevas guerras: Asimetría y privatización de la guerra*. Siglo XXI.

Sánchez, J., Montero, L., Ardila, C., & Ussa, A. (2012). Discusión epistemológica de la guerra asimétrica: Adopción contemporánea de la asimetría interestatal. *Revista Científica General José María Córdova, 10*(10), 91–05. https://doi.org/10.21830/19006586.229

Sigüeñas, O. (2018). Tareas operacionales de las Fuerzas Especiales: Optimizar el desempeño operativo del componente de Fuerzas Especiales del Comando Especial del valle de los ríos Apurímac, Ene y Mantaro. *Air & Space Power Journal,* (fourth quarter), 55–61. https://tinyurl.com/u75yxtnw

Trejo, P. (2018). Tropas de Operaciones Especiales: Herramienta útil para las guerras del futuro. *Visón Conjunta, 10*(19), 47–55. https://tinyurl.com/ycxd2vuh

Tung, M. T. (1967). *Selección de escritos militares*. Ediciones en Lenguas Extranjeras.

Verstrynge, J. (2005). *La guerra periférica y el Islam revolucionario: Orígenes, reglas y ética de la guerra asimétrica*. El Viejo Topo.

Walker, R. (1998). *SPEC FI: The United States Marine Corps and Special Operations.* Naval Postgraduate School.

Chapter 2

In the Mind of the Strategist: Identifying the Strategy Applied to the Target Acquisition System*

DOI: https://doi.org/10.25062/9786287818408.02

Helver Orlando Cepeda Daza
Oscar Leonardo Reyes Pulido
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: The strategic scope of the impact exerted by Colombian Special Forces units has allowed them to be recognized as a relevant tool that can be employed in military operations. The achievement of strategic objectives is the result of a combination of experience and the application of doctrine. This creative thinking, developed by Special Forces strategists, has enabled their tactical and operational development. This study describes the systemic approach to strategy applied to one of the critical capabilities of Special Forces operations: surgical strikes. Using the DOTMLPF military scientific method, the capabilities built by the Colombian Special Forces are analyzed. Finally, a conceptual model is presented that identifies the strategic capabilities of the process, drawn from case studies with interoperable characteristics for other Special Forces units.

Keywords: target acquisition; operational art; strategy; interoperability; 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.

Helver Orlando Cepeda Daza

Lieutenant Colonel of the Colombian Special Forces with twelve years of experience as a Special Operator. Master's in Strategy and Geopolitics, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Security Cooperation and Special Operations Planning from the U.S. Joint Special Operations University (JSOU). Graduated from the John F. Kennedy Special Warfare Center and School at Fort Liberty, United States. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Multinational Liaison Officer for the U.S. Special Operations Command (SOCOM). Email: **helver.cepeda@buzonejercito.mil.co**

Oscar Leonardo Reyes Pulido

Retired Major in the Colombian National Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Human Rights and International Humanitarian Law, Universidad Externado de Colombia. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Lawyer, Universidad Militar Nueva Granada, Colombia. Research Professor, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia.
https://orcid.org/0000-0001-6341-0283 - Email: **oscar.reyesp@esdeg.edu.co**

APA Citation: Cepeda Daza, H. O., & Reyes Pulido, O. L. (2025). In the Mind of the Strategist: Identifying the Strategy Applied to the Target Acquisition System. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 31-60). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.02

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 organizational architecture of the Colombian Special Operations Forces (hereinafter SF) has been characterized by its constant evolution to carry out unconventional operations. These modifications have enabled them to adapt to prevailing factors in the contemporary operational environment, including the evolving threat landscape and the most adverse, hostile, and dynamic geographic environments. Furthermore, the constant evaluation of threat systems has enabled them to identify tactical actions that are unique in terms of time, space, and purpose, thereby achieving strategic impact objectives in non-permissive, uncertain, and denied environments.

Specifically, this work addresses the evolution of the tactical capabilities of the SF from a scientific perspective, as described in military doctrine as DOTMLPF: Doctrine, Organization, Training, Material, Leadership and Education, Personnel, and Facilities.[1] Furthermore, it is taken into account that although the application of the strategic level—in which interdependence and integration are managed—has been customary in operational art, this does not blur its importance in teaching processes, which is used by models such as that of the United Kingdom (Montero et al., 2019).

In this regard, given that this British model has also influenced the procedures, tactics, and techniques of SF, the question that motivated this study is the following: How do the characteristics derived from the target acquisition process of the Colombian SF organization to achieve strategic objectives guarantee a degree of interoperability with other SF?

[1] In the North Atlantic Treaty Organization (NATO), they may include an "I" to refer to "Interoperability."

To examine this question, this chapter addresses the evolution of the strategy employed by SF within the strategic conceptual framework. It also analyzes how the latter adapted to the needs of conflict and security and defense policies, since these public policies inevitably shape the designs of the "how" and the "desired end state." Subsequently, the capacity of SF is studied with the aim of contributing to a comprehensive understanding of the Colombian case. For this purpose, the DOTMLPF is used, as the SF organization sought to refine all components of this methodology to ensure a successful target selection process.

Finally, based on a descriptive case study approach, the characteristics of the target acquisition process used by SF are analyzed to ensure effectiveness and interoperability within the Armed Forces. Furthermore, this chapter studies how this model contributes to achieving the strategic objectives of the Higher Command.

The descriptive horizon proposed in this chapter aims to illuminate the unique approaches that the SF strategy employs to develop a military operation. The analysis of specific cases was carried out following the guidelines of the method designed by Yin (1989, as cited in Martínez, 2006), who states that case studies can be descriptive "if the aim is to identify and describe the different factors that influence the phenomenon under study" (Martínez, 2006, p. 171).

Furthermore, this academic document aims to provide references for the *Special Forces Campaign Manual MCE 6-05, Integration, Interoperability, and Interdependence of Special Forces,* which will become a doctrinal document that projects the combat efficiency of SF in their dynamic interaction with conventional forces units and SF of other components of the Military Forces to execute joint and combined operations.

According to the *Army Fundamental Manual MFE 3-05, Special Forces Operations* (Ejército Nacional de Colombia, 2017a), the classification of operations may include *Joint Operations* when carried out with other forces, for example, the SF of the Army and the SF of the Navy, and *Combined Operations* when executed with foreign allied countries. The latter is the case of the Panamax exercise, a military operation conducted by the U.S. Southern Command aimed at developing a deterrent capability against any threat to the Panama Canal.

Contemporary Retrospective Description of the Colombian Special Forces Organization

Colombian specialized literature has identified unique success factors that are essential to ensuring the relevance of Special Operations within the framework of national and general military strategy. Among the available academic works, it is of utmost importance to mention the study published by the Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) entitled *Land Power: 21st Century Armies and Wars.* This study identifies some conditions of the political-military environment at the strategic level that should be considered among the success factors, such as "the identification of critical enemy capabilities to formulate effective military strategies, [...] and the transformation of the Armed Forces and their capabilities through innovation" (Montero et al., 2019, p. 122).

In this regard, it is appropriate to mention at this point the two critical capabilities that SF has developed in the context of the Colombian conflict: surgical strikes and special warfare. These critical capabilities serve as a starting point for visualizing the SF's approach to innovation in target selection and why it can be successful.

The SF organization has maintained substantial and sustained growth since 1970, when the 29th Infantry Battalion "Rifles" was transformed into the "Hermanos Almeyda Special Forces Group," the first unit with unique capabilities (Muñoz & Cano, 2020). This process enabled a transformative innovation in the military capabilities of SF, which revolutionized the way land power was utilized. This comprehensive transformation has allowed the SF organization to remain at the forefront in meeting the demands of safeguarding security and defending national sovereignty. In addition to these changes, SF has been able to transcend its limitations thanks to its alignment with the various security policies of the Executive Branch, which allows it to become a versatile option for targeting centers of gravity across the full range of military operations.

In August 2002, the Democratic Security and Defense Policy (2002–2010) emphasized the importance and projection of robust intelligence with coordination and integration capabilities to ensure its efficiency. Specifically, the doctrine refers to this aspect as *interdependence,* which is defined by the *Army Fundamental Reference Manual MFRE 3-05, Operations,* as the relationship of dependence between elements to maximize their complementary and reinforcing effects (Ejército Nacional de Colombia, 2017c).

However, security policy enables the alignment of national security strategy interests with the government's strategic objectives. Thus, in 2002, the Executive Branch established that intelligence collection, analysis, and dissemination systems should be improved to ensure operational synergy, allowing the Armed Forces to gather information and operate in a timely manner to achieve objectives with strategic implications.

Aligned with this strategic vision, in 2002, the Commander-in-Chief of the Armed Forces issued the order to create an inter-institutional group called "Cancerbero," an actionable intelligence element comprising the National Army, the National Navy, the Colombian Air Force, the National Police, and the Administrative Department of Security (DAS). The permanent objective of the group was to neutralize High-Value Targets (HVTs) using the critical capabilities of SF.

Without a doubt, within the context of strategy, a purpose was established by the strategist in its design and operational art as the desired military end state. They inevitably found it necessary to optimize existing resources and introduce an innovative and decisive capability: long-range reconnaissance, so that the design and implementation would allow SF to execute operations with intelligence collected by themselves.

As organic units of the Army Special Operations Command (ASOC), the Army Command recognized the need to establish a unit comprising small groups capable of conducting special reconnaissance and direct action operations. Thus, units were formed with personnel from the 1st Special Forces Battalion, and other National Army units were invited to participate in the selection process. The latter benefited from the advice of the United States military group, which provided high-tech equipment and specialized materials that enabled them to operate in militarily denied environments, such as communications equipment with satellite technology.

Thus, the 1st "Ambrosio Almeida" Commando Battalion was established, a unit with almost legendary abilities, known as the ghosts of the jungle—individuals with perseverance and self-control that were hard to imagine at the time. Moreover, their skills in HVT reconnaissance were only rivaled by their innovative organization. In this way, small, self-sufficient teams began to set a milestone in the development of special missions.

However, given that such a small unit requires immediate reaction forces with airborne and airstrike capabilities inherent to its organization, a unit was created in 2003 with the most characteristic features of the Colombian soldier: tenacity and combat drive. Thus, overwhelming combat power, agility, and versatility were the

distinctive and inherent capabilities of the Airborne Lancers Group (AGLAN) in its creation and activation.

To achieve HVTs, which is the desired end state, an innovative set of conditions was created, consisting of a scalpel (the Commando Battalion, BACOA) and a hammer (the AGLAN), units that excelled at executing surgical strikes at the time. During that period, the critical intelligence needed by commanders at all levels was provided by teams that delivered information about areas inaccessible to other units and even other institutional capabilities.

During that same year, the need to add units with specific skills to improve the COESE became clear. On May 17, 2005, the Urban Anti-Terrorist Special Forces Group (AFEAU) and the Marine Infantry Special Forces Battalion (BFEIM) joined this command. As a result of this organization, the Unified Special Operations Command (CUNOE) and later the Joint Special Operations Command (CCOPE) were established.

With the creation of these units and under the operational command of the General Command of the Military Forces (CGFM), the strategic management of narco-terrorist organizations was affected by the neutralization of middle-level commands. However, the mission of attacking their center of gravity, i.e., the HVTs, was not fulfilled (CCOES, 2014).

As a result, processes of transformation and innovation began within SF. Following a visit by the Colombian Minister of National Defense to the Israeli Army, the National Special Operations Planning and Intelligence Group was implemented, based on the Israeli model envisioned for 2007. In this context, the Joint Special Operations Command was established by order of the CGFM, comprising 22 officers, 24 non-commissioned officers, and two civilians, all of whom were members of the Army, Navy, Air Force, Police, and DAS (CCOES, 2014).

Thus, during 2007 and 2008, the center of gravity of the narco-terrorist organization known as the Revolutionary Armed Forces of Colombia (FARC) was affected through the planning and development of special operations. Among these, Operation "Sol Naciente" stands out, demonstrating the integration of SF units and the effectiveness of the Air Force (Brigada de Fuerzas Especiales, 2015).

To enhance the capabilities of SF units, external advice was also sought to establish a special operations command. Thus, in September and December 2008, meetings were held with various personalities and advisors from other nations to make memorandums of understanding, develop the initial guide, project the mission and vision, and obtain approval from the recommended organization. This

work continued until January and February 2009, during which the organizational structure, roles, and specific functions of the CCOES were consolidated. Finally, on May 27, 2009, the CGFM deactivated the Joint Special Operations Command (CCOPE) and created the Joint Special Operations Command (CCOES).

In this evolution, it is also important to mention the Strategic Review Committee meeting held in 2014, where key goals were established, including updating doctrine and adopting capabilities-based planning, to define the future of SF and maintain its leadership position. Subsequently, in 2016, the current military doctrine was established, which defines Special Forces Operations as one of the distinctive competencies of the National Army (Ejército Nacional de Colombia, 2016b).

During 2015 and 2016, the CGFM began consolidating the organizational structure of SF. Through the publication of force resolutions and provisions, the CGFM eliminated and restructured some of the most emblematic SF units within its command—the men considered best prepared for war and to confront threats against the Colombian State.

Finally, in December 2016, the Commander of the National Army created the National Army Special Forces Division (DIVFE). As can be seen, in the context of strategic thinking, the pragmatic nature of the strategic culture employed by the Colombian SF is evident, as its sound decisions and evolution have enabled it to adapt and innovate in scenarios characterized by high volatility, uncertainty, complexity, and ambiguity. This is how Gallardo and Faundes (2014) describe it: "In addition to understanding the context, strategic thinking seeks guidelines to influence and shape the scenario" (p. 10).

Analysis of the Colombian SF's DOTMLPF Capability and Its Interdependence with the Target Acquisition Process

First, it is worth highlighting that the target selection and prioritization process is the result of capacity building; therefore, it is essential to describe the capacity that the National Army has built, based on a few key pillars and taking into account its capabilities and limitations (Figure 1). In compliance with the guidelines established by the Ministry of National Defense (MDN) in this planning model, the SF organization optimized the resources assigned to it and evolved around a prospective vision of threats. In this way, it not only adapted but also developed a

competence that the National Army declared distinctive in 2016 (Ejército Nacional de Colombia, 2017a).

Figure 1. *Capacity-Based Planning Methodology*

Source: MDN (2016).

The capacity analysis used by SF to select and prioritize targets will be conducted from a comprehensive DOTMLPF perspective, which encompasses a scientific methodology employed by the National Army to evaluate, innovate, and modernize capabilities. This tool also covers the doctrine, organization, material, personnel, and infrastructure available to the unit to develop its critical capabilities, such as special warfare and precision strikes.

Doctrine

The new doctrine of the National Army defines Special Operations (SO) as military actions conducted by organized, trained, equipped, and certified units, which can execute actions in hostile, militarily denied, and politically sensitive environments (Ejército Nacional de Colombia, 2017c).

Among SO, a series of operations are distinguished that, in turn, are part of the two critical capabilities of SF: special warfare and surgical strikes. These two critical capabilities are developed within a common and interoperable framework according to clear parameters and guidelines, which allow them to integrate and employ concepts of organization, planning, and execution to carry out SO successfully.

The men of the SF of the National Army are governed by rigorous military standardized documents that define the tactics, techniques, and procedures to be

employed by units of a different, "special" nature. These documents transcend the pillars that sustain the organization's legitimacy and constitute its doctrine, which the *Army Fundamental Manual MFE 1-01* defines as the "fundamental principles with their relevant tactics, techniques, procedures, and terms used for the guidance and conduct of military operations" (Ejército Nacional de Colombia, 2016a, p. I). For the SF organization, these principles are translated into standardized documents at the local and regional levels, with the aim of ensuring that allied Military Forces have a common, interoperable language within the shared framework for developing combined operations.

The experience gained from the Colombian conflict has contributed to the development of this current doctrine, as noted by Active Reserve Colonel Pedro Rojas Guevara (2017), director of the National Army Doctrine Center between 2015 and 2018, a master's degree holder in National Security and Defense, and an analyst and lecturer in security and defense issues. In his article "Doctrina Damasco: eje articulador de la segunda gran reforma del Ejército Nacional de Colombia," he states:

> The current doctrine of the Colombian Army is the product of a combination of influences derived from fifty years of armed conflict. Apparently influenced by the United States in its formal aspects, its development has been more closely tied to the facts within an asymmetric context than to theory. (Rojas, 2017, p. 114)

It is then evident that these documents have not only facilitated the conceptualization of the bold and innovative actions performed by SF units but also include categories of information that describe the execution of the processes, that is, the know-how of the critical capabilities of SF. Specifically, Llobregat (2007) and Viloria et al. (2008), as cited in Castaño and Arias (2015), explain that the "organizational know-how includes the knowledge, processes, procedures, and techniques that lead to the achievement of a service that is different and difficult to copy by other organizations" (p. 154). In this regard, the main documents that summarize this knowledge are:

- Army Fundamental Manuals (MFEs), which outline the philosophy of SF, their principles, foundations, and imperatives, as well as the characteristic elements of the operational environments where they can be used.
- Army Reference Manuals (MFREs), which consist of more detailed doctrinal documents that describe the types of operations that SF can execute

and their planning methods. Furthermore, they refer to the operational-tactical level and demonstrate both the capabilities and qualities of the SF organization.

- Field Manuals (MCEs), which explain the specific capabilities of SF operations and expand on the information contained in MFREs on specific capabilities. The MCEs build upon the concepts that the organization needs to further develop.
- Army Technique Manuals (MTEs), which describe in detail the non-mandatory methods used by military units to carry out missions assigned by higher commands. These techniques are applied in a disciplined manner, based on the operational conditions imposed by the scenario.
- Military Training Manuals (MEMs), which provide very precise technical specifications detailing the specific tasks to be performed. An example of this type of document is a manual that describes the techniques and procedures used in a military free-fall jump operation, a procedure that requires precise knowledge and expertise.

Organization

SF comprises around 4,000 special operators with critical capabilities in surgical strikes and special warfare; however, specific locations that characterize their participation cannot be highlighted due to circumstances related to their organizational architecture. As part of the land component of the CCOES, they do not have an assigned theater of operations because it is a Functional Joint Command, a status that allows them to conduct operations throughout the national territory, subject to efficient execution times that guarantee the military response required by the strategic objective.

Specifically, the DIVFE was established in 2016, and together with other components of the Air Force and the National Navy, it represents a strategic trident for the Colombian Military Forces, reflecting the organization's interoperability, interdependence, and collaborative nature through the CCOES. These characteristics are part of the organization's DNA, allowing it to exploit unique and exclusive capabilities, as well as strategic resources, in a decisive manner at the right time and place across the full range of military operations.

Furthermore, the DIVFE, as the land component of the CCOES, is supported by a modern and functional structure to meet all the requirements imposed by SO to be conducted by SF, as it is the unit responsible for centralizing their planning.

In its ongoing quest to refine the target acquisition process, the DIVFE utilizes a system described by the acronym F3EAD: focus, fix, finish, exploit, analyze, and disseminate. This cycle enables it to anticipate and decipher ambiguous scenarios in which the threat may operate (Ejército Nacional de Colombia, 2017a).

This process enables the DIVFE to identify, locate, and neutralize the threat, as well as conduct analyses subject to strict judicial procedures and prospective studies on the modus operandi of the terrorist threat. Furthermore, its application enables the implementation of a target selection and prioritization process (TSP) through rigorous dynamic assessments, allowing it to conduct intelligence preparation of the combat field (IPB) in alignment with the critical information requirements necessary for commander decision-making.

In this process, it is important to highlight that SF has developed a unique and exclusive analysis tool, vital in the context of the Colombian Military Forces: the Special Operations Planning Tank (TPOE), which acts as a bridge between the art and science of warfare. Specifically, the TPOE is a functional unit composed of personnel with expertise in evaluation and foresight, who form highly trained and versatile teams with the capabilities needed to analyze the various operational environments in which the SF battalions will operate (Ejército Nacional de Colombia, 2017c).

The TPOE proposes potentially viable courses of action for executing an operation using war games and various matrices, enabling science to assess whether the mission variables are adequately considered. For instance, since meteorology plays a crucial role in the insertion and extraction of units during an airstrike, the TPOE investigates patterns and matrices related to atmospheric conditions in this planning cycle and, with the assistance of an expert meteorologist from the Colombian Air Force, identifies the optimal windows or times to carry out the operation. As demonstrated, at this level of military power, joint operations are essential.

It should be noted that the TPOE's strongest capability is defining and preparing the operational environment affecting an operation. Its ability to identify the critical requirements and values in that ecosystem is demonstrated by its expertise in detecting constraints, needs, initial requirements, characteristics, and properties of the terrain, as well as the weather in a geographic area. In other words, the TPOE not only determines "what" but also all the factors that can influence mission execution, which is undoubtedly crucial for developing dynamic and suitable courses of action for SO.

Furthermore, its ability to analyze terrain and its effects on actions is vital for executing operations. Because of this, the TPOE's creative and critical thinking continuously evolves to improve their capacity to conduct the military decision-making process and, therefore, achieve early integration with the target construction premise.

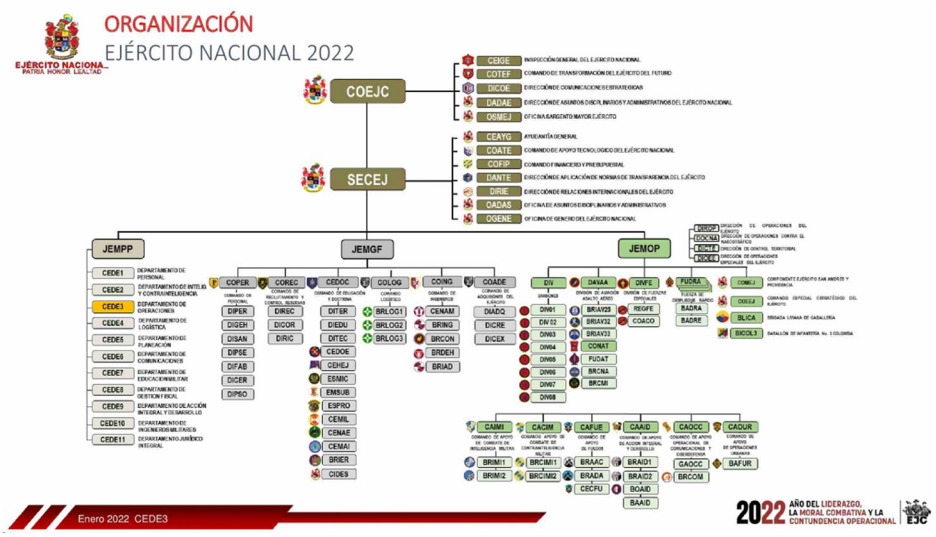
In this context, TPOEs are responsible for carrying out the SF Operations Processes, which consist of a series of steps to analyze and determine courses of action for decision-making. This enables them to accurately assess and mitigate risks in the execution of missions carried out in various operational environments against High-Payoff Targets (HPTs) and their centers of gravity throughout the country.

Based on the work of the TPOE, it can be noted that the DIVFE has extensive experience, as reflected in the planning of more than 200 SF operations, and that its structure enables it to execute joint operations with units that, under the command of the CCOES, are interoperable. This is precisely one of the greatest strengths of the land component, which, within the combat-generating structure, reports to the Army Deployment Command. For their part, units assigned to the CCOES can be used in any operation through command relationships established by the organization. So, if a commander needs, for example, specific waterborne infiltration skills, such as K-DUCK or K-DROP, they can request that the CCOES provide special reconnaissance teams from the Marine Infantry Special Forces Battalion within the planning process, and they will be assigned.

As shown in Figure 2, the DIVFE is subordinate to the Chief of the Operations Staff as a force-generating element, but its combat-generating element and ground component depend on the CCOES. In this respect, the DIVFE is a larger operational unit with a wide range of capabilities that it develops based on the continuous employment of its battalions. These skills in planning, preparation, execution, and ongoing assessment of different operational environments are described in its mission.

Finally, the DIVFE is also composed of SF regiments with airborne capabilities, which are its combat-generating element and a force-generating component. This dynamic and self-sufficient organization allows the commander to keep SF units operationally active without impacting their training and sustainment cycle.

Figure 2. *National Army Organization Chart*



Source: Ejército Nacional de Colombia (2023).

Materials

The acquisition of materials used by the Special Forces Organization is carefully planned by a DIVFE planning department, which conducts a thorough process with the ultimate goal of ensuring that the equipment and improvements are implemented properly and on time. This is outlined in the CCOES structural book for the Odiseo project, where material acquisitions are carried out in an organized and comprehensive manner to guarantee the interoperability of the acquired materials.

The operational capabilities of SO units depend on a strong satellite-based communications system that is compatible with allied countries in the Western Hemisphere. This technology helps synchronize products so they can operate together efficiently, enabling the exchange of information. This innovative CCOES communications system allows it to connect units at the tactical level to command and control at the strategic level, thereby enhancing mission command in the execution of SO. In this scenario, real-time data and voice transmission are crucial for carrying out its key capabilities.

The land component of the CCOES (specifically the DIVFE) has the necessary equipment to carry out SO involving aerial assets. Being part of the CCOES enhances the DIVFE's combat capabilities, enabling it to operate with a strategic fleet in support of the Colombian Air Force. This high level of interdependence

allows it to reach launch bases across the country and access remotely piloted aircraft systems and aircraft with intelligence capabilities, giving it advantages in the electromagnetic spectrum that ensure operational initiative. While these units are equipped with state-of-the-art weapons, the most important aspect is not the hardware but the software, as the saying goes.

Staff, Leadership, and Training

Throughout its history, the National Army has developed a comprehensive doctrine, robust infrastructure, and strong values, contributing to the formation of military leaders with the necessary capabilities to conduct military operations at various levels of warfare, from tactical to strategic. The different types of training offered by the institution are outlined below.

Individual Training

Formal Preparation

It is the one received in the different schools and training centers of the National Army:

1. *"General José María Córdova" Cadet College (ESMIC):* The alma mater of the National Army is responsible for thoroughly training future Army officers as platoon commanders and professionals in military science and other fields. It provides solid foundational skills in institutional principles and values for national development and security. ESMIC teaches officers tactical leadership of units and equips them with the skills needed to manage small units. This training helps develop abilities in planning, preparing, executing, and evaluating operations in hostile environments and difficult conditions, thereby enhancing their technical and tactical skills in commanding and controlling platoon- or detachment-sized units.
2. *"Sargento Inocencio Chincá" Military Academy of Non-Commissioned Officers (EMSUB):* Its mission is to train future non-commissioned officers of the multi-mission Army in Military Training and Management Technology, so that they have the skills to command, instruct, and manage squads at the tactical level.
3. *Arms and Services College (EAS):* The Army Command, through Regulation No. 007 of June 23, 1980, created this educational center to exclusively meet the institution's academic demands and structure the professional training of its command cadres. Thus, this college provides training and

specialization courses for promotion and techniques to officers of the arms and services, as well as technical training to non-commissioned officers. In addition, it establishes tactical and technical doctrine guidelines for arms and services up to the battalion level.

The mission of the EAS is to thoroughly train officers, junior officers, and non-commissioned officers of the Military Forces as commanders of basic units, such as companies, and as members of the general staff through the development, updating, dissemination, and implementation of doctrine at the tactical level to improve military operations and maneuvers that support the security, defense, and growth of the country.

4. *"General Rafael Reyes Prieto" War College (ESDEG):* This is a higher education military institution (HEI) that trains senior officers of the Armed Forces. It works to develop skills and competencies by coordinating, integrating, and executing plans for joint decision-making.

Specialized Instruction

These courses are intended to specialize those who will execute SF operations and include: Lancer, Parachuting, SF, Jumpmaster, Aircraft Scout and Guide, High-Altitude Infiltration, High-Precision Shooter, Air Strike Master, and Security Swimmer.

Furthermore, within the framework of interoperability and as part of cooperation programs with SF, the CCOES has developed advanced skills to execute advanced tactical infiltration operations. Thanks to this partnership, it has been able to train officers at the U.S. Army John F. Kennedy Special Warfare Center and School (USAJFKSWCS) in these courses:

a. *Military Free Fall JumpMaster Course (MFFJMC):* The interoperable doctrine used by SF has enabled them to develop strengths in the advanced training required for this type of SO. This exclusive course, in which organic personnel from the DIVFE participate alongside expert officers in military free fall jumping, specializes in training jump masters to inspect free-fall parachutists, execute emergency procedures, operate supplemental oxygen equipment, plan insertion points and heights based on terrain analysis, give jump commands, manage guidance and capabilities of aircraft used for military free fall jumping (MFFJ), set impact or jump points, pack and inspect gear, perform emergency procedures for night navigation, prepare packing materials, weapons, and configure advanced military guidance systems. During MFFJ training, each student

plans and executes a nighttime operation, which includes jumping armed, equipped, and with supplemental oxygen. Students are subjected to rigorous evaluations at each stage of this training.

b. *Special Forces Qualification Course (SFQC):* The USAJFKSWCS trains captain-ranked officers in this qualification course to integrate SF and, through exchange and knowledge transfer programs, appoints them as organic members within the select group of instructors that comprise the American institution. The course includes six sequential training phases designed to develop and profile the SF operator: 1) unconventional warfare; 2) small unit commander; 3) SF specialists or occupational model; 4) special warfare; 5) foreign languages; and 6) strategic planning and MFFJ training. Officers participating in this program focus on planning and executing courses of action related to distinctive SF operations.

Collective Training

This training combines all the capabilities of SF (direct action, special reconnaissance, and counterterrorism) as outlined in the annual training cycle, the Instruction and Education Plans (I&EP), and the Instruction and Training Plans (I&TP), which are developed based on operational needs. The technical and tactical tasks are performed both individually and collectively at each level, following the specialized organization of the unit conducting SO, as described below.

1. *Commando Training Battalion (BECOM):* As a subordinate unit of the largest operational element of SF, it is responsible for individual and collective training of SF, developing doctrine, and handling all matters related to instruction; it conducts and sustains SF training programs; and offers basic and advanced individual training and education for SF members. BECOM trains, educates, develops, and maintains optimal readiness levels for SF. It is also charged with providing SF regiments with professional officers, non-commissioned officers, and soldiers who are skilled, highly educated, innovative, and adaptable to diverse operational environments.

Infrastructure

As the SF organization grew in size and capabilities, its ecosystem of planning, preparation, readiness, concentration, and revitalization in terms of infrastructure evolved to support agile environments. These environments allow special operators to access the services they need to meet specific objectives.

This modern infrastructure features facilities such as the CCOES smart building, which functions as an integrated hub for capabilities including intelligence and SO, as well as advanced command and control systems. These systems enable SF to maintain the demanding, ever-changing assessments necessary for their missions. At the tactical level, there is an SO complex called Odiseo, located at the National Training Center (CENAE) on the Tolemaida military plateau. It houses two of the three SF military regiments along with other support units. Currently, Odiseo is envisioned as a center of excellence for training regional SO units and is where the elite teams that compete in the regional "Fuerzas Comando" competitions, of which Colombia has been the champion eleven times, receive their training.

This infrastructure enables the SF organization to provide essential services for revitalization, training, rest, and operational readiness, effectively supporting its military actions.

The Beginning of the End: The SF's Target Selection Process and Interoperability

Building a perspective on interoperability must begin by defining the term, which should be observable according to the National Army's doctrine manuals. Regarding its importance in SF manuals, the *Army Fundamental Reference Manual MFRE 3-37 Protection* warns that "fratricide may be more frequent during joint and multinational operations, when communications and interoperability challenges are not fully resolved and clear" (Ejército Nacional, 2017d, pp. 1–18).

However, although the *National Army Manual of Terms and Symbols* defines interoperability as the ability to operate in synergy when units execute tasks or missions assigned by a command (Ejército Nacional, 2017b), for this exercise, the much more specific approach of the *DOD Dictionary of Military and Associated Terms* of the U.S. Department of Defense is proposed:

> interoperability — 1. The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (Office of the Chairman of the Joint Chiefs of Staff, 2021, p. 110)

According to Pablo Moreno (2014), in contemporary warfare, with current command and control structures and new forms of global threat, it is difficult to imagine purely specific land, naval, and air operations employing military capabilities independently, rather than what the interdependent nature of an SF operation demands (Moreno, 2014). As the conflict has demonstrated, operations have been carried out unilaterally. However, the desired effect can be maximized by integrating interdependence and interoperability into the joint nature of planning, which are determining factors in making a strategy efficient and effective for the operational commander.

Similarly, this quality allows it to carry out operations with precision, discretion, and scalability within any major operation or campaign, aligned with its strategic goals and two essential capabilities: surgical strikes and special warfare (Ejército Nacional de Colombia, 2017a). It is important to note that response and execution time are critical when planning courses of action to meet strategic objectives. These qualities have enabled the Colombian SO Forces to excel in surgical strikes against strategic targets. These include the neutralization of Walter Patricio Arizala, aka Guacho, in Nariño Department in December 2018, as well as the operation against Fabián, leader of the Western War Front of the National Liberation Army (ELN) guerrilla group, in September 2021.

The skills acquired through the conduct of typical SF activities against hybrid threats have allowed the development of tactics, techniques, and procedures (TTPs) exclusive to SF that have served and will continue to serve as a benchmark for military strategists within the SF organization due to the boldness and effectiveness of the unique methods they employ.

According to Dr. Tom Searle (2017), special operations are those that are "outside the box" in terms of the conventional nature of military operations. In his Special Operations Theory, Searle (2017) argues that these are neither elite nor specialized; rather, their special quality means they are "different." Although its theory refers to unique capabilities and methods of employment, it is also pertinent to mention the creative thinking that allows for problem-solving from different perspectives, "generating new and useful ideas, reevaluating and combining old ideas to solve problems" (Ejército Nacional de Colombia, 2019). This integration of ends, ways, and means employed by commanders and their staffs is based on the comprehensive application of their skills, knowledge, and experience. Specifically, this cognitive approach is referred to as *operational art* (OPART) according to the *Army Techniques Manual MTE 5-01, Army Design Methodology.*

The evolution of SF in operational art, supported by their creativity, discretion, and judgment in the conduct of their activities, has enabled them to perform effectively in their missions and achieve high-reward objectives with significant efficiency.

Operational art is not directly related to a specific level of warfare, but can occur at both the tactical and strategic levels. Furthermore, it involves four essential elements: time, space, purpose, and the method or manner in which the strategic objective will be partially or totally achieved, so that the appropriate balance will allow the commander to retain, maintain, and exploit the initiative of his tactical action (Ejército Nacional de Colombia, 2019). In this regard, it can be clearly stated that operational art, critical thinking, and thinking outside the box are inherently multidimensional and interdependent arguments that enhance and maximize the planning and execution capabilities of operations of a "different" nature.

The evolution, interoperability, and "outside the box" nature of SF operations have enabled the concentration of strategies that adapt to the existing ambiguous operational environment. This adaptation is possible thanks to the constant and customary application of knowledge (art) to operational dynamics. This particularity has enabled SF to maximize the impact of applying experience to science, and consequently, achieve strategic military objectives that positively influence the overall military strategy (Centro de Doctrina Conjunta [CEDCO], 2018).

In turn, this dynamic allows SF to maintain an efficient level of performance in their training, readiness, and interoperability. To achieve these high standards, SF develops top-quality training plans and programs, which are evident in the success its units have achieved in carrying out operations. For example, we can mention the specific operation "Osiris," which was carried out in October 2021 as part of the "Agamemnon" SO campaign against Darío Antonio Úsuga, aka *Otoniel*, the top leader of the Organized Armed Group Clan del Golfo. As the then-President of Colombia mentioned in a press conference at the Tolemaida Military Fort, this operation is "the hardest blow inflicted on drug trafficking in the 21st century and is only comparable to the fall of Pablo Escobar in the 1990s" (CNN en Español, 2021).

The commanders who have executed these types of missions have understood the concept of *strategy:* the science and art of planning to achieve strategic objectives determined by national interests, with the aim of decisively impacting national threats. Regarding political-strategic objectives, the *General Military Strategy Manual 3-34* establishes that to achieve political objectives, national strategic leadership must be considered through "the use of the fields of power" (CGFM, 1997). This strategic leadership, which establishes goals and allocates

forces and resources, thus provides a broader perspective than the commander's sole knowledge of the doctrine and capabilities of the men under his command. It also encompasses the combination of art and science to contribute to achieving strategic objectives (Ejército Nacional de Colombia, 2016a).

According to Professor Dale Eikmeier (2015), a professor at the U. S. Army Command and General Staff College in Fort Leavenworth, Kansas, some differences can be considered between science and art:

- Art must be considered subjectively, and science objectively.
- Art is nonlinear and advances laterally; science is linear and progresses step by step, interacting vertically.
- Art is studied holistically as a whole; science divides the problem into parts to address it.
- Ultimately, art is the path, "the journey," while science is "the destination."

Hence, these two concepts are combined in different proportions in military strategy, so that success is to determine "when to act like a scientist and when to act like an artist" (Eikmeier, 2015).

As *MTE 5-0.1 Army Design Methodology: Art and Operational Design* (Ejército Nacional de Colombia, 2019) indicates, operational art can be applied at all levels of warfare by commanders and their staffs. It is manifested through plans and orders that describe how (forms) forces should employ their capabilities (means) to achieve the objectives imposed on them, what they call the desired end state, which transcendentally represents the success of the mission (Ejército Nacional de Colombia, 2019).

The following is an overview of the concepts commonly used in SF Operations to execute a mission. Additionally, it explores what operational art describes as *science* and what the *scientist* would express, so to speak; that is, the commander in his planning. Specifically, these concepts would have the following information:

The *mode* of strategy refers, on the one hand, to how the commander of an SF unit, as part of a typical activity within his capabilities, designates an operation and a task, and on the other, to how he will employ the capabilities at his disposal to accomplish a specific strategic objective. The *means* refer to the air, naval, and special infiltration capacities that the commander requests during planning and that are allocated to him after an assessment. The *end* is to use these capacities to achieve the desired end state, which is science.

At this point, it is essential to note that to arrive at this operational concept, an *artist* has had to evaluate multiple courses of action within their military

decision-making process. That is, this commander, together with his staff, has deciphered a strategy to achieve a strategic objective.

According to this approach, such a strategy could be expressed through an equation: Strategy = Ends + Modes + Means (Luttwak, 1989). However, according to specialized literature, additional elements must be taken into account, such as the adversary's environment and strategy, which undoubtedly transcend the outcome of the equation (Álvarez et al., 2018).

Within the Range of Military Operations (RMO), SF has demonstrated its ability to execute actions not only at the joint force level, but also at the interagency, interorganizational, and multinational levels, for a multitude of missions ranging from SF training in host nations to the most significant combat operations at the local level.

As has been shown, SF is a versatile and efficient response at every point of the RMO, enabling them to provide the Colombian State or a host nation with deployable, agile operations that contribute to joint efforts to quickly reverse unstable conditions through ethical and decisive conflict resolution. However, these responses will always be conditioned by uncertain operational environments, as described in the National Army doctrine, which refers to the term VUCA (volatility, uncertainty, complexity, and ambiguity). This strategy, then, is conditioned by changing circumstances in an environment where luck and uncertainty predominate (Álvarez et al., 2018).

Now, in the operational context of SO, one observable factor in the strategists of the SF organization is intuition—not so much luck—which arises from a correct understanding of the operational variables that affect the mission. A proper understanding of the operational environment enables the strategist to devise dynamic approaches to a mission and to consciously and responsibly manage the operation's *tempo.* He knows that his assessment of a clue, an animal, or a footprint can significantly impact the success or failure of an operation.

In general, the National Army employs four primary activities in the operations process: planning, preparation, execution, and evaluation. These constitute a common denominator in the three planning methods that, according to the National Army's military doctrine, the SF organization employs: 1) the Army Design Methodology (ADM), 2) the Military Decision-Making Process (MPMP), and 3) the Command Procedure (CP). Although these scientific methods are applied at different levels, they are aligned and ultimately contribute to the same desired end state.

One of the factors that SF constantly evaluates within its distinctive capabilities is planning methodologies. In this respect, identifying the characteristics of the target acquisition process in SF Operations in a case study goes beyond what science dictates, as it is not linear. To better understand this point, it should be noted that interoperability has been developed to the extent that the institution's organizational culture identifies "the execution" of this process as its added value. This is one of the essential characteristics for achieving the success of its missions.

This planning process occurs at the operational level and is managed by the CCOES and the DIVFE. Although this activity is carried out at a higher level, it must be closely linked to execution at the tactical level to be effectively realized. This interdependence with different levels guarantees the success of the strategic objectives established in the General Military Strategy. Consequently, the CCOES and the DIVFE "construct" strategies to achieve targets based on what is considered a cornerstone: "Early Integration," defined as the result of a three-dimensional effort that combines the analysis of intelligence agencies and the forward-looking vision of planning and operations specialists to maximize the strategy's outcome.

Following this process, the strategies are translated into courses of action that emerge within the TPOE. This statement can be exemplified by the description given by the Commander General of the Military Forces at the press conference following Operation "Osiris," in which aka *Otoniel,* a feared drug trafficker and top leader of the Clan del Golfo, was neutralized:

> This definitive operation against this bandit was planned for October 15, 2021. The Commander-in-Chief of the Military Forces met with National Police Intelligence, Special Operations, and Planning officers, resulting in a conceptual leap in the strategy used by the units to capture this bandit on October 23, 2021. (Noticias Caracol, 2021, para. 2)

This arrangement of capabilities shows the first factors that refer to conceptual planning:

1. Reception of information
2. Exhaustive analysis of that information and operational variables
3. Feasibility of the operation
4. Initiation of conceptual planning and development of operational reports that describe the purpose and means to achieve the desired end state
5. Approval by higher commands; at this stage, the operation can be redesigned according to the guidelines they issue.

6. Delivery of the operational report and initiation of military planning for decision-making. This process includes Early Integration and convenes the commanders of smaller operational units, known in the Colombian case as Special Forces Regiments. While this milestone marks the beginning of a step, the "parallel planning" developed by the units enables them to anticipate events or rehearsals, which must be planned in advance due to the time-constrained conditions under which this planning is carried out

It should also be noted that these steps also encompass several events within the target selection process, which are considered in the conceptual planning: 1) the initial planning that guides the commander's initial guidance, 2) the elements that determine the desired end state, and 3) the lines of effort that will lead to the mission's accomplishment. In this phase, the center of gravity of the operation emerges, constituting the defeat mechanism to be employed and triggering the elements that focus the detailed planning.

These aspects can be seen in the press conference given by the Commander-in-Chief of the Armed Forces on Operation "Jupiter" against *Iván Mordisco,* in which he emphasized that,

> [...] The President of the Republic needs a strategy with lines of action that bring together the capabilities of the Military Forces, including Intelligence, inter-institutional support with the Prosecutor's Office, and specialized training in units with surgical capabilities. (Semana, 2022, para. 3)

On that occasion, the Commander-in-Chief of the Military Forces also described some aspects of the missions that create an operational environment conducive to confronting Organized Armed Groups. Specifically, he noted that this configuration operation was carried out over nearly 24 months, demonstrating the level of participation of SF in the full range of military operations, which is referred to as a "Special Operations Campaign."

During the execution of the Special Forces Operation "Jupiter" against terrorist Iván Mordisco, we report over 288 days of leveraging strategic intelligence; the involvement of more than 700 special operators with strict command and control; the assessment of approximately four areas of general interest; and the execution of 12 operational events. Consequently, the high-precision search and persistence, after covering 1,900 km, enabled the Military Forces to locate him in a specific area of interest for a surgical strike.

This joint, inter-institutional operation demonstrates interoperability and interdependence, the Air Force's analytical and attack capabilities, and the use of ground power through National Police SF and intelligence units. Several operational launch platforms were used, and the key task was maintaining the operation's legitimacy by following the relevant legal procedures.

Continuing with the conceptual analysis, the process of target planning, selection, and prioritization proceeds as follows:

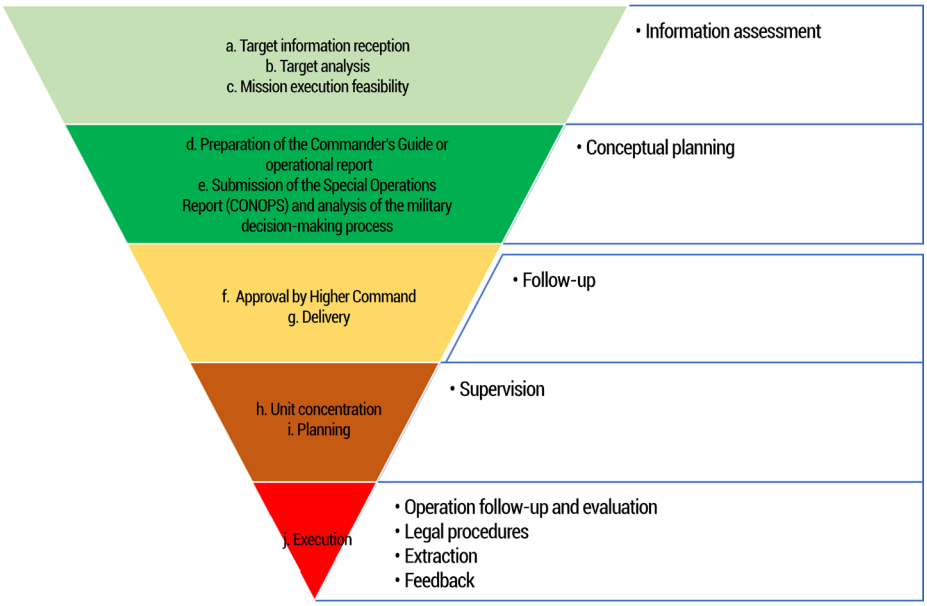
1. Concentration of technical, technological, and air means and SF units in locations that allow for mission accomplishment in terms of time, space, and purpose
2. Planning of maneuver units based on mission variables
3. Battle monitoring. The dynamic assessments conducted at this stage enable reevaluation of the tactics, techniques, and procedures necessary to effectively sustain the operational effort at crucial points in the mission.
4. Legal procedures, vital to ensuring the legitimacy of tactical procedures. This action is carried out in parallel throughout the planning process, is coordinated from the operational level, and directly influences the execution and subsequent evaluation of the mission.
5. Withdrawal of units, either to relocate them or to revitalize them and keep them operationally ready for new missions

Based on the above, Figure 3 summarizes the planning process for selecting and prioritizing the targets of the Colombian SF organization.

So, the effective analysis of this process must have characteristics that transcend the science of doctrine and include "non-tangible" elements (UNIMINUTO, 2012), which are strictly related to four relevant aspects of the definition of targets:

1. The execution of the strategy.
2. The credibility of the organization's leaders, i.e., the commanders, who, beyond strategy, formulate and design a strategic outlook to anticipate actions or turbulences that contingencies could dictate. These strategists must consider categories of information known in the military as *operational variables* and *mission variables,* which help them identify the actors involved and anticipate the risks of an operation.
3. The quality of the proposed strategy. This aspect relates to the distinction the National Army makes between planning methodologies, design methodologies, military decision-making processes, command procedures, and, finally, operational development at the tactical level.

Figure 3. *Special Forces Planning Process*



Note. The inverted pyramid design is based on a statement by Professor Humberto Serna Gómez, an expert in strategic planning. Dr. Serna refers to the top-down design and bottom-up execution of strategies (Corporación Universitaria Minuto de Dios [UNIMINUTO], 2012).

Source: Own elaboration based on the Army Campaign Manual MCE 3-18 Special Forces Operations (Ejército Nacional de Colombia, 2018).

The importance of including these aspects in the analysis lies in the fact that "more than 60 % of an organization [is made up of] those intangible elements, such as the principles of an institution" (UNIMINUTO, 2012).

It should also be noted that two types of advantages can emerge: a comparative advantage, which persists until another organization copies it, and a competitive advantage, which is inherent in the process that grants it a value chain. Specifically, the target selection and prioritization process represents a competitive advantage within the organizational culture of SF, as reflected in their human capital: "culturally cunning, regionally aligned, politically nuanced men, trained in mediation and negotiation, competent in interorganizational coordination, mature, and expected to operate autonomously" (Ejército Nacional de Colombia, 2017a). This is the know-how that characterizes the interoperability process.

Conclusions

In all fairness, this academic work does not intend to emphasize the organizational proposals evident in the contemporary description of the history of SF. While this evolution enabled the creation of a strategic culture that guides the planning methodologies employed by SF, it is essential to highlight that the results are neither ambiguous nor obtained by chance. Instead, they derive from the synergy and interdependence of the capabilities within the system.

Thus, the research describes the target acquisition process in surgical strikes carried out by the Colombian SF. Furthermore, it demonstrates how their scope and successes are not merely the output of a tactical exercise but rather result from a mechanism that combines a capacity that was built geostrategically, as explained when addressing DOTMLPF. In this regard, these elements are not in themselves a factor of success. Rather, they participate in a process that requires innovation and broad understanding, so that these "notes" flow like a symphony that challenges the ambiguity of operational variables and allows the operation's *tempo* to be maintained.

Regarding the question that arose from this research on the SF's target selection processes, it is concluded that they are interoperable, as exemplified in two case studies: the major operation "Agamenón" and the operation against Walter Arizala, aka *Guacho*. These two SO demonstrate a high level of interoperability. The first campaign employed elements of the National Police, conventional forces, and SF, while the second mission involved forces from allied countries (Colombia and Ecuador) to achieve a common objective.

In this respect, the study of the SF's target selection process allows for the following diagnosis. Regarding interoperability, the DOTMLPF capability was built in alignment with regional interests and elements used by allied countries such as the United States. Indeed, the process that other organizations can employ to be successful must take into account elements that transcend the purely material.

The above leads to the conclusion that the characteristics derived from the target selection and prioritization process are "the organization's non-tangibles" and are represented in four important aspects for strategic planning: 1) the execution of the strategy, 2) the credibility of the organization's leaders, 3) the quality of the proposed strategy, and 4) the development of operations. This selection process, as Serna (UNIMINUTO, 2012) mentions, provides a competitive advantage for the SF organization. It is difficult to copy, endures over time, and generates added value, making it a distinctive competence of the Colombian National Army.

References

Álvarez, C., Corredor, C., & Vanegas, O. (2018). Pensamiento y cultura estratégica en seguridad y defensa: Bases para la construcción de una gran estrategia del Estado. In C. Álvarez & A. Fernández (Eds.), *La "Gran Estrategia": Instrumento para una política integral en seguridad y defensa* (pp. 15–63). Sello Editorial ESMIC. https://doi.org/10.21830/9789585692862

Brigada de Fuerzas Especiales. (2015). *Historia y cultura militar del arma de Fuerzas Especiales.* Publicaciones Internas.

Castaño, C., & Arias, J. (2015). Aproximación a la valoración del know-how de una institución del sistema regional de innovación en Antioquia. *Revista Civilizar Ciencias Sociales y Humanas, 15*(28), 151–164. https://tinyurl.com/2kdzkjep

Centro de Doctrina Conjunta [CEDCO]. (2018). *Manual Fundamental Conjunto MFC 1-0 [Público].* Publicaciones Comando General de las Fuerzas Militares de Colombia. https://doi.org/10.25062/MFC10

CNN en Español. (2021, October 23). Iván Duque: captura de alias "Otoniel" es comparable con la de Pablo Escobar [Video]. *YouTube.* https://www.youtube.com/watch?v=9hPiTwhuNWY

Comando Conjunto de Operaciones Especiales [CCOES]. (2014). *Libro Estructural Comité de Revisión Estratégica del Comando Conjunto de Operaciones Especiales CCOES.* Comando General de las Fuerzas Militares de Colombia.

Comando General de las Fuerzas Militares [CGFM]. (1997). *Manual de Estrategia Militar General* (2nd ed.). Publicaciones de las Fuerzas Militares.

Corporación Universitaria Minuto de Dios [UNIMINUTO]. (2012, June 19). Planeación estratégica: doctor Humberto Serna Gómez [Video]. *YouTube.* https://www.youtube.com/watch?v=WqfFwYQaiow

Eikmeier, D. (2015, October 13). Operational art, design and the center of gravity [Video]. *YouTube.* https://www.youtube.com/watch?v=nBStKk3fE4E

Ejército Nacional de Colombia. (2016a). *Manual Fundamental del Ejército MFE 1-01 Doctrina [Public].* Imprenta Militar del Ejército. https://tinyurl.com/h8ywavpv

Ejército Nacional de Colombia. (2016b). *Manual Fundamental del Ejército MFE 3-90 Operaciones Ofensivas y Defensivas [Public].* Imprenta Ejército. https://tinyurl.com/2w7zdbzm

Ejército Nacional de Colombia. (2016c). *Manual Fundamental del Ejército MFE 5-0 Proceso de Operaciones [Public].* Imprenta Militar del Ejército. https://tinyurl.com/2t56cvyx

Ejército Nacional de Colombia. (2017a). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Public].* Imprenta Militar del Ejército. https://tinyurl.com/2p8b7nse

Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 1-02 Términos y Símbolos [Public].* Imprenta Ejército. https://tinyurl.com/3byekp57

Ejército Nacional de Colombia. (2017c). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones. [Public].* Imprenta Ejército. https://tinyurl.com/ducm7tje

Ejército Nacional de Colombia. (2017d). *Manual Fundamental de Referencia del Ejército MFRE 3-37 Protección [Public].* Imprenta Ejército. https://tinyurl.com/4pved58t

Ejército Nacional de Colombia. (2018). *Manual de Campaña del Ejército MCE 3-18 Operaciones de Fuerzas Especiales [Restricted].* Imprenta Ejército.

Ejército Nacional de Colombia. (2019). *Manual de Técnicas del Ejército MTE 5-0.1 Metodología de Diseño del Ejército [Public].* Imprenta Ejército. https://tinyurl.com/3zjfspr2

Ejército Nacional de Colombia. (2023, November 2). *Organigrama.* https://tinyurl.com/bddtmw64

Gallardo, M., & Faundes, C. (2014). ¿Qué es el pensamiento estratégico? *Escenarios Actuales, 19*(3), 7–23. https://tinyurl.com/56jmk66j

Luttwak, E. (1989). *Estrategia: La lógica de guerra y paz.* Instituto de Publicaciones Navales.

Martínez Carazo, P. C. (2006). El método de estudio de caso: Estrategia metodológica de la investigación científica. *Pensamiento & Gestión,* (20), 165–193. https://tinyurl.com/5hd4xftn

Ministerio de Defensa Nacional [MDN]. (2016). *Visión futura de las Fuerzas Armadas.* Imprenta Nacional de Colombia. https://tinyurl.com/bdzfy898

Ministerio de Defensa Nacional [MDN]. (2019). *Política de Defensa y Seguridad PDS: Para la legalidad, el emprendimiento y la equidad.* Ministerio de Defensa Nacional. https://tinyurl.com/5n98jdwf

Montero, L., Garzón, O., Quevedo, O., Tobón, A., & Player, N. (2019). Relevancia estratégica de las Operaciones Especiales: Lecciones de la experiencia colombiana. In L. Montero (Ed.), *El poder terrestre: Ejércitos y guerras del siglo XXI* (pp. 173–199). Escuela Superior de Guerra. https://doi.org/10.25062/9789585698369

Moreno Delgado, P. (2014). *Poder y capacidad: El ocaso de los poderes* [Opinion document, No. 93]. Instituto Español de Estudios Estratégicos. https://tinyurl.com/y2zuy6ct

Muñoz, L., & Cano, D. (2020). Evolución histórica de las Fuerzas Especiales en Colombia. In J. Valdés & A. Rodríguez (Eds.), *Memorias imborrables: Guardias de honor* (pp. 61–90). Planeta. https://doi.org/10.25062/9789584289001

Noticias Caracol. (2021, October 23). Así fue la intensa cacería a alias 'Otoniel', máximo cabecilla del Clan del Golfo [Video]. *YouTube.* https://www.youtube.com/watch?v=UfkEGC1dJIA&t=156s

Office of the Chairman of the Joint Chiefs of Staff. (2021). *DOD Dictionary of Military and Associated Terms [Public].* The Joint Staff. https://tinyurl.com/rdekurva

Rojas, P. (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. http://dx.doi.org/10.21830/19006586.78

Searle, T. (2017). *Outside the box: Special Operations theory* [JSOU Report, No. 174]. The JSOU Press. https://tinyurl.com/mr6hwcy9

Semana. (2022, July 26). *Alias "Iván Mordisco", su estructura armada disidente de las FARC y sus planes criminales.* https://tinyurl.com/3brbchk9

Chapter 3

Prospective Analysis of Special Forces Operations in Megacities: Colombia and Brazil*

DOI: https://doi.org/10.25062/9786287818408.03

Álvaro Iván Torres Cabra
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Guilherme Lopes da Cunha
Escola Superior de Guerra – ESG, Brazil

Abstract: New threats in urban environments stand out as one of the significant challenges for States. Addressing changing threats requires combining different methods and means, especially when urban growth or conurbations can lead to the creation of megacities. Large concentrations of inhabitants create the potential for disputes that can result in internal conflicts. This study presents an empirical analysis comparing the urban centers of Rio de Janeiro and Bogotá, D.C. It employs both qualitative and quantitative methodologies, including an analytical proposal, an explanatory proposal, and a case analysis. The research offers a prospective view of Special Forces, considering aspects such as operational design, the determination of threat centers of gravity, Special Forces doctrine in megacities, and operational and strategic scope in megacity conflicts.

Keywords: urban conflict; strategy; Special Forces; megacity; urbanization.

* 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.

Álvaro Iván Torres Cabra

Lieutenant Colonel in the Colombian National Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Military Resources Management for National Defense, Army Logistics College. Bachelor's in Military Sciences, Escuela Militar "General José María Córdova," Colombia. Bachelor's in Occupational Health and Safety Management, Universidad Militar Nueva Granada, Colombia. Email: **alvaro.torresca@buzonejercito.com.co**

Guilherme Lopes da Cunha

Postdoctoral candidate in International Relations, University of Brasília. PhD and Master's in International Political Economy, Federal University of Rio de Janeiro. Lecturer at Escuela Superior de Guerra "General Rafael Reyes Prieto" **https://orcid.org/0000-0002-8639-747X**
Email: **guilherme.lopes@esg.br**

APA Citation: Torres Cabra, A. I., & Lopes da Cunha, G.(2025). Prospective Analysis of Special Forces Operations in Megacities: Colombia and Brazil. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 61-86). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.03

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

Urban warfare is not a new phenomenon. Cities have been a setting for violence since humans began building them. Wealth disparities have led to the formation of urban criminal ecosystems (a term that is convenient for examining the correlation between outlaw groups and the geographic environment).

The above allows us to observe the urban criminal ecosystem and determine the setting in which outlaw groups, the civilian population, and other interdependent actors interact. Criminal ecosystems are usually located in slums or red light districts. The stories of Aleppo, Mosul, Marawi, Mogadishu, Donetsk, and Mekelle serve as examples, confirming that both towns and cities will be future strategic military targets.

The unplanned and disorganized population growth of urban areas in the world's major cities is advancing rapidly. Some studies provide alarming data projected for 2050, indicating which urban centers will face the most complex security and defense challenges (United Nations Educational, Scientific, and Cultural Organization [UNESCO], 2017).

If we add to this the pursuit of improved quality of life, the strategic value of cities is reinforced, and it becomes evident that they are becoming vital hubs for nations. Consequently, the unique physical terrain and a large population considerably increase the complexity of collateral risks when conducting operations in urban environments.

Megacities are a difficult scenario to predict, as they require the conduct of joint, coordinated, inter-institutional, and multilateral (JCIM) operations to counter transnational organized crime (TOC). It should be noted that this is the fundamental basis of the doctrine adopted by the Commander-in-Chief of the National Army

to address current challenges (Escuela Superior de Guerra [ESDEG], 2021). Thus, the scenario is a volatile, uncertain, complex, and ambiguous (VUCA) operational environment, which characterizes the nature of some difficult conditions and situations (Wigmore, 2017).

Another advantage of the threat is the use of information technologies, which enhance behavioral stereotypes. This has added an additional layer of difficulty to traditional conflict spaces and, as a result, changed their usual dynamics. Global access to the virtual environment has created countless opportunities to foster online conflicts that affect online domains (computer systems), cognitive domains (people's attitudes, knowledge, and beliefs), and physical domains. Consequently, this means that war would no longer be limited to armed adversaries but would expand to encompass all aspects of the human experience (Álvarez et al., 2018).

Accordingly, this research document makes a prospective analysis of the Special Forces (SF) Operations in Bogotá, D. C., and Rio de Janeiro, two Latin American cities that are not alien to the evolution of deviant globalization[1] and which reflect their "dark side": the proliferation of illicit trade (enabled by the same technological means) and the prosperity of licit globalization (which has increased global mobility) (Zambrano & Álvarez, 2017).

Additionally, studying the challenges faced by the SF of Latin American States in this scenario allows us to propose the relational hypothesis that the emergence of megacities implies a greater potential for conflict. Consequently, this necessitates enhancing state security apparatuses to protect individuals and institutions. In this regard, the following questions are posed: What are the implications for SF Operations in megacities as a conflict scenario? How does a comparison of other experiences (such as those occurring between Rio de Janeiro and Bogotá, D.C.) contribute to investigating the phenomenon of urban conflict in future South American megacities?

This chapter is composed of three main topics. The first is the investigation into the nature of urban conflicts and the scenario of demographic intensification, aspects that encourage reflection on the challenges of containing multidimensional threats. The second is the search for political and strategic responses related to the tactical and operational adaptation capacity of SF to address the situation identified in the first part. The third is a proposed case study comparing Rio de Janeiro and Bogotá, D.C. The research results reveal differences and similarities between Brazil

[1] That is, one in which individuals commit all kinds of crimes by taking advantage of the benefits of technology.

and Colombia, highlighting the need to continually modernize the mechanisms that ensure the neutralization and suppression of threats in an urban environment.

The Formation of Megacities and Conflict Scenarios

Urbanization is undergoing a continuous expansion that relies on connectivity to integrate transportation, energy, and communication. These factors enable it to make a quantitative leap in the mobility of people, goods, resources, and knowledge, shaping the global network civilization of the 21st century. As part of planetary urbanization, by 2030, more than two-thirds of the world's population will live in cities, and there will also be fifty clusters of megacities (including Rio de Janeiro and Bogotá, D.C.) in an environment where cities seek to be part of the global value chain (Khanna, 2016a).

In "Architecture, Globalization and Identity," King (2008) explains the important and observable trends that foreshadow the future of war. For example, he points out that cities have always been meeting points where goods and services are exchanged and that their inhabitants receive protection in exchange for subordination to a political power. Furthermore, he adds that there are several factors fueling the dynamism of the urban transition: on the one hand, people feel pressure to migrate from the countryside to escape poverty and threats to their security; on the other, they do so because they are attracted to a city that promises a more complete way of life, interconnected with globalization.

In addition, statistical evidence points to a challenging future for the urban environment. Population expansion in cities and the changes resulting from this reconstruction of space create a context of uncertainty, which underscores the need to establish effective plans to manage security mechanisms. According to UNESCO (2017), urban centers will undergo a challenging transformation:

> For the first time in history, more people live in urban areas than rural areas, a proportion that is expected to increase by 2050. With cities growing vertically and populations becoming denser, urban centers will become increasingly congested, complex, and interdependent (p. 22).

The UNESCO (2017) report highlights a reality that will significantly impact the security of the international system. Aware of these conditions, members of

the United Nations (UN) propose lines of action that detail the analyses conducted by its Department of Economic and Social Affairs.

Thus, it is evident that the conflict scenario has shifted to the urban environment, which comprises a wide range of social structures within a given space. To help contextualize the research objective, it should be noted that the terms *city* and *urban* are often used synonymously, but they can denote different concepts:

> City refers to the statistical grouping of people in a single area, while urban refers to the transformation of mentality that occurs in cities. In other words, the concept of urban generally denotes altered patterns of social, economic, political, and cultural interaction. (Comisión Económica para América Latina y el Caribe [CEPAL], 1989, p. 72)

As will be seen later, these characteristics make it necessary to study a variety of variables to generate doctrine.

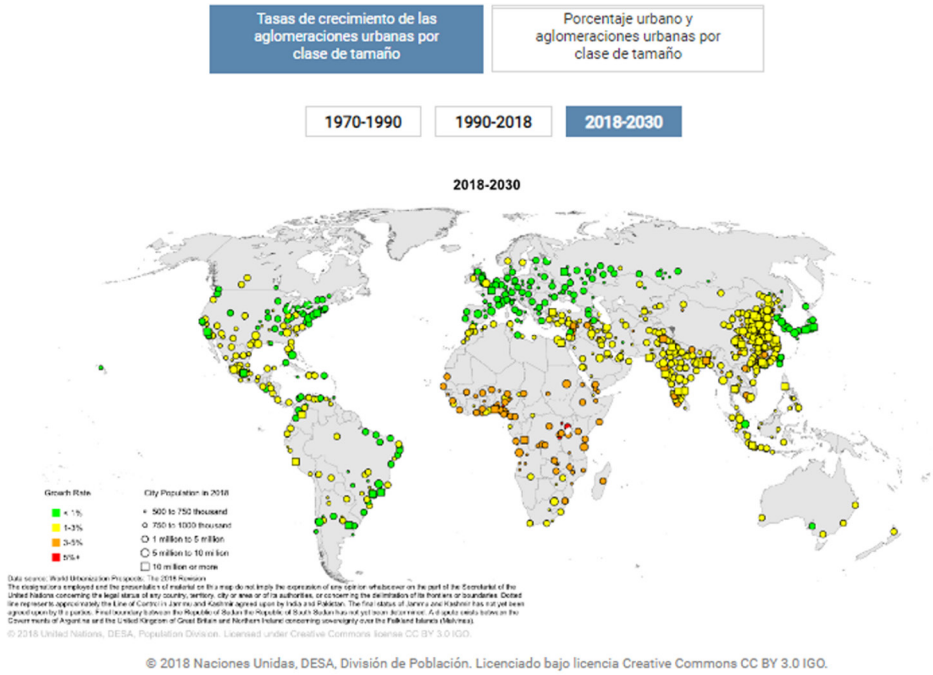
However, the growth of cities represents a challenge for public management in the present and the future. Some characteristics stand out in reflections about cities, such as demographic expansion, the disorder in the logic of expansion, and conurbation, among other elements. In this process, the international community presents policy options, such as the proposal for the New Urban Agenda (Urban Agenda Platform, 2022), which was adopted by the UN at the United Nations Conference on Housing and Sustainable Urban Development (Habitat III) in Quito, Ecuador, on October 20, 2016.

In this context, members of the organization and other stakeholders have mobilized to implement urban development at the local level. In fact, through Resolution No. 70/1 of the United Nations General Assembly (September 25, 2015), 17 Sustainable Development Goals (SDGs) were established, one of which, SDG 11, aims to ensure the creation of inclusive, safe, resilient, and sustainable cities (UN, 2015).

However, data provided by various international bodies raises concerns from a multilateral perspective. For example, the UN Department of Economic and Social Affairs published a study on the growth of urban agglomeration indices (UN, 2018), which forecasts alarming urban growth rates for the coming years (Figure 1).

Forecasts point to an increase in urban growth rates in the coming years (Figure 2). The statistics show significant data for South America, but less alarming than for other regions of the world, a fact that Milton Santos (2004) describes as "urban macrocephaly." However, the prospects for urban agglomeration constitute a scenario of uncertainty in cities with high population concentrationsa.

Figure 1. *Urban Agglomeration Growth Rate (2018–2030).*



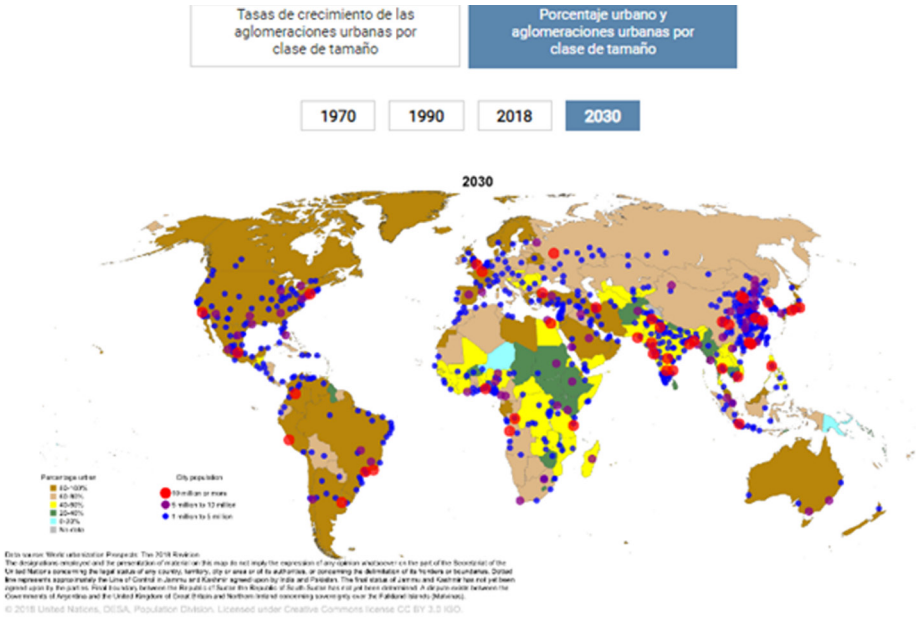
Source: UN (2018).

According to the United Nations (2018d), a megacity is defined as a city with more than ten million inhabitants. There are currently 24 megacities, and it is estimated that at least 27 cities will be classified as such by 2025. Furthermore, it is projected that 752 million people will live in megacities by 2030, i.e., 8.8 % of the world's population.

Based on the above, it can be stated that megacities and metropolitan areas are a key element of geopolitical reconfiguration on a global scale. According to Iberdrola (2020), the largest megacity today is Tokyo, Japan, with a population of more than 32 million inhabitants in an area too small to accommodate them.

Another characteristic of megacities, especially those in the developing world, is their association with high poverty rates, social disintegration, poor infrastructure maintenance, deficiencies in basic services, very high birth rates, limited job opportunities, and disease transmission, among others.

Figure 2. *Urban Percentage and Urban Agglomerations for 2030*



Source: UN (2018)

Regarding modern States, there is concern about the situation in large cities, which reveals an increase in various forms of crime. The growth of urban areas and various illicit activities allows criminal groups to entrench themselves in less fortunate sectors, posing a challenge to national security and defense (NSD). The concept of the "gray rhinoceros" (Izquierdo, 2018; Wucker, 2016) indicates that the problem is visible from afar, but the necessary measures are not being taken to contain the future threat.

Urban Conflicts between and/or within States

In the 21st century, humanity's priority is to achieve sustainable urbanization, which requires technology, knowledge, and public policies. However, inequality in various aspects creates friction among the population and often triggers conflicts.

Despite being an ancient phenomenon, the nature of conflicts needs to be differentiated. On the one hand, there is the type of combat caused by a conflict

between States, whose war can occur in an urban area; on the other, there is urban conflict, in which a State must enter into conflict against its own citizens, which is conceptualized as "non-war" (Alves, 2018).

Although conflicts between States must be the subject of constant analysis, the main focus of the research proposed in this document is to verify intrastate conflicts (one of the great challenges facing Latin America). However, it is considered important first to evaluate the unique characteristics of the Armed Forces' actions in the urban environment.

Military operations involve multiple types of risks, such as tactical risks (including the possibility of soldiers being injured or killed, or mission failure) and accidental risks (including the possibility of civilian deaths or the destruction of critical urban infrastructure). These factors must be considered during planning to study their potential implications and instruct units on legal frameworks.

In this respect, a forward-looking view of operations carried out by SF must take into account not only that urbanization is a relentless trend, but also that as cities grow and expand, armed conflicts and violence become urbanized as well (Lehmann, 2015). This has been evident in cities such as Aleppo in Syria, Sana'a in Yemen, and Mosul in northern Iraq, which have suffered siege warfare, aerial and artillery bombardments, as well as heavy street fighting (Espinosa, 2017).

Based on a detailed analysis of recent urban battles and their historical background, King (2008) argues that exploration of the changing topography and evolving tactics of the urban conflict landscape demonstrates that operations in today's cities have become distinctive. This does not mean that all the methods used in urban warfare are new, but rather that urban warfare has transformed into grueling microsieges waged by combatants fighting through individual buildings, streets, and districts.

Implications for Special Forces Operations

The uncertainty and complexities of the urban environment demonstrate the present and future challenges facing the Armed Forces. In light of this, we propose to investigate the three main lines of modernization of SF: 1) the new requirements regarding operational design and the determination of centers of gravity; 2) the doctrine of SF in megacities; and 3) the operational and strategic scope of SF in conflicts in megacities. These elements reveal common challenges that can be verified.

New Requirements for Operational Design and the Determination of Centers of Gravity

Urban centers present challenges of greater scale and complexity because they contain strategic territories interconnected with local, national, and, in some cases, international centers of gravity. Although it has been addressed for several decades, the concept of "center of gravity" is fundamental in current conflicts, and its use must be assessed in different social and historical contexts (Cazumba, 2021).

Those responsible for planning urban operations need tools that help them make sense of a complex confrontation environment and develop an acceptable level of situational awareness, which is essential to separate the relevant from the irrelevant, the central from the peripheral. The importance of the center of gravity in military planning is reflected in four criteria: improving understanding, emphasizing planning, enhancing efficiency, and eliminating distraction.

The urban environment has unique qualities. It consists of disorganized three-dimensional spaces that create significant logistical and navigational challenges. Its man-made terrain features angular shapes that rarely appear in non-urban areas: a flat planimetric pattern and a third dimension, where verticality is crucial because it forms barriers that are difficult to breach and offers defense through another artificial height, such as tall urban ground levels, and often includes a subterranean layer.

However, in the particular case of Latin America, urban violence, fueled by the TOC, stands out. Part of its formation consists of alliances with different armed groups, which not only leads to criminal convergence between insurgents and criminal groups but also generates a network that shares the same interests and expands to different countries.

Some examples worth mentioning are Mexico and Brazil, which have some of the highest homicide rates in the world (Morán, 2021). It should also be mentioned that in Colombia, multiple cities, ranging from medium to large, serve as epicenters of urban conflicts caused by the TOC to maintain dominance and supremacy in the micro-trafficking business. This crime eventually connects with others and has gradually displaced the drug cartels of the 1980s and 1990s, whose modus operandi was very different.

In this context, the critical importance of urban operations requires a well-structured force with top capabilities and skills to face the threat. Two notable events in Colombia are worth recalling: the first is the siege of the Dominican Republic embassy in Bogotá, D.C., in 1979. At that time, there was no trained or

experienced unit capable of rescuing the hostages, which prevented a military rescue and resulted in Cuba mediating. The second is the guerrilla siege of the Palace of Justice in 1985 by the self-proclaimed Movimiento 19 de Abril (M-19), also in Bogotá, D.C. This incident had devastating consequences for Colombian society, from which it has not yet recovered.

Actions like these occurring in urban areas made it necessary to have trained, equipped, and certified military forces to prevent, detain, or respond effectively. As a result, through Ministerial Resolution No. 2270 of April 30, 1986, the Urban Anti-Terrorist Special Forces Group (AFEAU) was established with the specific purpose of having a unit capable of handling crisis and hostage situations in urban environments when the nation's interests are seriously threatened (Valdés & Rodríguez, 2020). To date, this unit has been trained, qualified, and certified in techniques, tactics, and procedures for managing urban crisis situations, with specific missions.

It is important to mention that, within the Table of Organization and Equipment (TOE) of the Military Forces, the AFEAU is part of the Joint Special Operations Command (CCOES) (Comando General de las Fuerzas Militares [CGFM], 2016), a unit that represents a strategic trident based on the combination of capabilities, training, and interoperability to combat a completely amorphous and irregular adversary.

For its part, the Ministry of National Defense (MDN) has adopted the idea of urban combat as a pressing need to confront terrorism by Organized Armed Groups (OAGs), which have threatened the national security and defense of Colombian territory.

The Doctrine of SF in Megacities: Case Study and Lessons Learned

Throughout history, military theorists have acknowledged that defense is the most powerful tactical stance. In fact, it requires more force to attack and overcome an enemy in a fortified and well-designed defense than in an open area. This is especially true in urban terrain, where many physical structures provide immediate, military-grade defensive positions for the defender.

Typically, most citizens adopt a position in the midst of conflict, based on their ability to act, limit, block, or displace ongoing urban operations. For example, John Spencer (2022), who focuses on urban warfare studies at the Modern War Institute (West Point), published a series of messages on Twitter (now X) on February 26, 2022, addressing civilian resistance fighters in Ukraine, particularly in the country's capital, Kyiv, with a population of approximately three million. This

professor believes that if the capital's adults mobilize and make Russian forces fear that a gun could be pointed out of every window and that every street could be a death trap, they could turn Kyiv or other cities into "enormous porcupines" that can successfully confront any soldier, no matter how advanced (Spencer, 2022).

Regarding this example, it should also be noted that physical dominance is a prevailing concept in the Russian-Ukrainian conflict because either side can use it. Basically, the ruins of old buildings and downtown or commercial areas can be used by committed forces, which will undoubtedly guarantee them adequate protection, since urban terrain provides a significant advantage to the defending force, even the weakest. Therefore, assessing the difficulty of warfare in a specific environment requires considering the scenario itself as one of the military capabilities available to accomplish the mission.

Another conflict that served as a benchmark for the use of Urban Special Forces took place in Mosul, a city in northern Iraq's Nineveh Province. Its seventy square miles are crossed by the Tigris River, which flows through the city from northwest to southeast (Arnold & Fiore, 2019). This battle began on October 16, 2016, and ended on July 20, 2017, after Iraqi soldiers had cleared the last pocket of the defending Islamic State forces.

This example undoubtedly represents a unique urban conflict, as despite the Iraqi forces having the essential technology and equipment, it was very difficult for them to recapture the city because they encountered aggressive jihadist resistance using snipers, bombs, and vehicles loaded with explosives. Some sites in western Mosul had narrow streets that impeded the passage of armored vehicles and forced infantry troops to retreat and remain unprotected. Another challenge faced by regular forces was the number of tunnels, which delayed or impeded their advance.

These experiences also show that the challenge in future urban conflicts will be to mount a successful psychological operations campaign, with providing information being essential to persuading civilians to leave the city. In Mosul, for example, the attempt to disseminate messages to the population via cell phones, the internet, and leaflets, to eliminate them safely and quickly, and then to provide shelter, food, and medical support to prevent further casualties from the violence on both sides, could only be considered partially successful. In fact, "Mosul demonstrated that this may be impossible" (Amnesty International, 2017).

As can be seen, the war is fought in urban areas, and people today are accustomed to monitoring these scenarios through various technological means to stay informed. Cities, in particular, are centers of power that concentrate the

economic, political, and social control of any modern civilization; hence, Russia's need to take over Ukraine's main cities in this war—a situation it has struggled to achieve. Additionally, urban areas concentrate resources and elements that can be used to hold the civilian population hostage, which calls into question the right to war and the intervention strategies adopted by humanitarian organizations.

In their book, *Tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder cíber en el siglo XXI,* González-Martínez and Montero-Moncada (2020) refer to the applicability and readiness of Urban Special Forces to face Colombia's future challenges. Furthermore, they establish that the country's Military Forces must devise a doctrine to prepare strategies for combating the new threats that have emerged due to diverted globalization.

Events such as the siege of the Dominican Republic embassy in Bogotá, D.C. (February 28, 1979), the attacks on the Twin Towers in New York (September 11, 2001), and the invasion of Iraq (2003) created the need to adjust the mission of the Military Forces and, in particular, of their SF. In the Colombian case, according to data from the National Commission of Historical Memory, between 1965 and 2013, all armed insurgent actors in the internal conflict frequently used the strategy of taking over towns and municipal capitals, which drew regional, national, and global attention.

Currently, Colombia is facing multiple challenges. For example, the so-called "front line" has become a challenge in the urbanization of the conflict, given that it uses peaceful protest as a perfect shield to carry out its actions. In this regard, it is important to recognize that these protests have resulted from both the serious economic and social imbalances the country has endured for decades, as well as the impact of new technologies and media, from the internet to social media.

This type of threat to the nation's interests and security is what Guattari (2017) calls a "dissipated molecular revolution." This mode uses the ideas expressed by Antonio Gramsci as historical sources, emphasizing the need to carry out the revolution from the "superstructures" by combining nonviolent and violent means. The theoretical foundation is the assumption that the "molecular revolution" is a universal system of social struggle and emancipation (Guattari, 2017).

Based on this phenomenon, Security Forces, specifically the National Army, outline in their new doctrine (called Damasco) the capabilities to support urban operations (Ejército Nacional de Colombia, 2017a). These are established as part of the Army's operational concept (Unified Land Operations [ULO]) and are conducted in Unified Action (UA) as part of decisive action. Specifically, they carry out Defense Support of Civil Authorities (DSCA) tasks, which have seven main

purposes: saving lives, restoring essential services, maintaining or restoring law and order, protecting infrastructure and property (public and private), supporting the maintenance or restoration of local government, shaping the operational environment for interagency success, and supporting the social recovery of the territory (Ejército Nacional de Colombia, 2017a).

Operational and Strategic Scope of Special Forces in Megacity Conflicts

Uncontrolled urbanization could contribute to the growth of insurgency, terrorism, and other forms of violence when the demands of cities exceed institutional capacities. Local governments are often overwhelmed by the proliferation of informal and/or criminal practices that foster territorialization by criminal groups. Consequently, it is essential that the Armed Forces and the Police, depending on the country and context, have units trained to act as a unit or disaggregated into combat teams—made up of four men with specific individual specialties—that enhance interdependence and freedom of action during an assault.

As mentioned, the Colombian Armed Forces have the AFEAU, whose main mission is

> to conduct special counterterrorism military operations and other Special Forces missions in urban and semi-urban areas, designated by the high command, against military targets of high strategic value (OMAVE) and military targets of national interest (OMINA) that contribute to the fulfillment of the objectives of the Higher Command. ((Ejército Nacional de Colombia, 2021, p. 32)

Due to its high level of training and specialized equipment, an SF unit is not limited exclusively to conducting counterterrorism operations. Depending on the analysis of the operational environment, it can employ one or more of its distinctive capabilities, such as hostage rescue and personnel recovery, assistance to security forces, internal defense abroad, non-combatant evacuation, direct action, and special reconnaissance. In this regard, it is important to mention this unit's outstanding participation in the military competition known as "Fuerzas Comando." This competition began in 2004, when the United States Southern Command, under the responsibility of Special Operations Command South (SOCSOUTH), created and sponsored competitions to measure the capabilities of each team,

strengthen relationships among members of the continent's Armed Forces, and share knowledge and experiences acquired in the fight against terrorism.

Furthermore, the Joint Special Operations University addresses a series of vital topics for Urban SF Operations, such as adversary approaches in political warfare, strategic blind spots in modern conflict, and human rights as a weapons system (Joint Special Operations University, 2021). The latter is based on the UN Universal Declaration of Human Rights.

Finally, it is important to highlight that the International Committee of the Red Cross (ICRC, 2021), in order to minimize the impact of urban warfare, wrote a manual that serves as a guide to the main applicable frameworks of International Humanitarian Law in urban operational environments, aimed at commanders at all levels.

Case Study: Brazil and Colombia

Prospective analyses of intrastate-motivated urban conflict reveal the challenges that SF will face in the future. The tactical and operational implications for addressing threats indicate substantial changes in security management. In this context, to illustrate the proposed theoretical approaches, a comparative case study between Brazil and Colombia is presented to identify convergences and divergences in how to "operationalize" effective redesigns to combat this problem.

Brazil

Latin America stands out for having achieved the fastest urbanization in the 20th century. Brazil is the largest country in South America and one of the most populated, with a density of 22.5 inhabitants per square kilometer and a population that has tripled since 1950. It has a vast area and includes vast virgin forests and uninhabited regions. Nearly 86 % of the population lives in cities, of which about a third reside in the country's ten largest metropolitan regions alone (Datosmundial, 2022).

Although this case study focuses on Rio de Janeiro, it should be noted that the other largest cities in Brazil are São Paulo, Brasília, Salvador, and Fortaleza. In addition to its tourist attractions, Rio de Janeiro is known for its high rates of violence and crime and, along with São Paulo, stands out as a center of tension in Brazil. According to Lawrence (2019), "megacities are becoming epicenters

of human activity across the planet and, consequently, will cause the majority of frictions requiring military intervention" (p. 529).

The violence in São Paulo is more related to the 1,300 attacks committed by various groups linked to the drug trafficking gang Primeiro Comando da Capital, as well as riots in 73 prisons in the city (Harris et al., 2014, p. 18). The violence in Rio de Janeiro, on the other hand, is related to the use of more than 3,000 police and military officers to put an end to acts of violence that were spreading throughout almost the entire city after having begun in one of the 600 communities (Langewiesche, 2008).

In the contemporary context, economic globalization has given rise to a new world order. Queiroz et al. (2022) detail their impact on highly underdeveloped States, where politically motivated actors emerge unconnected to national States, seeking to impose their position through force due to a lack of state representation.

These "new threats"—insurrections, organized crime, drug trafficking, piracy, and terrorism—remove the State's monopoly on war, as they present a challenge to military institutions as a whole. For example, in some cases, the "asymmetric warfare" modality they propose ignores the International Humanitarian LAW (IHL) and the Law of Armed Conflict (LOAC), which is governed by the terms of the Geneva Convention.

Certain elements of association between criminals and pseudo-religious groups are also part of an emerging phenomenon in urban conflicts in Rio de Janeiro. In fact, criminals have found common ground with the growth of the evangelical movement, which has unleashed "narco-Pentecostalism," which treats believers of African origin as enemies in a kind of tropical jihad—movements like Bonde de Jesus, and criminal territorializations like Complexo de Israel.

At this point, it is important to note that the process of forming a unit of men capable of conducting unconventional military actions (Special Operations) requires a combination of factors that depend fundamentally on national security policies, the initiative and military force in question (Navy, Army, or Air Force), the financial contribution allocated for this purpose, the availability of time (operational training), existing resources (men, equipment, and weapons), technological adaptation and modernization to employ the acquired skills, and combat experience (Denécé, 2009; Lisboa, 2017).

Colombia

Located at the crossroads of Central and South America, Colombia serves as a conduit for legal and illegal global trade. For Zambrano and Álvarez (2017), this characteristic makes it a gateway State or region, as it plays an extremely important geostrategic role by uniting different parts of the world, facilitating the exchange of people, goods, and ideas, and fulfilling various positive economic and social functions. However, in some cases, due to diverted globalization, these functions can become more problematic (Zambrano & Álvarez, 2017, p. 290).

Regarding the dynamics of demographic expansion, Colombia faces the forced migratory flow of people from neighboring countries, along with its associated social, economic, political, and national security implications. This country has five major cities: Medellín, Cali, Cartagena, Barranquilla, and Bogotá, D.C., the capital of Colombia, located in the center of the country. It wields great geopolitical power (Instituto Geográfico Agustín Codazzi, 2022) and has a triple constitutional status: capital of the Republic, capital of the department of Cundinamarca, and Capital District with a special regime. Furthermore, according to Parag Khanna (2016b), it is projected to become a megacity in the coming years.

Regarding security, it has a long history marked by various events over the past thirty years. The rise of different criminal groups—sponsored by organizations with global networks and financed through drug trafficking—has facilitated terrorist acts, causing significant social panic. This issue is not new, but it leaves deep and lasting effects on the minds and hearts of the population.

This increases the potential for unrest, disruption, and large-scale disorder. In this regard, Kilcullen (2013) predicts a world centered on megatrends and highlights the following factors: urbanization, coastalization, conflict, and rapid population growth. For this reason, security forces face multiple challenges in providing adequate protection to strategic assets and the population. Current threats have access to new technologies and use this valuable support tool to hide, coordinate their criminal activities, and carry out armed actions with irregular and sabotage means in urban environments, which differ from rural ones.

In this regard, Rojas (2017) points out the need for the Colombian National Army to focus on overcoming the challenges it currently faces and anticipating those of the future. This reality requires it, within the context of its strategic management systems, to continually consider modernization and adaptation processes to

develop capabilities that provide timely, effective, and sustainable responses to the strategic requirements arising from the study of the battlefield.

Urban Conflict in Rio de Janeiro and Bogotá, D.C.

Rio de Janeiro and Bogotá, D.C., symbolize cities challenged by violence and crime, reflecting conflicts in the urban environment. Nevertheless, they preserve their unique characteristics, representing natural and intangible human diversity and overlapping trends. These features help us understand their status as megacities (Khanna, 2016b) and the urban conflicts that afflict them (Fidalgo et al., 2010; Mendonça, 2018). In structural terms, the post-Cold War era shows increased intrastate conflicts involving non-state actors, offering concrete data that emphasize the complexities of criminal behavior in the 2.0 world order, as outlined by Queiroz et al. (2022).

In the comparative exercise between Rio de Janeiro and Bogotá, D.C., each city represents a culture and offers divergent imagery, highlighting positive aspects (such as tourism) and negative ones (like the feeling of insecurity).

The climate of insecurity involves different criminal organizations and militias. Since the end of the 20th century, conflicts around the world have mutated and acquired a more intrastate than interstate nature due to the emergence of violent non-state armed actors. In this regard, Muggah (2017) argues that this new type of conflict arises from the convergence of organized crime and open warfare, which has challenged the traditional rules of urban confrontation.

The emergence of urban conflicts demands the constant evolution of capabilities, weapons, and command, control, and communications doctrine. This, in turn, has an undeniable influence on the daily lives of millions of citizens living in the slums of Rio de Janeiro and São Paulo, where state control is limited or nonexistent.

Criminal groups such as Comando Vermelho and Terceiro Comando Puro (Bartolomé, 2019) have thrived in Brazil due to limitations in policing and ineffective security management. In this scenario, urban criminals have taken advantage of the State's inability to address socioeconomic disparities. Arms and drug traffickers, militias, gangs, and even pseudo-religious groups destabilize state mechanisms and terrorize community residents, holding them hostage while maintaining control over the government and its institutional apparatus.

However, in these scenarios, the Brazilian president can decree operations to ensure law and order (GLO), in accordance with Complementary Laws 97/1999

and 117/2004 (Presidência da República do Brasil, 1999, 2004), according to which the Armed Forces can be called upon to assist in taking control. Precisely, one notable difference with Colombia is the expansive role that the Brazilian Armed Forces can assume.

Regarding the city of Bogotá, D.C., the analysis reveals unique parameters. Considering the background information, the current dynamics of its conflict are more complex and involve multiple combinations of actors, unlike the historical events that marked the violence of the 20th century. Without a doubt, the turning point of the Colombian conflict was the assassination of presidential candidate Jorge Eliécer Gaitán, which occurred in the capital on April 9, 1948, sparking a series of riots and demonstrations by the people known as "El Bogotazo."

Until the 1980s, the violence in Bogotá was due to the armed conflict; there were no actions by drug trafficking or organized crime. However, it is also essential to consider the aforementioned events regarding the sieges of the Dominican Republic embassy and the Palace of Justice by the M-19.

Some of the methods used by conflict actors since the 1980s have become a hallmark of Bogotá, D.C., to maintain, impose, or contest their territorial control: homicide, human trafficking, extortion, micro-trafficking, etc. A significant portion of the phenomena experienced in recent years is due to the lucrative micro-trafficking business, the dispute over control of localities, and the presence of several criminal groups coordinated by external leaders. One of the most dangerous areas in Bogotá is the so-called "Bronx," as it is home to several crimes and a high rate of unmet basic needs (UBN) (Avendaño et al., 2019; Escobar, 2020).

As an epicenter city, it receives a large number of displaced people fleeing the country's internal conflict. This increases crime rates, unleashes a wave of violence and struggles for control of micro-trafficking, and causes collateral damage to development and civic coexistence.

As can be seen, both Rio de Janeiro and Bogotá, D.C., have been hotbeds of criminal gangs that have taken over certain areas in the face of the challenges of an ineffective State. They have created an environment of fear in the community, allowing them to maintain absolute control over what happens in their territories. These gangs generally use micro-trafficking to expand their businesses and obtain resources to finance long-established mafias, creating internal wars between mini-cartels and leading to an escalation of the conflict.

Thus, it is found that crime is more concentrated in densely populated areas, interrelated with conflict and sustained by weak governments and political

instability. This allows for empirical verification of the direct relational hypothesis that the greater the degree of state fragility, the greater the likelihood of conflict-related actions anchored in the use of violence and force to provoke a state of terror in pursuit of the political and/or ideological objectives of criminal groups (Queiroz et al., 2022).

Conclusions

This research aimed to analyze the challenges facing SF in future megacities. These challenges were empirically verified by comparison in the cities of Rio de Janeiro and Bogotá, D.C. Furthermore, a prospective analysis was proposed regarding the constant evolution of conflicts in megacities as a conflict scenario and the use of security forces through SF units.

Conflict studies infrequently consider cities as a backdrop for confrontation, and it is often unclear whether they are directly or indirectly impacted by hostilities. Indeed, throughout human history, cities have been destroyed using specific techniques of urban conflict, such as sieges in Antiquity or the Middle Ages.

Regarding the security and defense of States, September 11, 2001, marked a benchmark for the capabilities and scope of threats when two planes crashed and destroyed symbols of the United States' economic and military power. This fact demonstrates the vulnerability of cities as targets for different types of terrorist attacks.

The phenomenon of threats in urban areas, examined from different perspectives, is unified in a common concept of criminality: convergence (Luis Alexander Montero Moncada, interview conducted by M. A. Cabra in 2022). Several factors come together, such as transnational organized crime and criminal networks, which operate as interconnected entities aiming to weaken democracy and governance, with the goal of creating conditions to infiltrate or control cities.

Background information, such as that discussed in this chapter, supports the trend for urban operations to dominate 21st-century conflicts. The continual growth of urbanization, societal diversity, and persistent threats and dangers contribute to the escalation of conflict, as there are many political and economic incentives for state adversaries to choose this setting as their center of gravity.

In this context, it is important to apply and mainstream operational law within the Military Decision-Making Process (MDMP). Among other challenges is the decision to establish the yardstick for the use of force in each situation. It is also crucial to adjust and consider the use of principles that guide actions during hostilities, including military necessity, distinction, proportionality, limitation, non-reciprocity, humanity, and precaution in attack (Ejército Nacional de Colombia, 2017b).

Regarding the actions of the Armed Forces, the research findings highlight the need for further consideration. For instance, the use of weapons during military operations must adhere to a legal framework and be governed by a broad range of rules, principles, and norms of conventional origin. Similarly, its legitimacy must be grounded in the application of the guiding principles of International Humanitarian Law (IHL) and International Human Rights Law (IHRL), which are legal frameworks that complement, coexist with, and converge in non-international armed conflicts (NIACs), in accordance with the Geneva Conventions (Ejército Nacional de Colombia, 2017b).

In this regard, SF must continually analyze and evaluate lessons learned, including those from the Armed Forces of different countries. This will enable them to consult on defense and security matters regarding responses to crisis management situations to address the evolving and adaptable nature of criminal activities.

The research demonstrates that alliances with countries sharing the same threat dimension enable strengthening consultation and improving interoperability through ongoing collaborative efforts. These contexts are suitable for assessing the appropriateness of conducting multinational crisis management operations and establishing suitable mechanisms for exchanging procedures and intelligence for military cooperation with governmental and non-governmental agencies, multinational forces, and other inter-institutional partners.

The main contribution of this study is that it highlights the crucial role of SF. It emphasizes the need to develop versatile mechanisms to devise detailed, suitable, and effective plans, with an appropriate allocation of resources that help identify the enemy's center of gravity (its source of power and moral resistance) and restrict its freedom of action. This allows for the effective direction of military efforts.

In this respect, it is essential to highlight that the Armed Forces of Colombia and other countries have been adapting to a changing scenario, ensuring that SF military units are always trained, qualified, certified, and specialized in critical capabilities according to sociopolitical needs.

Finally, while the comparative case study between Brazil and Colombia presents both similar and contrasting points, it reiterates in a prospective scenario that crime tends to take various forms and suggests that SF will always face additional challenges not investigated in this work. The best way to address conflicts or crises in urban environments is to recognize the need to maintain a dynamic nature that enhances protection effectiveness. Preventing, adapting, and planning ahead is the best way to effectively accomplish the mission in a conflict scenario in megacities and guarantee the stability and security of the population.

Referencias

Álvarez, C. E., Barón, P., & Monroy, V. (2018). Poder astuto: Estrategia del empleo del poder en el siglo XXI. In C. Álvarez Calderón & A. Fernández Osorio (Eds.), *Hacia una gran estrategia en Colombia: Construcción de política pública en seguridad y defensa* [vol. 1: *La "Gran Estrategia": Instrumento para una política integral en seguridad y defensa*] (pp. 171–168). Sello Editorial ESMIC. https://doi.org/10.21830/9789585692862

Alves, L. A. (2018). A *interação civil-militar na situação de não guerra: Uma análise das lições da MINUSTAH* [Presentation]. 10 Encontro da Associação Nacional de Estudios de Defesa, São Paulo, Brasil. https://tinyurl.com/4jeas3w3

Amnesty International. (2017, July 11). *At Any Cost: The Civilian Catastrophe in West Mosul, Iraq*. https://www.amnesty.org/en/latest/campaigns/2017/07/at-any-cost-civilian-catastrophe-in-west-mosul-iraq/

Arnold, T. D., & Fiore, N. (2019). Five operational lessons from the battle for Mosul. *Military Review,* (January–February), 58–71. https://tinyurl.com/4ndbyzj3

Avendaño Arias, J. A., Forero Flórez, J. A., Oviedo Yate, B. S., & Trujillo Vanegas, M. Y. (2019). Entre el Cartucho y el Bronx en Bogotá: ¿Territorios del miedo o expresiones de injusticia socioespacial? *Cuadernos de Geografía: Revista Colombiana de Geografía, 28*(2), 442–459. https://doi.org/10.15446/rcdg.v28n2.73531

Bartolomé, M. C. (2019). *Terrorismo y crimen organizado en Sudamérica* [Research paper, No. 2]. Instituto Español de Estudios Estratégicos. https://tinyurl.com/2p99hcs3

Cazumba, R. A. (2021). O conceito de centro de gravidade: Seu emprego como ferramenta de planejamento nos EUA e no Brasil. *Hoplos, 5*(9), 9–31. https://tinyurl.com/yjepvfta

Comando General de las Fuerzas Militares [CGFM]. (2016). *Disposición N.º 004 de 2016, "por la cual se reestructura el Ejército Nacional, se aprueban sus Tablas de Organización y Equipo TOE y se dictan otras disposiciones"*. https://tinyurl.com/dxxv6da3

Comisión Económica para América Latina y el Caribe [CEPAL]. (1989). *La crisis urbana en América Latina y el Caribe: Reflexiones sobre alternativas de solución.* Organización de las Naciones Unidas. https://tinyurl.com/mvn3p82b

Comisión Económica para América Latina y el Caribe [CEPAL]. (2015). *Objetivos de Desarrollo Sostenible (ODS).* https://tinyurl.com/2pcbr9d3

Datosmundial. (2022). *Crecimiento demográfico en Brasil.* https://tinyurl.com/mva4tjzx

Denécé, E. A. (2009). *A história secreta das Forças Especiais: De 1939 a nossos dias* Larousse do Brasil.

Ejército Nacional de Colombia. (2017a). *Manual Fundamental del Ejército MFE 1.0 El Ejército [Public].* Imprenta Militar del Ejército. https://tinyurl.com/45sujuw5

Ejército Nacional de Colombia. (2017b). *Manual Fundamental del Ejército MFE 6-27 Derecho Operacional Terrestre [Public].* Imprenta Militar del Ejército https://tinyurl.com/2s3627j3

Ejército Nacional de Colombia. (2019). *Disposición N.° 000002 de 2019, "por medio de la cual se reglamentan las reglas de enfrentamiento relativas al uso de la fuerza en las operaciones militares que desarrolla el Ejército Nacional en el marco de los Derechos Humanos y del Derecho Internacional Humanitario"*. Departamento Jurídico Integral. https://tinyurl.com/458ry7dc

Ejército Nacional de Colombia. (2021, September 13). *Agrupación de Fuerzas Especiales Antiterroristas*. https://tinyurl.com/3d7e47b8

Escobar Correa, C. (2022). Should a human rights-based approach to the homeless be used in the neoliberal city? Case study in Bogotá, Colombia. *Latin American Law Review, 1*(8), 111–124. https://doi.org/10.29263/lar08.2022.07

Escuela Superior de Guerra "General Rafael Reyes Prieto" [ESDEG]. (2021). *Revista Fuerzas Armadas, 41*(257) [Protesta social: una visión desde la academia]. https://tinyurl.com/mr4d2uzz

Espinosa, A. (2017, June 14). *La mitad de los civiles muertos en guerras fallecieron en Siria, Irak y Yemen.* https://tinyurl.com/4thuudt7

Fidalgo, A. S., Suárez, C. J., Vallejo, E., & Brasil, A. (2010). Faces da ilegalidade em Bogotá. *Tempo Social. 22*(2), 123–142. https://doi.org/10.1590/S0103-20702010000200007

Freedman, L. (2019). *La guerra futura: Un estudio sobre el pasado y el presente.* Planeta.

González-Martínez, M. A., & Montero-Moncada, L. A. (Eds.). (2020). *Tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder cíber en el siglo XXI*. Sello Editorial ESDEG. https://doi.org/10.25062/9789584288943

Guattari, F. (2017). *Revolución molecular*. Errata Naturae.

Harris, L. C., Dixon, R., Melin, N., Hendrex, D., Russo, R., & Bailey, M. (2014). *Megacities and the United States Army: Preparing for a complex and uncertain future.* Chief of Staff of the Army; Strategic Studies Group. https://tinyurl.com/2hwmuduv

Iberdrola. (2020). *Megaciudades, un reto de futuro.* https://tinyurl.com/4cux4nuf

Instituto Geográfico Agustín Codazzi [IGAC]. (2022). *Colombia en mapas.* https://tinyurl.com/y4cexwer

International Committee of the Red Cross [ICRC]. (2021, November 5). *Reducing civilian harm in urban warfare: a commander's handbook.* https://tinyurl.com/nemctjyh

Izquierdo, J. C. (2018). Cisnes, elefantes, medusas y rinocerontes: Las relaciones internacionales y sus animales. *Comillas Journal of International Relations*, (12), 1–8. https://doi.org/10.14422/cir.i12.y2018.001

Joint Special Operations University. (2021). *Special Operations Research Topics 2022.* The JSOU Press. https://tinyurl.com/yjs9tsk3

Khanna, P. (2016a). *Conectografía, mapear el futuro de la civilización mundial.* Paidós.

Khanna, P. (2016b). How megacities are changing the map of the world [TED Talks]. *YouTube*. https://www.youtube.com/watch?v=U7y4GlmwPLQ

Kilcullen, D. (2013). *Out of the mountains: The coming age of the urban guerrilla.* Oxford University Press.

King, A. D. (2008). Architecture, globalization and identity. In P. Herrle & E. Wegerhoff (Eds.), *Architecture and identity* (pp. 221–232). LIT.

Langewiesche, W. (2008, March 20). City of fear. *Vanity Fair.* https://tinyurl.com/4rcxf3yk

Lawrence, F. (2019). *La guerra futura: Un estudio sobre el pasado y el presente.* Critica.

Lehmann, A. P. (2015, January 15). *¿Ciudades en crecimiento, peligro en crecimiento?* https://tinyurl.com/j65zr6xw

Lisboa, R. A. P. (2017). Avançando pelo labirinto: Procedimentos de progressão em ambiente urbano por FOpEsp [e-mail]. *Revista Segurança e Defesa,* (127).

Mendonça, M. J. (2018). A cidade como espaço de batalha: De Gaza ao Rio de Janeiro, *GEOUSP. Espaço e Tempo, 21*(3), 685–702. https://doi.org/10.11606/issn.2179-0892.geousp.2017.105565

Morán, C. (2021, April 23). Las seis ciudades más violentas del mundo están en México. *El País.* https://tinyurl.com/2n46ayd2

Muggah, R. (2017). El auge de la seguridad ciudadana en América Latina y el Caribe. *International Development Policy,* (9). https://doi.org/10.4000/poldev.2512

Organización de las Naciones Unidas [ONU]. (2015). La Asamblea General adopta la Agenda 2030 para el Desarrollo Sostenible. https://tinyurl.com/2p8sfnpk

Presidência da República do Brasil. (1999). *Lei Complementar N.° 97 de 9 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas.* https://tinyurl.com/mr3445dn

Presidência da República do Brasil. (2004). *Lei Complementar N.° 117 de 2 de setembro de 2004. Altera a Lei Complementar no 97, de 9 de junho de 1999, que dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas, para estabelecer novas atribuições subsidiárias*. https://tinyurl.com/ycys4w6f

Queiroz, F. A., Cunha, G. L., & Correa, A. J. (2022). Terrorismo em Estados Frágeis na Ordem Mundial 2.0: Um estudo exploratório da África Subsaariana. *Omnidef Analisys, 5*(2), 3–14. https://tinyurl.com/yftnd66a

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

Santos, M. (2004). *O espaço dividido.* EDUSP.

Spencer, J. (2022). *Cuenta de Twitter analista militar guerra urbana.* https://bit.ly/3Df8cow

United Nations [UN]. (2015). *70/1. Transforming our world: the 2030 Agenda for Sustainable Development.* https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf

United Nations [UN]. (2018). *World Urbanization Prospects: The 2018 Revision, Online Edition* [Database]. https://tinyurl.com/ybesp72r

United Nations Educational, Scientific, and Cultural Organization [UNESCO]. (2017). *Culture: urban future; global report on culture for sustainable urban development*. https://unesdoc.unesco.org/ark:/48223/pf0000245999

Urban Agenda Platform. (2002). *The New Urban Agenda*. https://tinyurl.com/3rrhp7zr

Valdés-Ramírez, J. C., & Rodríguez-Gómez, A. (Eds.). (2020). *Memorias imborrables: Guardias de honor*. Sello Editorial ESDEG. https://doi.org/10.25062/9789584289001

Wigmore, I. (2017). *VUCA (volatilidad, incertidumbre, complejidad y ambigüedad)*. https://tinyurl.com/nhemcc8j

Wucker, M. (2016). *The Gray Rhino: How to recognize and act on the obvious dangers we ignore*. St. Martin's Press.

Zambrano Gómez, J. A., & Álvarez Calderón, C. (2017). *Globalización desviada: Plataforma de convergencia criminal* [Master's thesis, Escuela Superior de Guerra "General Rafael Reyes Prieto"]. ESDEG.

Chapter 4

Contemporary Cyber Threats: Challenges for Special Operations in Colombia*

DOI: https://doi.org/10.25062/9786287818408.04

José Nicolás Rodríguez Rodríguez
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Oscar Garzón
Joint Special Operations Command

Abstract: This chapter provides a comprehensive examination of the challenges faced by Colombian Special Forces units in cyber threat scenarios, which include both regular and irregular situations, the use of advanced technical and technological tools, information operations, cyberattacks, and high levels of information manipulation capabilities. To achieve this, the effects of modern cyber threats are identified based on their key elements, and the nature of these new types of conflicts is analyzed to assess the strengths and weaknesses of the Special Forces. In this way, full immersion of these units in the digital age is proposed, preparing them for cyber warfare and encouraging them to adapt in critically sensitive areas, such as the fifth element of warfare.

Keywords: threats; capability; cyber; warfare.

* 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.

José Nicolás Rodríguez Rodríguez
Lieutenant Colonel in the Colombian National Army's Special Forces. Master's (cum laude) in Cyber Defense and Cybersecurity, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Military Unit Leadership and Specialization in National Defense Resource Management, 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: **jose.rodriguezrod1@buzonejercito.mil.co**

Oscar Garzón
Lieutenant Colonel in the Colombian National Army's Special Forces. Master's in Strategy and Geopolitics and Diploma in General Staff, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Master's in War Studies, King's College London. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia.
https://orcid.org/0009-0001-5826-9008 - Email: **oscar.garzon@buzonejercito.mil.co**

APA Citation: Rodríguez Rodríguez, J. N., & Garzón, O. (2025). Contemporary Cyber Threats: Challenges for Special Operations in Colombia. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 87-104). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.04

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 wealth of information on developing operations in cyberspace has reached a new level, enabling security and defense organizations to develop unique skills or specialties within each institution or force. Faced with an exponential growth in the concept and significance of cybersecurity worldwide,

> […] state and non-state actors have developed cyber capabilities, both offensive and defensive, that have triggered a reexamination of traditional notions of global power, influence and even warfare. (Inter-American Defense Board, 2020, p. 6)

Various institutional strategies have been implemented to address the various risks and threats identified in cyberspace, allowing for the exploration of new initiatives in the development of military operations and, primarily, their direct inclusion in areas such as Special Forces (SF).

The main reason for using SF in any country is to protect national sovereignty, independence, territorial integrity, and the constitutional order from both internal and external threats. The achievement of this goal is always overseen by civilians, carried out under the constitutional authority of the President of the Republic as the Supreme Commander of the Military Forces (Ejército Nacional de Colombia, 2018).

The thesis is that Special Operations (SO) in Colombia face certain challenges. Given the implications of cyberattacks, their use by SF units is critically important, especially when dealing with hostile forces that threaten national security and defense. Therefore, the doctrinal and operational nature of these offensive and defensive capabilities can offer a strategic advantage in conducting military operations, especially SO.

In a context where "cyber threats to the security of the Western Hemisphere are becoming more frequent, complex, destructive, and coercive" (Inter-American Defense Board, 2020, p. 6), state actors, mainly security and defense organizations like the Colombian Armed Forces, are compelled to consider the need to incorporate the challenges of the fifth domain of warfare into their doctrine. To do this, they must analyze historical events at both the national and international levels, understand the cyber system and its components (Patiño, 2019), assess the challenges posed by the increase in cyber threats to Colombian SO, and analyze specific reference topics to improve their capacity.

In this regard, it is worth highlighting the document *Media Literacy and Digital Security: The Importance of Staying Safe and Informed,* prepared by the Organization of American States (OAS, 2019), and Twitter (now called X). It aims to inform and raise awareness about managing, consuming,, and distributing information online, with a greater focus on social media and the entire social structure that connects individuals in a digital domain. Furthermore, it aims to help all individuals, government authorities, and organizations better understand the importance of literacy and cybersecurity. In this way, it projects how SF units should use these tools to take advantage of enemy misuse.

The rise in digital activities has revealed existing vulnerabilities in the digital realm. The increasing number of cyberattacks and the digitization of many daily processes emphasize the need to improve cybersecurity literacy and awareness (Nivea & Gazapo, 2016). This edition of the guide offers a renewed emphasis on tools and best practices for consuming information and content safely and responsibly.

Technological platforms and social media have introduced new forms of communication, broadening the opportunities for political participation by integrating the digital environment into democratic processes. Digital literacy is crucial for strengthening democracy, as it encourages widespread participation and promotes active, responsible citizen engagement. Similarly, literacy helps combat issues like misinformation and interference from external actors in domestic politics, among other factors, which can directly or indirectly affect and shape democratic processes.

Through its various sections, the guide compiles information on cybersecurity and digital self-care. It has been updated to address the new threats and tools that have emerged as a result of changes in the environment and the increase in remote work. It also includes specific recommendations regarding the consumption of information on Twitter and the updating of its rules of use, as well as essential tools for people's experience on the platform.

All of this leads us to consider that the widespread use of digital technologies worldwide will continue to be part of daily life. Therefore, cybersecurity and digital literacy, practiced by each individual, are crucial to ensure they can benefit from connectivity and information securely. This way, it will be possible to create an environment with greater opportunities for development, social well-being, and the strengthening of democracy in a country.

Thus, the resulting research question is: What should be the mechanism by which Colombian SO can face the challenges posed by current cyber threats? It is important to note that SF operations are strategic for the nation, so this mission, applied to a hybrid warfare scenario within a cyber environment (Colom, 2012), allows them to put their unconventional warfare capabilities into practice.

Specifically, the latter emphasizes the vulnerabilities of civil and military societies that are typically not visible to the naked eye, enabling them to maintain a specific design to influence all types of operational environments and carry out lethal and non-lethal actions both domestically and internationally, while remaining below certain detection and response thresholds (Mitaritonna, 2019). These features provide a broad strategic context for utilizing SF capabilities alongside other instruments of national power, such as cyber threats to national security and defense (Realpe & Cano, 2020).

Regarding the specific situation in Colombia, it should be noted that the cyber threats posed by disruptive technologies to state law enforcement indicate a dangerous trend toward compromising national security and defense. To address these risks, a comprehensive strategy is needed to counter, if necessary, the resistance to disruptive and destructive attacks. This strategy must be incorporated within a digital transformation framework (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017).

Indeed, this document offers a general overview of the current state of cyber defense in Colombia. It identifies and references latent and emerging cyber threats using the AREM (Spanish acronym for emerging threats and risks) Window. According to Realpe and Cano (2020), this analysis tool examines seven disruptive technologies in the short term, aiming to develop a military cyber defense strategy that enables organizations—such as SF—to have a technological immersion. This approach helps them respond to cyber threats with a strategic, comprehensive, systemic, and forward-looking perspective.

In addition to the above, an organization with highly trained, capable, mobile, flexible, and adaptive units appears on the scene, capable of operating independently

in a volatile, uncertain, complex, and ambiguous (VUCA) environment for extended periods and offering significant strategic value for a nation, with an urgent need to enhance its operational dynamics and develop new capabilities in the fifth domain of warfare.

Threats to Colombia's Security and Defense with Cyber Capabilities

To identify the strengths and weaknesses of security and defense operations in the fifth domain of warfare, it is essential to understand the nature of new confrontations emerging in the digital age. Cyberspace is not inherently secure or protected, making it vulnerable to latent or emerging cyber threats and attacks. This can lead to significant losses in economic, political, and social sectors, as well as pose serious risks to defense or national interests. Therefore, developing cyberspace capabilities is a priority for Colombia's security and defense, especially as the country becomes more dependent on technology. Consequently, deploying military operations in cyberspace is necessary for the advancement of current defense models (Sánchez & Rodríguez, 2010).

Day after day, the landscape seems to produce a new class of threats, each one more technologically advanced than the last, as it takes advantage of the massive explosion of technology. In this scenario, the risks that can jeopardize a nation include the proliferation of information and the ease with which people communicate via any medium, global network connectivity, informal remote work, the misuse of cyberspace for illegal activities, and the degradation of social media management.

In response to this situation, there has been growing interest among the specialist community in ensuring national security and defense, deciphering the role of SF units, and addressing emerging threats inherent in the activities of the contemporary international system. For this reason, from an operational perspective, the actions of modern militaries include cybersecurity, cyberdefense, information operations, electronic warfare, cyberwarfare, hybrid warfare, and other concepts that cover a broad spectrum of risks that had not been considered in the traditional functions and capabilities of the Armed Forces (Miguel-Gil, 2019).

To understand the efforts that states make to guarantee their security and defense in digital scenarios, it is essential to understand the theory of realism

and, particularly, Hans Morgenthau's theory of state-centricity. According to Barbe (1987), each State is a rational actor that always acts according to its own interests and with the primary objective of ensuring its own security. To this end, it defines and implements certain parameters related to the defense of its sovereignty as the exclusive objective of international relations and the protection of its defense interests through military power or soft power.

In this regard, defining a proposed military cyber defense strategy constitutes an effective response to the evolving risks and threats that a country's security and defense face due to disruptive technologies in a contemporary conflict. In line with the above, Colombia proposed a systemic model based on strategic objectives that were analyzed in each of the cyber components. To achieve this, it was necessary to delimit and prospectively define the direction in which SF should go, in order to develop the military capabilities they need to carry out cyber operations, supported by a legal and constitutional framework, as well as to involve all the organization's capabilities to execute SO in an unconventional war.

The importance of establishing a cybersecurity model lies in significantly enhancing a nation's defensive and offensive capabilities in cyberspace. This improvement allows the nation to enhance its adaptability and control, enabling it to develop a modern national cyber force with unique strategic capabilities. Thus, an effective and fully interoperable organization could be established to defend and secure a territory, with distinction in the fifth domain of warfare.

Furthermore, it must be taken into account that cyberspace is changing rapidly, such that the world's cultural landscape will increasingly challenge traditional concepts of society and national identity. According to Colom et al. (2013), "situational awareness in cyberspace means that once a sufficient level of maturity in cyber defense techniques and means has been reached" (p. 90), it is necessary to continue improving and have the ability to dynamically determine the security level of the systems under one's control. This will enable the appropriate use of resources and the application of risk management principles by leveraging threat information and probabilistic models obtained from the analysis of security data.

This constantly changing situation requires States to respond immediately to threats based on the information they receive about security incidents. To achieve this, they must rely on complex data visualization techniques that allow them to make the right decisions in the shortest possible time. They must also consider the current state of situational awareness systems for cyber defense and the importance of information visualization.

Indeed, according to Medina-Ochoa (2019),

> Cybersecurity is a challenge for Colombia, presenting a scenario where the State must use all available means to preserve its interests and protect not only its critical infrastructure, which falls under the jurisdiction of the Military Forces. (p. 5)

Raising awareness about these new threats in the field of cybersecurity and cyberdefense requires the participation of all public, private, and mixed entities, as well as the academic sector, given that the risks can escalate and, therefore, seriously impact state security (Miranzo & Del Río, 2014). Aware of this situation, in the case of Colombia, the National Council for Economic and Social Policy (CONPES) defined the multiple stakeholders in the National Digital Security Framework (CONPES 3854 of 2016): the national government and territorial governments; public and private organizations; law enforcement; owners or operators of national critical cyber infrastructure; academia; and civil society. These actors rely on the digital environment for all or part of their economic and social activities, which may lead them to assume different roles and specific responsibilities in digital security actions (CONPES 3854 de 2016).

As can be deduced, maintaining the pace of development in this domain is a challenge for national defense, as it requires not only dedication but also an immense investment of resources. For this reason, it is essential that cyber capability be implemented as a tool in all areas of the Armed Forces, which is only possible with immersion in the cyber domain, at the doctrinal and expert levels (Aguilar-Antonio, 2019). It should be added that despite all the challenges described, the most basic problem in the cyber domain is the lack of a shared conceptual basis to address them. The absence of shared terminology, procedures, and international judicial precedents makes it difficult to establish effective deterrence. This situation arises despite the fact that the focus on maintaining state sovereignty and security has been one of the concerns on the political agenda of countries (Guerrero, 2022), given the transformations in the environment, globalization, and the transnationalization of practices such as terrorism and drug trafficking, which have delegitimized social and political institutions. In a national and international strategic scenario, threats that disrupt a nation's balance, stability, and security must be prioritized, along with the numerous actions that can be taken in the non-physical world.

Challenges for Colombian Special Operations: Lessons from the Russian Annexation of Crimea

The fourth technological revolution expanded the spectrum of risks and threats to national security and defense. It transformed the domain of cyberspace and initiated the construction of new scenarios for implementing strategies to counter adversarial actions (Medina-Ochoa, 2019). For example, terrorist attacks, whose intensity was magnified by the perception of insecurity they generated in public opinion, are now drastically transformed through the use of technological tools and social media. As a result, cyberterrorism has become a global weapon that threatens States, military organizations, business empires, banking institutions, and individuals without distinction (Poveda & Torrente, 2017).

This phenomenon has raised the need for secure means of data transmission (secure networks). However, the ability to effectively respond to threats in cyberwarfare comes with the challenge of defining borders and specific areas to combat them. This also raises awareness that this is a global problem, and it is not possible to counteract all the risks of the cyberspace domain.

According to Arteaga (2019), "as the postwar liberal order disappears and the new global order continues to grow" (p. 109), geopolitics returns, and the great powers use their economic and technological instruments to strengthen their capacity for global influence. This return to geopolitics is fueled by the accelerated process of technological change underway, as well as the race among the great powers to control new technological developments and analyze the impact of technological disruption on the dynamics of geopolitical competition among countries such as Russia, the United States, and China, key players that have developed this capability in offensive and defensive operations in the cyber domain.

During military operations, battlefields become fractured zones where the level of confusion, noise, and ambiguity significantly impacts the achievement of operational and tactical objectives. In this context, situational awareness (SA) becomes a challenge because situational perception is unstable, leading to degraded understanding and the soldier's inability to project appropriate outcomes. To address these challenges, several military projects have focused on designing integrated digital systems to support personnel decision-making and employing cyber soldiers to mitigate risk in the fifth domain of warfare.

Furthermore, the incorporation of new technologies and communication media significantly impacts decision-making in cyberspace. For instance, in the

context of the conflict between Russia and Ukraine, it has been documented that General Valery Vasilyevich Gerasimov (Chief of Staff of the Russian Armed Forces) developed a war approach that employs hybrid instruments and non-military actions that can have a greater impact in a gray zone—that is, a combination of capabilities to execute military operations in the course of the conflict. In the 2014 invasion of Crimea (Ukraine), the Russian Special Forces (Spetsnaz) were key players because they employed this type of special organization in an unconventional warfare environment.

Specifically, hybrid warfare is a type of compound confrontation in which destabilizing a nation, gaining control of its resources, and destroying the values of its society play a decisive role. To this end, an unprecedented disinformation operation (Beleño, 2020) is being developed, significantly transforming the inclusion of SF parameters into cyberwarfare. In the case of Ukraine, Russian forces employed different strategies that enhanced the effectiveness of the invasion of the territory and the subsequent annexation of Crimea to the Russian Federation.

According to Hoffman (2007), hybrid warfare consists of a threat that is susceptible to use by both state and non-state actors, taking advantage of the full range of available modes and styles of combat (p. 23). In short, these characteristics of hybrid warfare have been applied in international conflict to exploit non-regular capabilities, aiming to dismantle the aggressor system through a machinery of disinformation, sabotage, and cyber operations.

In any case, the truth is that Russia understood in 2014 how to integrate technological capabilities with SF and Russian separatist groups, with the aim of using them in the invasion of Crimea and on the border with cyberattacks. Similarly, it managed to attack critical infrastructure in the region using cyber capabilities, thus destabilizing government and banking entities, as well as logistics and railway infrastructure.

Still, in order to understand the capabilities of the Russian SF in this conflict and to distill the lessons learned, two important questions arise: Who are the Spetsnaz really? Why were the special units able to integrate cyber capabilities into their missions?

The Spetsnaz are military units formed on October 24, 1950, composed of elite SF men who belong to the Russian military and police forces. Hierarchically, they report to the Central Intelligence Department of the General Staff of the Armed Forces. According to García (2022), the United States stated that "1,500 soldiers called Spetsnaz were responsible for the first attacks on Ukraine […]. The Spetsnaz

are units specialized in stealth, sabotage, and infiltration of enemy lines." These characteristics are perfect and essential for them to carry out cyber actions against their adversaries, as they allow them to insert themselves behind enemy lines or maintain a low profile for long-term reconnaissance and surveillance missions.

Likewise, Russia sought to exploit the tools of cyberspace and recruited virtual "corsairs" and bounty hunters to carry out cyberattacks against Ukrainian government information. In the emerging geopolitical and virtually uncertain dimension, Spetsnaz managed to change its modus operandi. Russia generated epic flows of disinformation, both inside and outside Ukraine, not only to obscure cyber-enabled unconventional warfare, but also to create complete political illusions. Therefore, it was not a question of developing simple disinformation strategies, but rather ones that were structured in a complex and meaningful way. Accordingly, impersonations, forgeries, lies, leaks, and cybersabotage, generally associated with information warfare, were developed in advance to minimize resistance.

At that time, cyber disinformation managed to create a state of confusion and chaos among the Ukrainian population. This allowed cyberattacks to buy time and space for the Spetsnaz, armed with computer equipment, to execute their plans on the region's strategic infrastructure. Additionally, some of the characteristics of the "Spetsnaz GRU" were decisive in the performance of the cyber cells: teams of two soldiers or even individuals who apply techniques and tactics in special missions, allowing them greater mobility and rapid infiltration into critical areas.

Thanks to all these elements, Russia brilliantly achieved its objectives in the occupation operation, not only because of the hybridization of its cyber and SF capabilities, but also because it successfully invaded a European Union partner nation without provoking any significant Western military response. It should be noted that the Russian SF are a key player in the various counterterrorism fights taking place around the world due to their distinctive capabilities. These outstanding characteristics are based on the quality of their training in assault and infiltration, sabotage operations, cyber espionage, and target destabilization—areas that establish these units as a benchmark in unconventional warfare and high operational effectiveness (Sancho, 2017).

It should also be noted that Russia is a cyber superpower, with a significant arsenal of technological tools, accompanied by virtual mercenaries and hackers capable of executing disruptive and potentially destructive attacks. Likewise, a deeper analysis of their capabilities reveals they can carry out packaged attacks, exploiting their adversary's specific vulnerabilities.

This case study highlights the emerging capabilities that SF must develop to address cyber risks and threats on both offense and defense.

Recommendations to Colombian Special Forces on Special Reconnaissance and Direct Action in a Cyber Scenario

SF operations differ from those of conventional units primarily due to the risks they take and the operational techniques they employ to accomplish their mission (Ejército Nacional de Colombia, 2018). This means they have distinctive capabilities and focus on surprise, initiative, and decisiveness. Their effectiveness is further enhanced if, in addition to their skill, the advantages offered by cyberspace dominance in conventional warfare are leveraged to gain an edge in the battle against adversaries.

However, it should be noted that a series of factors affect the modern operational environment. The enemy, which is "not" present in the physical environment, is immersed in a cyber world and has chosen to carry out its activities through a "virtual identity," has a differentiating signature that modifies the way wars and battles are conducted. For this reason, responsible differentiation of the cyberspace environment must ensure the identification of the threats that abound in this type of domain.

Consequently, commanders must ask themselves: How should cyber capabilities be used in SO? And, therefore, for what purpose exactly are they being used? Furthermore, they must closely observe the changes that occur when trying to counter these types of threats.

In this regard, it is important to observe the behavior of internal threats, which effectively use the capabilities offered by cyberspace to further their criminal activities. For example, there are threats in the internal armed conflict that also use the capabilities offered by the cyberspace domain, as was the case with Andrés Felipe Vanegas Londoño, aka *Uriel* or *Pedro,* who was the third-in-command of the Western War Front of the National Liberation Army (El Tiempo, 2020) and who carried out his terrorist and drug trafficking activities in Chocó.

Despite having a physical presence in the region, he decided to use the cloud as a tool for recruiting young people. Using the anonymity and secrecy offered by social media, he financially supported the higher education of young militants in

exchange for their completion of a work plan within the ELN social and student movement (El Tiempo, 2020). This type of event supports the arguments of Jaime Blasco, director of the Alien Vault Security Labs in Silicon Valley, who asserts that

> […] cyberwarfare complements traditional warfare and at the same time reflects its customs and traditions. Cyberwarfare also involves soldiers and spies: employees of the armed forces and intelligence services, many of them recruited from universities, but also members of the criminal hacker underworld, dedicated to carrying out missions against the interests of other countries. (Bassets, 2015, p. 14)

To analyze these types of risks and threats, it is essential to elaborate on key concepts that foster the doctrinal structuring needed to counter them, as they will surely continue to evolve with technological innovations. However, according to Vergara and Trama (2017), "currently there are no common definitions for expressions related to cybernetics, not even in regional contexts" (p. 21). Therefore, to identify the cyber capabilities that SF must develop, it is important to take into account the military doctrines in the field of cyber defense developed by countries such as the United States, France, Denmark, Finland, Italy, Israel, the Netherlands, Estonia, Spain, and Brazil, as well as the contributions that can be drawn from the North Atlantic Treaty Organization (NATO) and the European Union (UE).

Cyber Capabilities in the Special Forces

At this point, it should be noted that the idea of integrating cyber capabilities into SF crosses the line proposed by the United Nations Security Council on March 5, 2011, which, through Resolution No. 1113 of 2011, called on all nations to cease the development of cyber capabilities and to repudiate the use of cyberwarfare tactics.

Even so, distinctive cyber capabilities are necessary to contain "symmetric or asymmetric offensive and defensive threats by the State" (Vergara & Trama, 2017, p. 37), which may be related to accessing, disrupting, destroying, or otherwise altering state or interstate actors that put the security and defense of the nation at risk.

Education and Cyber Culture

For Conti and Surdu (2009),

> Cyber warfare requires unique technical skills as well as skills in creative problem solving, poise under pressure, and critical thinking. Attributes that are

> desirable in soldiers, such as physical endurance, marksmanship, and technical skills associated with the employment of traditional forces and weapons systems, do not translate well to cyber warfare. (p. 17)

Therefore, the training and preparation of "cyber warriors," as they would be called in the SF, or in our particular case "cyber commandos," must go far beyond common skills developed in other domains so that they can be more effective in the strategic missions they execute for the nation (González-Martínez & Montero-Moncada, 2020).

Doctrinal Legitimacy in the Cyber Environment

The complex use of these capabilities must consider the *Tallinn Manual* to legitimately and alignigly implement the doctrine in cyber operations of SF. At this point, it can be said that information operations in the vast majority of States have a strong connection, allowing them to focus the efforts of SF and promote various actions, potentially becoming the primary approach to a real doctrine of employment.

Cyber Special Forces in the National Army

Military information support operations (MISO), deception operations, computer network operations (passive, active, and exploratory), security operations, electronic warfare, public relations, and civil-military operations would largely be the first phase of development of Cyber Special Forces in the National Army, as they would in turn allow the integration of more complex techniques, tactics, and procedures than could be executed in the long term (Espitia et al., 2021). In addition,

> Achieving the integration of a cyber force into the Special Forces component of the National Army will allow, in specific missions, to guide activities that will be related to computer network attacks (CNA), computer network defense (CND), and computer network exploration (CNE), which are contained in offensive, defensive, and information network cyber operations. (Vergara & Trama, 2017, p. 239).

Cyber Cell Capabilities

Including cyber cell capabilities in the reconnaissance teams of the Colombian SF provides differential access to the cyberspace domain, offering the organization the

opportunity to acquire unique skills for SO development, as defined in Colombian doctrine.

Cyber cells are, in essence, a capability for national cybersecurity and cyberdefense (Colom et al., 2013). The work of Colom et al. (2013) shows that currently, with the exception of pioneering countries in cybersecurity and cyber defense, such as the United States, China, and Israel, most States are developing their basic cyber capabilities, information and communications technologies, organizations, and procedures that will make them operational when they reach maturity. When that occurs, it will be necessary to coordinate the organization and operational procedures, such as cyber cells, to operate with these capabilities. They are also defining the concept of cyber cells, including their functions, tasks, scope, and the enablers that will make their operation possible (Pons, 2017).

Although this is a next-generation capability and complements those currently being deployed, the authors propose that, in the case of Spain, it is necessary to reflect on the type of cyber cells that would enhance the cybersecurity and cyberdefense capabilities being developed by the Armed Forces and state security forces. This is especially true considering that a cyber cell can be an effective tool for both the security forces and the Armed Forces of a State to improve the security and defense of a specific cyber environment (Colom et al., 2013).

Finally, it should be noted that cyber cells would consist of operational and tactical teams under the control of a strategic cyber command. This setup requires the prior existence of mature traditional cybersecurity and cyber defense capabilities, a modern ICT infrastructure, and experienced personnel accustomed to operating in this environment. In this way, cyber cells could conduct defensive and offensive cyber operations, support the evaluation and improvement of national, multinational, or allied capabilities, while allowing for experimentation with new operational concepts or training of personnel assigned to this organization.

Recruiting Ethical Hackers

In the context of this work, it is important to analyze the recruitment of white hat hackers to work with SF in a hybrid war, whether in an internal or external conflict, and to fully understand the operational environment related to cyber threats.

Currently, personnel with these capabilities are primarily experts in computing, who have had to empirically or academically explore the knowledge necessary to acquire these skills. In some very specific cases, there are hackers for hire who, while participating in cyberwars or developing highly specialized technologies,

do not do so alongside troops on the ground. There are also the classification or types of hackers, which in academia are classified as follows: black hat (malicious hacker), white hat (ethical hacker), grey hat (not malicious, but not very ethical), green hat (amateurs), blue hat (vengeful), and red hat (vigilant).

Therefore, it must be taken into account that the recruitment process involves some negative variables that can potentially have dangerous consequences for security and defense institutions. Thus, coordination is required to focus on new institutional transformations.

The Department of Special Operations in Cyberspace

Including a department dedicated to SO in cyberspace is a short-term priority because, as discussed in the previous section, there are risks that must be managed by an organization capable enough to determine the doctrine, organization, material, and equipment, personnel, and infrastructure (DOMPI) necessary to structure specific plans for the multiple activities required at the strategic, operational, and tactical levels.

Conclusions

Colombia is experiencing an evolution in the doctrinal concepts and precepts of modern warfare, which requires strengthening initiatives that transcend traditional security and defense capabilities. The influence of sixth-generation warfare in current conflicts, such as those in the Middle East and Eastern Europe, is setting the roadmap for the preparation that the Armed Forces must have to contain the expansion of risks and threats in cyberspace.

The use of SF in SO enhances all security measures before, during, and after the planning and mission, necessitating numerous security activities to counter their vulnerability.

The involvement and use of both SF and cyber operations can significantly enhance the nation's cybersecurity and cyber defense, allowing for the creation of specialized cyberwarfare cells.

Therefore, this chapter recommends that the Colombian Military Forces: develop cyber capabilities within SF; establish a cyber education and culture program; ensure doctrinal legitimacy in the cyber realm; create Cyber Special Forces units in the National Army; enhance cyber cell capacity; recruit ethical hackers; and set up a Department of Special Operations in Cyberspace.

References

Aguilar-Antonio, J. M. (2019). Hechos ciberfísicos: Una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad,* (25), 24–40. https://doi.org/10.17141/urvio.25.2019.4007

Arteaga, F. (2019). Disrupción tecnológica y orden global. *Revista UNISCI,* (51), 109–128. https://tinyurl.com/mrxnrzst

Barbe, E. (1987). El papel del realismo en las relaciones internacionales: Teoría de la política internacional de Hans J. Morgenthau. *Revista de Estudios Políticos,* (57), 149–176. https://tinyurl.com/mpwzp726

Bassets, M. (2015, February 8). El más fuerte es el más vulnerable: EE.UU. es víctima y, a la vez, el más poderoso agresor en el 'cibertablero' mundial. *El País.* https://tinyurl.com/mrx756zy

Beleño, B. (2020). *Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam* [Specialization capstone, Universidad Nacional de Colombia Abierta y a Distancia]. Repositorio UNAD. https://tinyurl.com/2susm9p9

Colom, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova, 10*(10), 77–90. https://doi.org/10.21830/19006586.228

Colom, P., Coz, J., Fojón, E., & Hernández, A. (2013). Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales. *ARI,* (26), 1–10. https://tinyurl.com/2p8puuvv

Consejo Nacional de Política Económica y Social [CONPES]. (2016). *Política Nacional de Seguridad Digital, CONPES 3854.* Departamento Nacional de Planeación. https://tinyurl.com/bdzhjvdy

Conti, G., & Surdu, J. (2009). Army, Navy, Air Force, and Cyber: Is it time for a cyberwarfare branch of military? *A Newsletter, 12*(1), 14–18. https://tinyurl.com/2bscnp7h

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357–377. https://doi.org/10.21830/19006586.588

Ejército Nacional de Colombia. (2018). *Manual de Campaña del Ejército MCE 318 Operaciones de Fuerzas Especiales [Restricted].* Imprenta Ejército.

El Tiempo. (2020, October 25). ¿Quién era y cómo operaba "Uriel", el terror del ELN en Chocó? https://tinyurl.com/shjz4t8x

Espitia, A., Agudelo, J., & Ramírez, T. (2021). Percepciones sobre innovaciones tecnológicas en el Ejército colombiano. *Revista Logos, Ciencia & Tecnología, 13*(2), 85–102. https://doi.org/10.22335/rlct.v13i2.1408

García, B. (2022, March 9). Las Fuerzas Especiales de Rusia: ¿Quiénes son los Spetsnaz? *Noticiero Televisa.* https://tinyurl.com/4d4dxhec

González-Martínez, M. A., & Montero-Moncada, L. A. (Eds.) (2020). *El tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder cíber en el siglo XXI.* Sello Editorial ESDEG. https://doi.org/10.25062/9789584288943

Guerrero Vallejo, G. Y. (2022). *Operaciones cibernéticas y seguridad hemisférica en Colombia: Análisis desde la cooperación regional e internacional* [Master's thesis, Universidad Santo Tomás]. Repositorio USTA. https://tinyurl.com/2s3s5st3

Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars.* Potomac Institute for Police Studies. https://tinyurl.com/dyc5rmnv

Inter-American Defense Board. (2020). *Cyber Defense Handbook. Guidelines for the Design, Planning, Implementation and Development of a Military Cyber Defense.* https://jid.org/wp-content/uploads/2022/01/Cyber-defense_handbook_ing.pdf

Medina-Ochoa, G. (Ed.) (2019). *La seguridad en el ciberespacio, un desafío para Colombia.* Sello Editorial ESDEG. https://doi.org/10.25062/9789585216549

Miguel-Gil, J. (2019). El tratamiento informativo de la guerra híbrida de Rusia. *URVIO, Revista Latinoamericana de Estudios de Seguridad,* (25), 108–121. https://doi.org/10.17141/urvio.25.2019.4006

Ministerio de Defensa Nacional. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia.* https://tinyurl.com/455ky3f2

Miranzo, M., & Del Río, C. (2014). La protección de infraestructuras críticas. *UNISCI Discussion Papers,* (35), 339–352. https://tinyurl.com/36k8z69t

Mitaritonna, A. D. (2019). *Empoderamiento de la conciencia situacional en operaciones militares utilizando realidad aumentada* [Doctoral dissertation, Universidad Nacional de La Plata]. Repositorio UNLP. https://tinyurl.com/yuz3ucke

Nieva, M., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *UNISCI Journal,* (42), 47–68. https://tinyurl.com/mrejyh6a

Organization of American States [OAS]. (2019). *Media Literacy and Digital Security: The Importance of Staying Safe and Informed.* https://www.oas.org/en/sms/cicte/docs/Media-Literacy-and-Digital-Security.pdf

Patiño Orozco, G. A. (2019). El sistema internacional cibernético: Elementos de análisis. *Oasis,* (30), 163–186. https://doi.org/10.18601/16577558.n30.10

Pons Gamón, V. (2017). Internet, la nueva era del delito: Ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 80–93. https://doi.org/10.17141/urvio.20.2017.2563

Poveda Criado, M. A., & Torrente Barredo, B. (2016). Redes sociales y ciberterrorismo: las TIC como herramienta terrorista. *Opción, 32*(8), 509–518. https://tinyurl.com/mr3r78tc

Realpe, M. E., & Cano, J. (2020). Amenazas cibernéticas a la seguridad y defensa nacional: reflexiones y perspectivas en Colombia. In V. Gauthier, R. A. Méndez, J. Cano, J. Ramió & L. E. Sánchez (Eds.), *Seguridad informática: X Congreso Iberoamericano, CIBSI 2020* (pp. 105–113). Universidad del Rosario. https://doi.org/10.12804/si9789587844337.10

Sánchez, D. R., & Rodríguez, F. (2010). Seguridad nacional: el realismo y sus contradictores. *Desafíos*, (15), 119–177. https://tinyurl.com/mu2vbmu6

Sancho, C. (2017). Ciberseguridad: Presentación del dossier. *URVIO. Revista Latinoamericana de Estudios de Seguridad,* (20), 8–15. https://doi.org/10.17141/urvio.20.2017.2859

Vergara, E., & Trama, G. A. (2017). *Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina. https://tinyurl.com/mr3cyap4

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.ilmar@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.

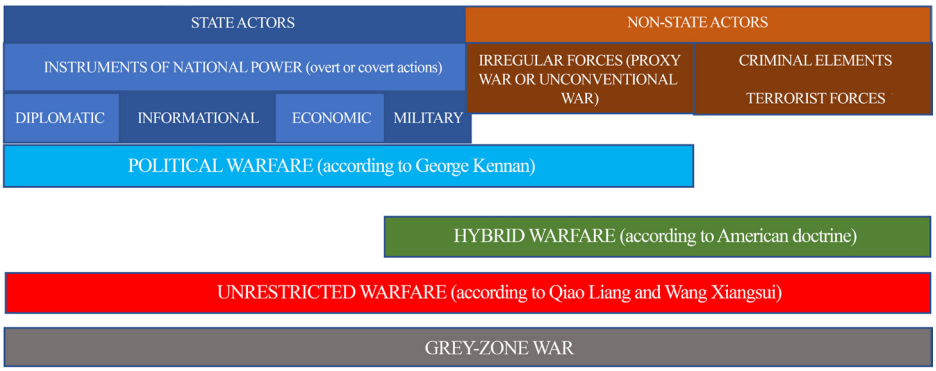
Likewise, the United Nations Charter has consolidated a progress derived from the mechanisms established in the law of war—hereinafter, *ius ad bellum*—that seeks to understand the reasons States give for just war and the confusion that arises from them. Thus, political war becomes an impermissible method 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).

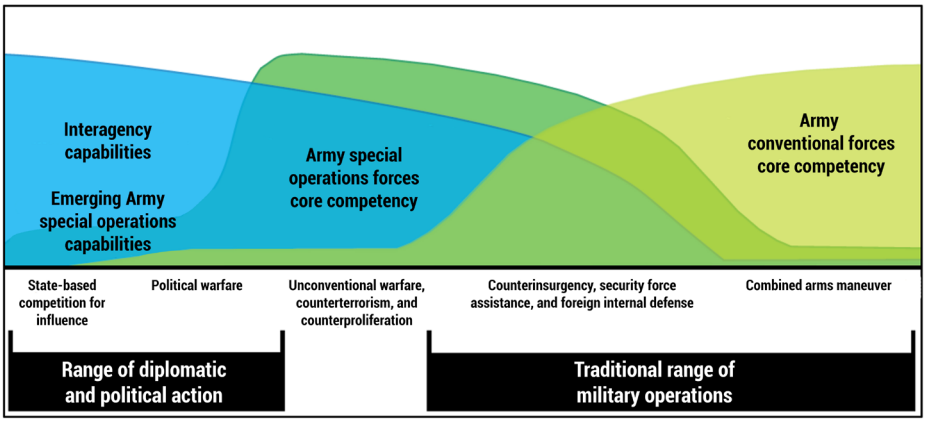
During the 1980s and 1990s, the American defense system reactivated the SF to respond to threats posed by nations in the Pacific Rim, the Caribbean, and Africa. This SF played a pivotal role in combating guerrilla movements and containing the spread of communism in Central and South America by leveraging 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/4vtdxtxd

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/mph8rb95

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/37wsnfnk

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

EDITORIAL ESDEG

Chapter 6

Special Warfare: From Tactics to Practice*

DOI: https://doi.org/10.25062/9786287818408.06

Jorge Rafael Gutiérrez Oliveros
Luis Alexander Montero Moncada
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This research chapter aims to highlight the importance of foreign internal defense operations and unconventional warfare as components of Special Forces Operations within the context of contemporary wars. It initially defines the concept of special warfare as a critical capability of Special Forces and describes two specific operations within this capability: foreign internal defense and unconventional warfare. Next, it discusses the benefits of developing Special Forces Operations, generally using examples of special warfare operations implemented by other countries as part of their national strategies. Finally, the chapter examines the impacts of these operations on contemporary conflicts.

Keywords: critical capability; contemporary conflicts; strategy; Special Forces; special warfare.

* 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.

Jorge Rafael Gutiérrez Oliveros

Lieutenant Colonel in the Colombian National Army Special Forces. Bachelor's in Military Science, Escuela Militar de Cadetes "General José María Córdova," Colombia. Specialization in Leadership and Management of Military Units and in Military Resources Administration for National Defense, Arms and Services College. Guest instructor at USAJFKSWCS. Email: **gutierrezjr@esdeg.edu.co**

Luis Alexander Montero Moncada

PhD candidate in Political Studies, Universidad Externado de Colombia, and in Political Studies and International Relations, Universidad Nacional de Colombia. Master's (honoris causa) in Strategic Intelligence, Escuela de Inteligencia "Brigadier General Ricardo Charry Solano," and in Analysis of Contemporary Political, Economic, and International Issues, Paris Institute of Political Studies Sciences-Po, Universidad Externado de Colombia, and Colombian Ministry of Foreign Affairs. Bachelor's in Political Science with an emphasis on International Relations, Universidad Nacional de Colombia.
https://orcid.org/0000-0003-3420-0863 - Email: **luis.montero@esdeg.edu.co**

APA Citation: Gutiérrez Oliveros, J. R., & Montero Moncada, L. A. (2025). Special Warfare: From Tactics to Practice. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 129-146). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.06

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 changing nature of warfare requires consideration of the appropriate approach to its management. In this context, Special Forces (SF) are emerging as a key component in the planning and development of military operations across an increasingly broad range of approaches and uses.

Although new concepts have recently emerged to identify the different types of warfare in our time, three central factors are related to the new definitions of "war": the diversification of threats, the multidimensionality of conflicts, and the constant evolution of information technologies. Currently, there is no consensus on a universal definition of war; rather, several meanings define distinct activities: world wars, religious wars, asymmetric warfare, hybrid warfare, conventional warfare, unrestricted warfare, among others. Specifically, for the purposes of this chapter, we refer to Clausewitz's definition of war, which is an act of violence to compel an opponent to do one's will.

In this context, there are also several approaches to classifying wars, such as that of evolutionary generations, which

> [...] seeks to frame war within a series of particularities that are repetitive, regardless of the place or region where the armed confrontation occurs, but which also allow us to observe distinctive elements from one generation to another. This theory is based on two variables: the first focuses on technology, understood as the means by which a particular war is fought; and the second variable is strategy, or, better put, the theory of war used in the armed confrontation. (Álvarez Calderón, 2017, p. 156)

Despite these approaches and the variety of definitions, the underlying problem is determining the most adaptive, flexible, and effective means to confront the

threats and dangerous situations that arise in these new wars. Here, SF, based on its unique capabilities, offers an important answer.

The SF of the Colombian National Army has proven to be a decisive capability within the strategy of the General Command of the Colombian Military Forces (CGFM). For Major General Carvajal, "the use of SF units has contributed to the fulfillment of the strategic objectives of the national security and defense policy" (Ejército Nacional de Colombia, 2017a, p. 14). The doctrine of SF in Colombia has been developed based on knowledge from other countries and on experience gained during the internal conflict. From this doctrinal perspective, "Special Operations are military actions conducted by organized, trained, equipped, and certified units with high mobility and flexibility in hostile, uncontrolled, and politically sensitive environments to achieve military objectives with strategic implications" (Ejército Nacional de Colombia, 2017a, p. 1-3).

For this reason, the objective of this chapter is to examine their critical capabilities and analyze which are best suited to addressing hybrid scenarios. As a working hypothesis, it is held that special warfare—specifically, unconventional warfare and foreign internal defense—offers the most and best insights in this regard.

The chapter is divided into four parts. The first defines SF capabilities to understand their value in a changing world of warfare and contemporary military operations. The second delves into the analysis of special warfare as not only a differential factor but also, in this case, a leading factor in addressing hybrid scenarios. The third section examines the tasks that, from the perspective of special warfare, encompass the widest range of options: unconventional warfare. The fourth section continues the study of foreign internal defense, as one of the tasks that comprises the special warfare capability ideal for confronting complex and hybrid environments. Finally, the chapter concludes by bringing together the most representative aspects of the study.

Delimiting the Capabilities of Special Forces: A Changing Universe

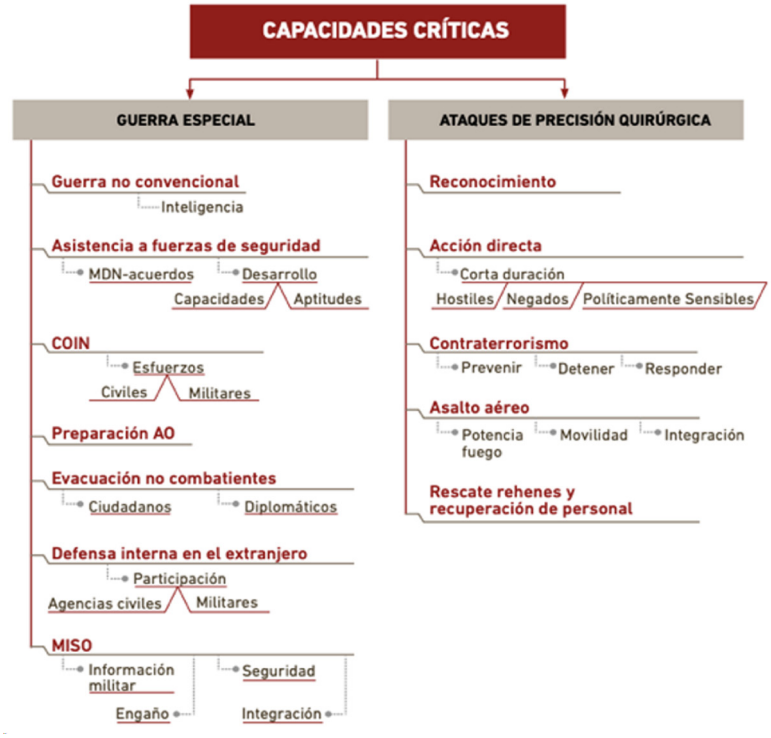
The Colombian National Army is a benchmark in the region for its ability to wage war across diverse operational environments. Particularly over the last two decades, it has taken the most important actions against irregular organizations operating in the country. In this regard, it is possible to affirm that "the government strategy" and "the actions of the Army, strengthened by Plan Colombia, tilted the counterinsurgency fight in favor of the State" (González & Betancourt, 2018, p. 18),

thereby successfully degrading the insurgents' operational and strategic center of gravity. In this process, it is essential to highlight the strategy the National Army has employed to transform its SF into a factor that empowers military operations throughout the country.

The concept of Unified Land Operations (ULO), adopted in 2015, paved the way for Special Operations (SO) to become, doctrinally speaking, one of the three distinctive competencies for decisive action (Rojas, 2017). Thus, the general concepts of SF were defined and embodied in the *Army Fundamental Manual MFE 3-05 Special Operations* (Ejército Nacional de Colombia, 2017a).

The starting framework for analyzing foreign internal defense operations is provided precisely by the *MFE 3-05*. It distinguishes SO from conventional operations because they are specifically conducted to meet the highest-level objectives outlined in the national military strategy (Figure 1). Due to their mission, SO can be developed through two critical capabilities that are clearly distinct from conventional forces—surgical strikes and special warfare, the central focus of this chapter.

Figure 1. *Critical Capabilities of Special Forces*



Source: Ejército Nacional de Colombia (2017c).

From a doctrinal perspective, special warfare comprises seven activities that imply "the ability to operate within a specific population, addressing sociocultural factors by understanding the culture of that population" (Ejército Nacional de Colombia, 2017b). However, the spectrum of special warfare remains extremely broad, and there are no regulations, manuals, or texts that specifically define unconventional warfare. This condition may have at least two explanations. First, the necessary operational emphasis on counterinsurgency tasks may have followed U.S. doctrinal guidelines—originating in British counterinsurgency—where the main effort lay in adapting conventional units rather than fully deploying SF. Second, by placing the concept of unconventional warfare within the spectrum of special warfare, it distances it from the more common tasks of surgical strikes.

Even the conceptual vagueness of unconventional warfare is present in doctrine. While it is true that the *MFRE 3-05* defines this type of operation as "activities conducted in a conflict environment, aimed at gathering intelligence to weaken the adversary's fighting capacity indirectly, through actions aimed at limiting its resources and critical capabilities" (Ejército Nacional de Colombia, 2017b, p. 1-14), this definition falls short of the reality and importance of unconventional warfare, especially in the conduct of hybrid warfare.

Unconventional warfare can be considered an art form, where "the negative space between war and peace is where actors are fighting modern wars in unconventional ways, such as activities in the cyber domain by the Anonymous hackers' collective" (Linnemann, 2016, p. 23). Linnemann's (2016) definition indeed considers a problem of great significance. The complexity of contemporary operational environments, coupled with a globalized society in which the domains of warfare are increasingly varied and interconnected, makes it difficult to define the operational environment for unconventional warfare—or, in other words, where the dividing line between conventional and unconventional warfare lies.

Therefore, there are multiple approaches to unconventional warfare operations—none of them comprehensive, of course—that nonetheless coincide in highlighting their characteristics for maximizing operational advantages within a hybrid environment. This strategic challenge is especially important for major powers, such as the United States, whose significant challenge, according to Linnemann (2016), is "to innovate, adapt, and adopt unconventional warfare through a broad strategic approach rather than sustaining its current view of a tactical capability for a niche mission" (p. 24).

In essence, unconventional warfare is a combination of direct and indirect applications of national power to achieve a strategic objective, and, due to its characteristics, requires special operationalization. "21st-century unconventional

warfare translates national strategy and policy into an operational concept, providing national policymakers with an appropriate and cost-effective strategic policy option" (Department of the Army, 2013, p. 23).

This is how the Commander of the U.S. Special Operations Command (USSOCOM) specifies that unconventional warfare is "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area" (Department of the Army, 2010, p. 14). Thus, the intent of efforts is "to exploit a hostile power's military, economic, and psychological vulnerabilities by developing and sustaining resistance forces to accomplish U.S. strategic objectives" (Department of the Army, 2010, p. 14).

It is important to emphasize that unconventional warfare has no direct conceptual or doctrinal relationship with military operations conducted abroad, or what are sometimes called *covert operations,* which are the subject of this chapter. Precisely because the concept is vague, unconventional warfare is not doctrinally limited to a specific set of actions; rather, it exploits the gray area to plan and execute the widest possible range of high-impact operations that transcend the limitations of conventional operations.

Thus, it is possible to propose that the conceptual difference lies in the fact that covert operations are another technique of unconventional warfare, or, to put it another way, unconventional warfare is the tactical concept, while covert operations are among the varied techniques used in its development.

Covert operations are usually relegated to the set of possible actions of Military Intelligence, especially when they are strategic-level operations carried out primarily abroad. Evidently, the conceptual limitation arises when covert operations are understood solely as the infiltration of a criminal organization, whereas the concept of *interference* decisively broadens the initial definition and takes it to the strategic level.

In this respect, interference actions carried out by a State cannot only be associated with the tools of strategic power—alongside area denial, deterrence, or compulsion—but also aim to influence security conditions, which could lead to a significant or extended military commitment, or in other words, to neutralize a threat (Rodríguez-Álvarez & Montero-Moncada, 2022).

However, given the evolving operational challenges, the conjunction between SF and Intelligence calls for a move beyond simple synergy toward a more ambitious fusion of capabilities. In this regard, U.S. and Russian fusion models propose that strategic operations in external environments yield much better results while maintaining simplicity and security, in a much more robust and effective manner than in the past (Montero et al., 2020).

Therefore, the scope of covert operations must be expanded to include a series of capabilities previously reserved solely for Intelligence. Clearly, at the doctrinal level, this presents at least two challenges: on the one hand, generating doctrine where none exists and, on the other hand, aligning two concepts that, although broad, differ: *covert operations* and *foreign military defense*. To achieve this, the best common analytical framework is the dyad of special warfare—as a critical capability—and unconventional warfare—as a task.

Special Warfare as a Critical Capability of SF

If we start from the assumption that a critical capability is "a means considered a crucial enabler for a center of gravity to work and is essential for the fulfillment of imposed or deduced objectives" (Ejército Nacional de Colombia, 2017b, p. 2-2), it can be stated that SO has two critical capabilities: special warfare and surgical strikes. Specifically, "special warfare is the conduct of activities that involve a combination of lethal and non-lethal actions carried out by troops with a broad understanding and comprehension of the operational environment" (Ejército Nacional de Colombia, 2017b, p. 2-2).

In national doctrinal construction, special warfare capabilities comprise the following distinctive types of operations: "unconventional warfare, assistance to security forces, counterinsurgency, preparation of the operational environment, evacuation of non-combatants, foreign internal defense, support for information operations, and civil affairs" (Ejército Nacional de Colombia, 2017b, p. 2-3).

Its strategic importance within the context of SO stems from its role in projecting SF into the new scenario of hybrid warfare, a clearly Western concept that encompasses many contemporary conflicts and finds comparable definitions in Russia—as non-linear warfare—and in China—as unrestricted warfare. This war can be defined as the "natural product of the adaptation of irregular and asymmetric warfare aimed at exploiting the vulnerabilities of regular forces" (Colom, 2018, p. 38) or, in the context of unrestricted warfare, as "a combined war that transcends the main areas and methods of military and non-military affairs, where all dimensions that influence national security must be included" (Ejército de Chile, 2013, p. 4). This way, the aim is to achieve a political objective through violence.

In other words, in the context of hybrid warfare, unconventional warfare—as part of the critical capability of special warfare—plays a very important role. Thus, it is essential to understand the definition of hybrid warfare:

> Hybrid warfare is a sophisticated form of warfare characteristic of the Information Age that, leveraging the possibilities offered by globalization and free access to advanced technologies, combines conventional and irregular actions at all levels and phases of an operation. (Colom, 2012, p. 82).

A third definition that illustrates the close relationship between special warfare and hybrid warfare capabilities is "the use of various instruments of power to target a specific social actor. Employing these tools of power becomes an attack aimed at identifying different vulnerabilities to produce various effects" (Equilibrium Global, 2020, para. 4). Because of the diffuse nature of confronting the power of the hybrid adversary, unconventional warfare and foreign internal defense are central. They enable the State to operate in the elusive terrain of proactivity instead of being confined to a permanent reactive stance.

Special warfare—and the tasks that comprise it—thus acquires prominence. For the United States Army, "the two primary missions of SF are unconventional warfare and foreign internal defense" (Department of the Army, 2014, p. 14). The choice of this path is based on the fact that these are the most powerful tools for containing first asymmetric enemies—adaptive, flexible, and diffuse—and then, hybrid enemies—a confluence of conventional power and unattributable, but highly destabilizing, means. At this point, unconventional warfare, in which special operators fully leverage their flexibility and adaptability to operate in diffuse environments, and foreign internal defense, with its preventive nature and its focus on keeping threats as far from the country as possible, become important.

Given that the concept of hybrid warfare is the most widespread format of contemporary warfare (Montero, 2022), it is essential that armies, starting with the Colombian one, conduct a thorough analysis of their capabilities—within the framework of special warfare—regarding the development of tactics, techniques, and procedures that allow the Colombian SF to ensure victory in a conflict without even firing a bullet.

Likewise, the various ways special warfare can be applied against any adversary must be analyzed, recognizing that the hybrid warfare operational environment is highly variable. Special warfare, developed through unconventional warfare and military defense abroad, is an extremely important military component of the government's national strategy in 21st-century conflicts, which is why its concepts, scope, and implications must be clear.

Unconventional Warfare as a Driving Force of Special Warfare

Unconventional warfare is the main force behind special warfare. This relationship works because SO must keep innovating as threats change quickly. This fast pace of change requires regularly updated tactics, techniques, and procedures to prevent the enemy from gaining any advantage.

Unconventional warfare has become a decisive tool in shaping the battlefield. Of course, it is not limited to this action, though it is important to answer the following seemingly tautological question: Is unconventional warfare the State's response to 21st-century conflicts?

And the answer is probably yes. It can be argued that unconventional warfare capabilities have been employed, directly or indirectly, across generations of warfare. Suffice it to mention, for example, the operations carried out by the British Special Air Service (SAS) and the French Resistance during World War II, or the missions carried out by the U.S. SF in Afghanistan after the September 11 attacks.

Unconventional warfare has several characteristics that make it a flexible technique, capable of being used across different operational environments without restricting it to a single situation. That is why it is so effective in gray, diffuse, asymmetric, or hybrid environments. As mentioned earlier, Colombian doctrine defines unconventional warfare as those "activities conducted in a conflict environment, aimed at gathering intelligence to weaken the adversary's fighting capacity" (Ejército Nacional de Colombia, 2017b, p. 21). This aligns with the proposal discussed in the first section, working alongside Intelligence without being its exclusive focus.

Now, from the perspective of the U.S. Army—which more closely aligns the SF with military intelligence—unconventional warfare is not limited to intelligence-gathering activities but encompasses a range of actions that shape the operational environment, facilitating future military operations structured around national strategy.

According to Appendix "A" of the U.S. Army's *ATP 3-05.1 Unconventional Warfare* (Department of the Army, 2013), the U.S. Army's SF has 17 specific unconventional warfare missions, including "locating and recovering personnel and equipment in and from the joint special operations area, and ensuring or coordinating joint combat." As this definition demonstrates, in some States unconventional warfare is used to go beyond intelligence-related missions and, conversely, to deploy these capabilities for offensive, defensive, and stability tasks.

In the Colombian case, although a defined doctrinal structure exists, not all of the Army Field Manuals (MCE) have yet been developed, nor have the Army Technique Manuals (MTE), which has affected the doctrinal development of the SF's critical capabilities.

The first step in establishing or validating unconventional warfare as a core component of critical special warfare capabilities is to define the field and develop the technique manuals aligned with the tasks performed by the SF. Another crucial factor is the High Command's willingness to credibly develop this capability, accepting the strategic risks involved. Unconventional warfare demands highly trained, carefully selected, fully equipped, and morally resilient personnel, since this mission, unlike others, must be executed with a very low profile and always under the authorization and guidance of a nation's highest decision-making authority.

Perhaps one of the biggest challenges in personnel selection is not just understanding foreign operational environments but also the closeness or distance of the special operator to different cultural patterns. In a hyperconnected world where transnational threats mirror the diffuse nature of hybrid threats, soldiers need the ability to operate in foreign languages, understand and internalize cultural norms that are completely different from their own, and have a much greater capacity for mimicry than ever before. This need has increased due to cultural hyperconnectivity and the very high levels of media exposure and databases that could be leaked to adversary governments, agents, or structures.

The process of target selection and prioritization is also a very sensitive issue in unconventional warfare. This process requires walking a fine line, given the blurred boundaries of what constitutes a legitimate military target. Therefore, it demands high-level, exceptional intelligence capabilities to select targets for destruction, sabotage, or neutralization behind enemy lines that do not directly impact civilians but are within the scope of an adversary operating in a gray zone across multiple dimensions.

Given the elements presented in this analysis, it is imperative to reconfigure the doctrinal concept of unconventional warfare in accordance with Colombian doctrine. This should not be limited to intelligence-gathering tasks but, following the U.S. model, be applicable across a broad spectrum, hybrid in nature, and grounded in an understanding of the multidimensionality of present and future threats.

As a preliminary conclusion, it is important to emphasize that operations conducted within the scope of unconventional warfare could be an effective response, at least in theory, to hybrid threats, which cannot be countered with traditional methods, since they involve a "diverse and dynamic combination of conventional

forces, irregular forces, terrorist groups, and criminal elements unified to achieve mutually beneficial effects" (Ejército Nacional de Colombia, 2017c). Perhaps the hybrid threat calls for a hybrid response from the State, where unconventional warfare stands out as the versatile warfare method offering the greatest flexibility in its tactics, objectives, and resources to address this type of threat.

Foreign Internal Defense as a National Security Strategy

Within the spectrum of special warfare, foreign internal defense becomes the ideal complement to combat in hybrid environments.

To begin with, it must be recognized that national security "is the national effort to prevent terrorist attacks, reduce vulnerabilities to them, and respond to natural disasters and other emergencies" (Ejército Nacional de Colombia, 2017c, p. 4-21). Therefore, national security should be viewed as a component of national security policy, which demands genuinely unified action, defined as "the synchronization and/or integration of activities of state and non-state actors with military operations to achieve unity of effort" (Ejército Nacional de Colombia, 2017c, p. 12). Without this coordination, developing a national security strategy becomes very difficult, since, as mentioned earlier, security involves not only the security forces but also political authorities and other stakeholders.

In border areas, unified action should not be limited to internal coordination; if the situation allows, it can be further improved through cooperation with friendly countries. To conduct military operations with other nations, certain conditions must first be met, such as standardizing military procedures among States and, of course, securing the political will to implement these measures. As mentioned, it is important to highlight that, due to their complexity and impact, the development and use of critical capabilities and distinctive operations of the SF must be authorized by the Commander and Chief of the Armed Forces, who, in the Colombian context, is the President of the Republic, as outlined by the Constitution in Article 189: "To lead and use security forces as the supreme commander of the Colombian Armed Forces" (Constitución Política de Colombia, 1991).

As part of special warfare capabilities, foreign internal defense multiplies unified internal action abroad; in other words, this type of SO consists of defending the interior from abroad. This concept should not be confused with other related

concepts such as *intervention, interference,* or *instability operations,* which—especially the latter—are controversial and have a very limited conceptualization. Specifically, foreign internal defense is the "participation of a government's civilian and military agencies in any of the action programs adopted by another government, with the purpose of protecting its society from subversion, anarchy, insurgency, terrorism, and other threats" (Ejército Nacional de Colombia, 2018, p. 1-6). Analyzing this definition, it can be concluded that foreign internal defense is a unified action coordinated and executed with the participation of organizations from other countries to protect the nation's interior.

The above statement refers exclusively to the doctrine of the Colombian National Army's SF. Therefore, it is important to highlight that, in other countries, foreign internal defense is not limited to SF units but rather has a global focus and involves the interaction of multinational efforts and joint operations among armed forces, governmental, and non-governmental agencies. "Army efforts, in general, include special operations forces units, particularly Civil Affairs, military information support operations, and Special Forces" (Department of the Army, 2015, p. 2-31).

It should be noted that, unlike Colombian doctrine, the U.S. Army doctrine includes Military Information Support Operations (MISO) and Civil Affairs (CA) units within the organizational structure of SO units. In Colombia, these types of units are not part of the SF organizational structure, specifically speaking (Table 1).

Table 1. *Tasks and Subtasks of Foreign Internal Defense*

Foreign internal defense (FID)	Tasks	Subtasks
Participation of civil and military agencies of a government in any of the programs of action adopted by another government or other designated organization to free and protect its society from subversion, anarchy, insurgency, terrorism, and other threats to its security (*MFRE 3-0*)	Indirect support	- Security cooperation - Assistance to security forces - Joint and/or multinational exercises - Exchange programs
	Direct support without combat operations	- Civil Affairs (CA) - Military information support operations (MISO) - Military training support - Logistics support
	Direct support with combat operations	- (APQ) Temporary solution, presidential decision

Source: Ejército Nacional de Colombia (2017c).

The development of foreign internal defense is a key element for national security, as these types of SF operations allow the government to design a

multidimensional national security strategy. This strategy is executed through military tools with SF capabilities, which, in conjunction with strong diplomatic relations, especially with neighboring countries, can enable unified action that integrates the military and civilian capabilities of both allied nations.

In U.S. doctrine, foreign internal defense is approached in line with its political and military capabilities, and, clearly, its status as a major power. Recent campaigns, such as those in Afghanistan and Iraq, have expanded the discussion of the forms, methods, tactics, and techniques used with this tool. Therefore, it can be argued that the shared experiences of the Special Operations Forces in Iraq and Afghanistan were beneficial. However, the joint command and even the SF command must consider the complexity of balancing short-term objectives with tasks aimed at achieving long-term solutions in the global counterterrorism effort. In these long-term strategies, the SF provides States with strategic and operational options that only they have, through special reconnaissance and direct action in support of Joint Task Forces. Thus, foreign internal defense activities are the most effective means of producing results against transnational terrorist structures and their host States (Liller, 2005).

In this regard, the *JP 3-22 Foreign Internal Defense (FID),* which addresses the issue from a doctrinal perspective, states that

> […] While FID is one of the designated core special operations activities of the United States Special Operations Command (USSOCOM) and its subordinate commands, FID may receive support from the Joint Force, Multinational Forces (MNF), and other USG departments and agencies. (Joint Chiefs of Staff [JCS], 2021, p. 14)

What is relevant is that, by its nature, the United States does not define foreign internal defense as a primarily military operation. Instead, it proposes that it typically includes an interorganizational approach to support the security, stability, and development of a State. Foreign internal defense requires a whole-of-government focus on achieving and leveraging unified action by all participants through practices such as interoperability, integration, and interdependence (JCS, 2021).

U.S. doctrine is emphatic in this regard, defining characteristics of foreign internal defense that highlight the need for a much broader vision than usual. Specifically, the United States establishes that foreign internal defense (JCS, 2021):

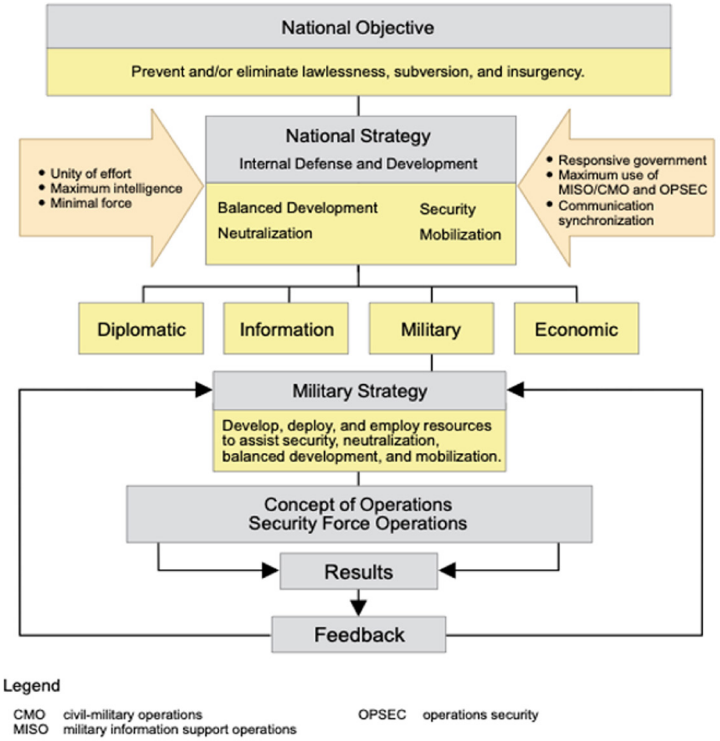
- involves all instruments of national power.
- can occur across the full range of military operations.
- is carried out by both conventional forces and Special Operations Forces.

- supports and influences the host nation's development and internal defense program.
- includes training, material, technical and organizational assistance, advisory services, infrastructure development, and tactical operations.
- has preferred methods of support such as assistance and development programs.

These characteristics allow us to see two elements. First, it requires a concerted, interoperable effort to conduct foreign internal defense. Second, the Range of Military Operations (RMO) is a complementary tool to unconventional warfare in the difficult context of hybrid warfare. Therefore, its military application is not exclusive but essential to the SF.

In its execution, and as shown in Figure 2, the structural nature of foreign internal defense is also evident. U.S. doctrine involves a wide range of actors and processes, ensuring that actions are sustainable and decisive.

Figure 2. *Internal Defense and Development Strategy Model*



Source: JCS (2021).

There is no doubt that, due to its nature, the United States' approach to foreign internal defense differs from Colombia's. However, it is possible to draw parallels in terms of how it complements unconventional warfare and the need to see it as a tool that involves most agencies to expand its reach and ensure coordinated impact.

In conclusion, foreign internal defense enables Colombia, through the SF, to project military capabilities to enhance and secure national security, as well as to build international relations with allied countries, with whom these types of operations would eventually be carried out. It is precisely because of this feature that foreign internal defense sets itself apart from other operations involving critical special warfare capabilities: the direct or indirect participation of another country within a comprehensive security approach, acknowledging that when regional security is maintained, national security is also strengthened.

Conclusions

In extremely changing and dynamic environments such as hybrid wars, equally changing, dynamic, adaptive, and flexible military components are required. This is why SF becomes the most valuable strategic tool in these operational theaters.

Beyond surgical strike capabilities, the answers to hybrid challenges lie in special warfare. Although unconventional warfare and foreign internal defense are complementary tasks within special warfare, their definitions and approaches must be reviewed to ensure coordination and full implementation.

First, a unity of effort—the product of successful unified action—is essential to prevent crises and defeat credible threats. Second, the construction of a new intelligence framework is fundamental, such that its optimized use requires that all operations be based on reliable, accurate, relevant, and timely intelligence, and that this intelligence be fused with SF in time, manner, and place.

Third, a synchronized use of MISO with other operational activities is required, as this can enhance the legitimacy of the SF involved in the action.

Finally, synergy must be fostered not only with the political leadership but also with the strategic and operational command. This organization must provide centralized planning and direction, support the decentralized execution of the plan, and be structured and authorized to coordinate and lead unconventional warfare and foreign internal defense efforts. Therefore, the doctrinal challenge in Colombia remains unresolved, and the necessity to develop the doctrine is evident.

References

Álvarez Calderón, C. E. (Ed.). (2017). *Escenarios y desafíos de la seguridad multidimensional en Colombia.* Sello Editorial ESDEG. https://doi.org/10.25062/9789585652835

Colom, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova, 10*(10), 77–90. https://doi.org/10.21830/19006586.228

Colom, G. (2018). Guerras híbridas: cuando el contexto lo es todo. *Revista Ejército,* (927), 38–44. https://tinyurl.com/4tk6b55d

Department of the Army. (2010). *Training Circular TC 18-01 Special Forces Unconventional Warfare.* https://tinyurl.com/49ez2xf4

Department of the Army. (2013). *Army Techniques Publication ATP 3-05.1 Unconventional Warfare.*

Department of the Army. (2014). *Field Manual FM 3-18 Special Forces Operations.* https://tinyurl.com/yn6h6atz

Department of the Army. (2015). *Army Techniques Publication ATP 3-05.2 Foreign Internal Defense.* https://tinyurl.com/ym23fyjx

Ejército de Chile. (2013). *Memorial del Ejército de Chile.* Departamento Comunicacional del Ejército. https://tinyurl.com/5d7nsukd

Ejército Nacional de Colombia. (2017a). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Public].* Imprenta Militar del Ejército. https://tinyurl.com/2p8b7nse

Ejército Nacional de Colombia. (2017b). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Public].* Imprenta Militar del Ejército. https://tinyurl.com/2p8b7nse

Ejército Nacional de Colombia. (2017c). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones [Public].* Imprenta Ejército. https://tinyurl.com/ducm7tje

Ejército Nacional de Colombia. (2018). *Manual de Campaña del Ejército MCE 3-18 Operaciones de Fuerzas Especiales [Restricted].* Imprenta Ejército.

Equilibrium Global. (2020, November 21). *Entendiendo la guerra híbrida en la práctica.* https://tinyurl.com/yjbzx836

González, M. A., & Betancourt, M. A. (2018). La transformación del Ejército Nacional de Colombia: una interpretación teórica. *Revista Latinoamericana de Estudios de Seguridad,* (22), 70–84. http://dx.doi.org/10.17141/urvio.22.2018.3093

Joint Chiefs of Staff [JCS]. (2021). *Foreign Internal Defense* [Joint Publication, No. 3-22]. https://tinyurl.com/bdf5bje8

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

Liller, O. K. (2005). *Special Operations Forces and Foreign Internal Defense: An effective counterterrorism method* [Capstone, Naval War College]. Repositorio DTIC. https://tinyurl.com/44tuxjax

Montero, L. A. (2022, March 7). Guerras híbridas: la naturaleza cambiante de la guerra [Video]. *YouTube*. https://www.youtube.com/watch?v=ZNYiBeEla_I&t=32s

Montero, L. A., Niño, J. A., Ríos, J. A., Orduz, A. L., & Yasno, J. A. (2020). El oso vuelve al combate: el tridente estratégico para operaciones encubiertas e híbridas en Rusia. In M. A. González-Martínez & L. A. Montero-Moncada (Eds.), *El tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder cíber en el siglo XXI* (pp. 43–62). Sello Editorial ESDEG. https://doi.org/10.25062/9789584288943.02

Rodríguez-Álvarez, F., & Montero-Moncada, A. (2022). Operaciones de interferencia en ciberseguridad y ciberdefensa: herramienta estratégica para la supervivencia de los Estados. In L. A. Montero-Moncada (Ed.), *Poder y estrategia: Elementos para la supervivencia del Estado* (pp. 227–301). Sello Editorial ESDEG. https://doi.org/10.25062/9786289530483.09

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

Chapter 7

Cyber Support for Colombian Army Special Forces in a Tactical Environment*

DOI: https://doi.org/10.25062/9786287818408.07

Juan Guillermo Cruz Segura
Ricardo Di Genaro
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Cyber operations offer governments an additional capability in their quest to impact their adversaries without resorting to conventional weapons. Fifth-generation warfare is the ideal setting for these operations. The objective of this chapter is to identify how the National Army's Special Forces could employ these capabilities to achieve tactical and strategic objectives, given that these units are the country's strategic bastion and that their targets are of high strategic value. The current doctrine of the Colombian military forces and the National Army is used to address this topic. This approach, along with some global tactical cases, helps us assess the importance and scope of this type of operation.

Keywords: Special Forces; fifth-generation warfare; hybrid warfare; hardware; cyber operations; special operations; software.

* 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.

Juan Guillermo Cruz Segura
Lieutenant Colonel in the Colombian National Army. Master's student in Strategy and Geopolitics, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Leadership and Management of Military Units and in Military Resources Administration for National Defense, Arms and Services College, Colombia. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: **juan.cruzse@buzonejercito.mil.co**

Ricardo Di Genaro
Major in the Argentine Army. Master's student in International Relations, Universidad de Belgrano. Specialization in Leadership of Land Military Organizations, Escuela Superior de Guerra "General Luis María Campos," Argentina. Diploma in Economic Intelligence for Defense, Universidad Bernardo O'Higgins, Chile. Diploma in University Teaching and Pedagogical Learning Tools, Escuela Naval de Cadetes "Almirante Padilla," Colombia. Bachelor's in Administration, Colegio Militar de la Nación, Argentina. Email: **rdigenaro@ejercito.mil.ar**

APA Citation: Cruz Segura, J. G., & Di Genaro, R. (2025). Cyber Support for Colombian Army Special Forces in a Tactical Environment. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare (pp. 147-170). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.07

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

According to the National Army Doctrine Center (CEDOC), doctrine is the set of fundamental principles, along with their corresponding tactics, techniques, procedures, terms, and symbols, that, when used together, enable the conduct of operations. Through these principles, the combat Army and the force-generating Army elements that directly support operations guide their actions in accordance with national objectives. Furthermore, doctrine can be understood as a guide on how (not what) to think, prepare, and execute essential parts of the operations and training process. Consequently, it can be said that doctrine adapts to the particular circumstances at the time of its application and is rarely mandatory (Salazar, 2020).

Despite this conceptual clarity, the Special Forces (SF) of the Colombian National Army lack a specific doctrinal basis for employing their capabilities in cyber operations in a tactical environment. At a higher level, one finds that the Army Command General Staff establishes the organization's operational doctrine, specifically in the *Army Field Manual MCE 3-12, Cyberspace Operations,* a restricted document. One level higher, within the General Command of the Military Forces (CGFM), there is currently a Joint Cyber Operations Command, whose mission is to plan, coordinate, integrate, and conduct military operations in cyberspace to defend national interests and critical national cyber infrastructure, in order to contribute to the fulfillment of the CGFM's mission (Comando Conjunto Cibernético [CCOCI], 2020).

It should be noted that a joint command is understood as a "unified or specific command with a broad and continuous mission, designated from the strategic level" (CGFM, 2018). In this regard, the primary roles and functions of the Joint Cyber Operations Command are to advise the President of the Republic, the Minister of Defense, and the High Council of National Defense on military matters, as well as to prepare and define plans to develop national security policies, among many others.

Despite the above, the lack of information and doctrine in the SF underscores the institution's knowledge gaps. When training levels are reduced, this shortcoming results in the loss of a capability that could be employed by the SF and in their roles within the tactical environment. Precisely, the objective of this chapter is to provide input that will help SF units develop cyber support capabilities or use them directly in a mission. To this end, a prospective analysis is made of the opportunities, advantages, and shortcomings that could arise from this type of military capabilities, with the understanding that this combination has a significant impact on the spectrum of hybrid warfare that Colombia experiences daily, a context in which a variety of criminal and unstable phenomena affect public order.

In this regard, analyzing existing doctrine constitutes a contribution to the nascent academic literature, which has addressed this topic only briefly. Thus, this chapter contributes to institutional efforts to continue methodical research on Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) (Ejército Nacional de Colombia, 2017) to measure the current state of a given military capability or unit.

As mentioned, academic research has not studied how the Colombian Army's Special Operations (SO) units, located within the Joint Special Operations Command—which governs the doctrine and employment of these types of units—can employ cyber capabilities, either as direct support for operations or as organic units within the specialties of the SF, in the tactical environment. The latter is understood as tactical action, battles, encounters, or combats that employ lethal and non-lethal actions designed for a specific purpose in relation to the enemy, the terrain, friendly forces, or other entities (Ejército Nacional de Colombia, 2017b).

For this reason, this work addresses topics not described in the National Army's SF doctrine, with the purpose of supporting the theories, techniques, and tactics required by this unit to execute cyber operations in support of the nation's strategic objectives. Specifically, it seeks to fill gaps in the operational and tactical scope of cyber operations within the SF, identify their weaknesses, assess the potential for the use and organization of this new specialty within special units, and, more importantly, explain how to apply them in the field of hybrid warfare in Colombia.

Doctrinal Relationship

Historically, humanity has been involved in various events in which two or more parties seek to impose their will by physical force or violence; this is precisely the

general definition of war. Over the years, this meaning has remained the same, but war, in its nature, has evolved in different ways. Today, we speak of hybrid warfare, a term coined in 2007 by Frank Hoffman (2007)[1] to refer to the confluence of conventional military modes and strategies of warfare, linked with terrorist tactics that encompass violence and criminal disorder (Azabal, 2021).

Cyberwarfare is among these types of wars, in which combat is carried out across multiple fronts. In recent years, one of the areas where technologies and the development of ICTs have gained strength, both in the civilian and military spheres, is cyberspace, understood as the non-physical environment created by computer equipment linked to interoperate in a network (EcuRed, 2012).

This virtual world has become a strength, an advantage, and a capability for the world's armed forces. In this context, the Colombian Military Forces have adapted to the challenges posed by globalization and technological advancements, creating doctrines and organizations capable of defending the nation in this scenario, including offensive operations and attacks to neutralize any hostile intent.

Another striking concept in the field of cybernetics is cyberwarfare, which can be understood as aggression by one State against another with the intent to achieve a strategic objective. In essence, cyberwarfare seeks to seriously damage the opponent's capabilities, forcing them to accept a specific objective or, simply, to steal or rob them of essential information that can be used later, cut off or destroy their communication systems, or alter their databases.

In other words, the concept encompasses what has traditionally been understood as war, but with the difference that the means employed is not physical violence, but rather a cyberattack (through systems and networks) that allows for an advantage over the enemy, gaining superiority, or even overthrowing them (Sánchez, 2009). In a cyberwar scenario, various operations are carried out, including exploitation—obtaining information from recipients; deception—manipulating the collected information; destruction—rendering the target inoperable; and, finally, disruption—rendering the target inoperable without destroying it.

One cannot talk about cyberwarfare without understanding the concept of cyberterrorism. This term refers to the convergence of cyberspace and terrorism, that is, the way in which terrorism uses and employs constantly evolving information technologies to intimidate, coerce, or harm specific social groups for political and religious purposes. Therefore, cyberterrorism is a new form of combat

[1] Lieutenant colonel in the United States Army Reserve, serving as a researcher at the National Defense University (Department of Defense).

in which terrorism replaces weapons, bombs, and missiles with computers and other IT elements to plan and execute offensive and defensive attacks that cause the greatest possible damage to the civilian population (Sánchez, 2009).

Information operations, for their part, are understood as activities that integrate the use of electronic warfare capabilities, computer network operations, military information support operations, military deception, and security operations to create conditions for success and prevail in the military information environment (Ejército Nacional de Colombia, 2017a). These are part of the large chain of operational possibilities that the SF can support in the cyberspace spectrum. Specifically, Colombian doctrine defines information operations as all electronic activities that could support a battle.

Information operations aim to affect the decision-making cycle of the adversary's leaders and protect their own by implementing actions across and targeting different domains. Operations executed in the physical domain seek to attack or defend the physical infrastructure associated with command and control, as well as the decision-making of commanders at all levels. In this scenario, typical targets are communications networks, sensors, search engines, and the commanders themselves, among others susceptible to traditional kinesthetic means (which employ movement by fire).

In the cognitive or knowledge domain, operations are executed to affect decision-makers' perceptions across different battlefields. In this case, the typical instrument for conducting psychological operations is military deception, although it can also be considered part of these (Ejército Nacional de Colombia, 2021). The goal of this type of attack is to create chaos in leaders' decision-making at different levels, so that tactical and strategic precision fails in pursuit of their objectives.

When discussing cyber operations, one cannot ignore the concept or term of fifth-generation operations, also known as *unlimited warfare*. Defined and introduced in 2009 as a strategic operational concept in the interventions of the United States and the North Atlantic Treaty Organization (NATO), fifth-generation warfare determines that it is not about winning or losing, but rather demolishing or destroying the enemy's intellectual strength, forcing them to seek a compromise by any means, even without the use of conventional weapons. In other words, it involves directly manipulating human perception by targeting the brain, specifically its neurological components—binaural waves and magnetite crystals—and the methods for manipulating them (Aharonian, 2018). In the current context, characterized by the enormous influence of social media and the media on a

State's decisions and paths, these actions are an important tool for both defense and offense, so it is essential to be very clear about this concept.

As can be inferred, technology, understood as the set of industrial instruments and procedures for a specific sector or product (Real Academia Española, 2022), plays an important role in fifth-generation warfare. Specifically, in this study, technology refers to elements such as computers, networks, software, and hardware that a military force employs to defend its information, thereby avoiding conflicts in decision-making that are crucial to the development of military operations.

A keyword within the current trend of technology and cyberwarfare is the internet. This concept, coined in the 1980s, was defined as "a network of computer networks capable of communicating with each other. It is nothing more. However, this technology is much more than a technology. It is a means of communication, interaction, and social organization" (Castells, 2000, p. 9). Currently, the internet is the key to connecting information across distances in real time, enabling the fluidity of data across various fields.

Obviously, military organizations cannot ignore this concept, since one of the essential functions of warfighting—directing strategy and tactics—is command and control. Command and control is exercised through communications media, including the internet, to convey the commander's intentions and the military objective to be achieved. For this reason, cyber defenses in this field of action are vital to prevent attacks that could compromise national security and sovereignty. This was the case on July 11, 2021, when Colombian media revealed details of the largest hacking attack against the Colombian Military Forces by the Venezuelan government. The journalistic investigation indicated that the intelligence of that country, from six different points in Venezuelan territory, had deliberately attacked the CGFM servers in Bogotá for months (BLU Radio Editorial, 2021).

Another important aspect to consider is social media. Without a doubt, one of the great social and technological revolutions resulting from the widespread use of the internet is the network of people connecting across the globe. The way we interact with others has shifted from in-person to online. Social media serves as digital meeting points where it is possible to access all kinds of information, share impressions, and check files and resources in real time, at speeds never before imagined, as is the case with Facebook, Hi5, Twitter (now X), MySpace, etc. Nevertheless, even more useful than simply exchanging photos, videos, or messages is the creation of other types of social networks: those aimed at supporting and disseminating various topics (Ledo, 2011).

An example of this was the 2016 United States presidential election, in which Donald Trump was elected. On that occasion, the Russian Federation exerted media influence through social media to ensure its preferred candidate reached the White House, thereby allowing it to pursue its strategic objectives. The newspaper *La Vanguardia* reported that this Russian campaign targeted African American users as part of its tactics to favor the vote of the Republican candidate, the then-president, Donald Trump. These are some of the conclusions reached in a detailed report prepared for the Senate Intelligence Committee, a draft of which was obtained by *The New York Times* (La Vanguardia, 2018).

Finally, another key aspect is the human factor. As military history has shown across generations of warfare, the combatant is one of the factors in its development. Any military force that has qualified personnel within its ranks to plan, conduct, and execute military operations will facilitate the achievement of its objectives. Of course, this is also true of cyber operations. Having military personnel specialized in cybersecurity is important, as these professionals monitor, analyze, detect, and respond to unauthorized activity in the space domain (Today's Military, 2022).

Nonetheless, it is important that personnel comprising operational-level staffs and commanders, who are ultimately the decision-makers, also have knowledge of cyber operations. During the planning and performance of the campaign, both defensive measures to protect one's own systems and offensive measures to affect critical infrastructure systems and enemy weapons systems through the use of cyber weapons must be taken.

In this regard, it is also important to highlight that the personnel responsible for physically inserting a device to infect a closed network of an enemy system must undergo rigorous training. For instance, in 2010, the Stuxnet computer worm—a "cyber-missile" of unknown origin—was used to sabotage Iranian nuclear facilities. This virus affected nuclear fuel-refining centrifuges, hampering the production of military-grade uranium. It should be noted that the Iranian nuclear program is a closed system, so the operation required privileged access to its computer systems. In this respect, the human factor was a key factor in obtaining the information that enabled the development of the computer worm. Put differently, unlike other viruses that can navigate through multiple networks to reach their target, Stuxnet infected its target through a removable device inserted by an individual, either accidentally or intentionally, since the only way to access the Iranian nuclear network was through physical access to the computers within it (Fink, 2014).

In conclusion, in modern combat, it is necessary to have qualified military personnel capable of physically infiltrating critical enemy infrastructure, obtaining information from closed enemy computer networks, or physically inserting computer programs like a "cyberspace missile" to inflict damage on their networks, affect their cyberspace, and ultimately cause material damage.

In the specific case at hand, it should be emphasized that the SF must have qualified cyber personnel to support the command's cyber operations, which they depend on. It must also rely on support for cyber operations to acquire the capacity to carry out its specific operations, such as neutralizing the security system of a military facility to infiltrate and sabotage it.

Characterization of Cyber Operations

As mentioned in the previous section, the final domain used in current and future wars—the fifth domain—is cyberspace. Specifically, cyberspace is a global domain within the information environment consisting of interdependent networks of information technology infrastructure and contained data, including the internet, telecommunications, networks, computer systems, and integrated processors and controllers (Ejército Nacional de Colombia, 2021).

In the current accelerated technological evolution, control of this global domain is vitally important, given its significance to any nation. National strategic objectives such as information, finance, transportation systems, military forces, strategic intelligence, health, education, and the economy all carry out their activities in virtual environments, which are conducive to the enemy, knowledgeable in cyberspace, being able to affect procedures in each of these strategic areas and put the nation in check. For this reason, this topic of study is a priority for the National Government and the agencies responsible for the defense and security of the Colombian State.

In this context, the analysis of operational variables by cybersecurity experts requires an in-depth study of the following elements: the political environment, in which the networks and nodes that require greater emphasis for the operation of the Force are established; the economic environment, that is, which networks and nodes are required to enable the nation's trade and economy; the military environment, where the nodes and networks through which the enemy operates are located; the social environment, in which the communication networks used by the country's population are analyzed to provide information and protect them from negative effects; the information environment, where the nature of the information in transit

that affects military operations is verified; the time environment, which determines the optimal times to support operations; the infrastructure environment, which seeks to understand which networks and nodes enable the functioning of critical infrastructure, the key capabilities of resources, and data control; and finally, the physical environment, which seeks to analyze how wireless networks are affected by the effects of climate and terrain (Ejército Nacional de Colombia, 2017b).

The analytical study of a specialized general staff in the cyberspace environment allows operational commanders to make better decisions when intervention is required, whether in defense or offensive action, in the fifth domain. Furthermore, analyzing the mission variables (METT-TC)—mission, enemy, terrain, troops, time, and civil considerations—with an emphasis on available troops allows for defining the type of units required, precisely the topic addressed in this chapter.

To better characterize cyber operations, it is important to understand what they are and which are used in Colombia. Specifically, cyber operations are the set of military operations that take place in or through cyberspace, that is, those that are planned and executed with and through the use of cyber resources. Their goal is to ensure the nation's security and defense, and to reduce or neutralize enemy actions to gain operational advantage and appropriately use one's military power (CGFM, 2016).

Cybersecurity operations contribute substantially to protecting and ensuring the functioning of the military's critical cyber infrastructure and the national critical infrastructure. This critical infrastructure encompasses thirteen sectors: 1) government; 2) security and defense; 3) information and communications technologies; 4) electricity; 5) finance; 6) education; 7) mining and energy resources; 8) industry, commerce, and tourism; 9) the environment; 10) health and social protection; 11) water; 12) transportation; and, finally, 13) food and agriculture.

A State's critical infrastructure comprises physical or virtual systems that facilitate essential functions and services supporting the most basic social, economic, environmental, military, and political systems. An impact, weakening, or slowdown in its functioning due to natural (e.g., a flood that affects the electricity supply) or man-made (e.g., a terrorist attack or a cyberattack on a nuclear power plant or a financial institution) causes could have serious long- and short-term consequences (Instituto de Seguridad y Bienestar Laboral, 2023).

Therefore, it is vitally important for any State to have a specialized military apparatus, up to date and trained in all types of cyber operations. The various external and internal threats, both legal and illegal, that have emerged in the current

international system following the September 11 attacks in the United States—which changed the way wars were viewed—make addressing these types of wars a priority.

Cybersecurity operations include defensive measures that protect and enable the cyber component to adapt to adverse situations. These, in turn, comprise prevention, analysis, and assurance operations (CGFM, 2016). These, as will be seen in the case study, aim to prevent cyber attacks through campaigns, training, analysis, planning, and monitoring of systems.

Another type of cybersecurity operation is cyber incident management, whose main objective is to restore the functioning of cyber systems and minimize negative impacts following a cyber attack. These operations aim to ensure the timely provision of essential services to society.

The third and final type of cybersecurity operation is protecting critical cyber infrastructure. This type of operation seeks to preserve the normal functioning of critical cyber infrastructure so that it can continue to provide essential services to the population and guarantee the country's governability (CGFM, 2016).

To conclude the topic of cybersecurity operations, another type of operation involving cyber is discussed below. Specifically, cyber defense operations are proactive actions; that is, they aim to prevent, detect, and counter threats that threaten the functioning of the Armed Forces and the national order. This category includes offensive operations, which are those whose ultimate goal is to interrupt, alter, degrade, deceive, and/or destroy computer systems, information, networks, programs, among others, with the purpose of disrupting the normal functioning and development of the enemy's operations, causing both direct and indirect effects on the battlefield (CGFM, 2016).

A clear example of this type of operation is the recent conflict between Russia and Ukraine, where Russian hackers used a fake video of Ukrainian President Volodymyr Zelensky ordering his troops and fellow citizens to surrender. This fake video appeared in the Russian-language Ukrainian tabloid *Segodnya,* which accused enemy hackers of creating and publishing the deepfake on its website. Zelensky himself also denied the fake video in another video in which he called on Russians to lay down their arms (Kardoudi, 2022). This cyberattack could have taken the war in a different direction if cyber forces had not realized in time the critical situation the video could create.

Within this type of operation, activities such as infiltration, infection, cyber denial-of-service, data security, service degradation (slowdown), service disabling,

application of custom-designed code, and recovery can be carried out. Generally, these activities are conducted by personnel known in computer terms as hackers/crackers. These concepts are ambiguous in their etymology, but are related to the topic of cyber defense and attack.

In a positive sense, hackers are computer professionals who identify weaknesses in computer applications and help resolve them. In a broader context, hackers are technophiles who enjoy solving complex problems (Rytewiki, 2021). These types of experts are the ones who, in most cases, guide companies' cyber defense activities and advise on how to conduct cyber operations. In the case of the National Army, advisors and personnel from units responsible for these types of operations complement each other in carrying out their duties.

Conversely, crackers are individuals with extensive knowledge who attempt to breach the security systems created by hackers (defenders) to commit illicit acts. Thus, although both parties possess advanced computer knowledge, their ideas differ. Some attack illegally, while others defend legally. It is well known that hackers have a professional code of ethics that crackers do not, and they use any situation and means to achieve their objectives (Martínez, 2021). These concepts must be differentiated so that each can be defined and assigned to the objective determined for carrying out cyberattacks or cyber defenses. In the military sphere, they are called expert personnel or cyber agents. They are intelligence agents, as defined in Law 1621 of 2013, who possess training or expertise in the use of the methods and means described in that law. This distinction is important because the terms "hacker" and "cracker" are primarily used in the civilian sphere.

The second type of operations in cyber defense is cyber intelligence operations. In short, these seek to conduct a realistic analysis of current and potential enemies in cyberspace, allowing them to assess the true threats for planning and conducting operations. As in human intelligence, the same cycle is used: search effort, collection, processing, analysis, dissemination, and use of intelligence, but applied to the cyber environment.

Finally, within cyber defense operations is the third type: operations to defend critical cyber infrastructure. As the name suggests, these include protection activities, such as cyberattack prevention and mitigation, active defense, and the use of special devices.

Having now defined the two main types of operations and their subtypes, it is possible to outline potential applications of cyber operations to support SO units in Colombia. This capability, thanks to technological evolution and globalization,

is currently a vitally important element in destabilizing any organization, whether governmental or non-governmental, military or civilian.

Special Operations Liaison

Before analyzing the advantages and disadvantages of cyber operations in support of SO in Colombia, it is necessary to understand the strategic role and use of SF units in the country. Throughout Colombian history, the SF has played a vital role in the development of law enforcement events, from the siege of the Palace of Justice, which led to the creation of the first SF unit in the country, to the most successful attacks on the leaders of the Revolutionary Armed Forces of Colombia (FARC), which successfully brought this subversive group to the negotiating table during the 2016 peace process.

And the importance of this type of force has not only been established at the national level. In the United States, after September 11, 2001, with the attack on the Twin Towers, the importance of using the SF in the war on terrorism became evident. In a report submitted to the United States Congress after the operations carried out against Osama Bin Laden in May 2011 in countries in the Middle East, the effectiveness and evolution of the Special Operations Forces after more than ten years of fighting were highlighted:

> Special Operations Forces and Intelligence operatives—essential elements of a State's national power trident—are the best forces, the best trained, the best equipped, and the best led […]. This success is a direct consequence of President Obama's leadership and the national security priorities he established when he came to office, as well as the green light he gave to Special Operations Forces this weekend. (Rodríguez & Jordan, 2015, p. 108)

Due to the public order situation our country has experienced for more than five decades, the experience acquired by the SF in the National Army has made them a benchmark for various countries in the region, such as Brazil, Peru, and Mexico, and has even become an object of analysis in irregular jungle warfare. This is the case of the United States Army, which has a liaison from the Joint Special Operations Command (JSOC) working directly at the Joint Special Operations Command (CCOES) facilities to provide advice, but above all, to capture the knowledge that CCOES units use in the planning and development of SO throughout the country.

This high level of professionalization was achieved thanks to several factors: an exhaustive selection process; a high level of training; the provision of the highest quality materiel; the acquisition of national and world-class military materiel; a joint, coordinated, and interagency integration capability; and, finally, the greatest possible well-being for a soldier. Thanks to the combination of these pillars, all viewed within the operations, rest, and training cycle (CODE), goodwill has been acquired that currently allows the export of this capability to other countries for use in both training and operations.

A clear example of the excellence of the Colombian SF, apart from their operational effectiveness against terrorist groups, is the prizes they have won in Colombia's various participations in the South American Commando Forces Championship, held by the United States Army. Annually, in different Latin American countries, these units compete against each other for victory, putting distinctive SO military capabilities to the test, including assaults in confined areas, shooting tests, physical tests, high-precision marksmanship, stress tests, and demanding marches. Specifically, Colombia has won 10 out of 15 times it has participated in this competition, which features around 19 countries on the continent. It should be noted that the Fuerzas Comando is a competition sponsored by the United States Southern Command (USSOUTHCOM) and directed by Special Operations Command South (SOCSOUTH), whose objective is to promote regional and multinational cooperation, mutual trust, readiness, and interoperability of the Special Operations Forces of the Western Hemisphere (García, 2019).

That said, it is now necessary to analyze the doctrine of the SF to understand the applicability of cyber operations in their missions. By understanding how these units operate, it is possible to conduct a prospective analysis to determine whether it is feasible to integrate cyber capabilities into SF detachments or whether it is better to add that capability to a specific operation where it is required.

The SO are military operations conducted by specially organized, trained, equipped, and certified units that possess high mobility and flexibility in hostile, unprotected, and politically sensitive environments to achieve military objectives with strategic implications (Ejército Nacional de Colombia, 2017b). This type of military action is performed by various tactical units within the National Army, which together form the Special Forces Regiments (REGFE). These regiments are part of the National Army Special Forces Division (DIVFE) and possess unique, specialized capabilities.

They possess key traits necessary for designing this type of operation, such as strategic goals, high risks during execution, political and diplomatic effects,

intelligence, planning, training, air assets, and communications. These operations are conducted in hard-to-reach areas. When these traits are combined, supported, and fully realized, they create optimal conditions for the mission's success.

They can carry out two types of critical capabilities: special warfare and surgical strikes, both primarily used in Colombia. The former are the conduct of activities that involve a coordinated combination of lethal and non-lethal actions by SO with a broad understanding of the operational environment, mastery of foreign languages, and the ability to train and fight alongside other combat formations in permissive, uncertain, or hostile environments (Ejército Nacional de Colombia, 2017c). This type of capability is more focused on deploying special forces into external (foreign) environments to work with unified action partners. In this scenario, their objective is to develop regional stability, improve global security, and facilitate future operations, all while leveraging the special operator's ability to navigate and adapt to accepted cultural, behavioral, and tactical norms. These capabilities include unconventional warfare, security force assistance, counterinsurgency, operational environment preparation, non-combatant evacuation, foreign internal defense, information operations support, and civil affairs.

Regarding the second critical capability, surgical strikes are precisely planned and conducted military actions employed by the SF to capture, destroy, seize, or recover pre-designated targets (Ejército Nacional de Colombia, 2017b). These capabilities are used in the development of military operations within Colombian territory and have allowed the nation to strike major strategic blows against the leaders of terrorist groups, such as the former FARC, the National Liberation Army (ELN), and the Residual Armed Organized Group (RAOG) Clan del Golfo.

Among these capabilities, in which the Colombian Army is expert, are special reconnaissance, whose main objective is the search for real-time information through surveillance and reconnaissance, with very small groups infiltrated in the most adverse operational environments; direct action, where, through the use of firepower, the neutralization of targets is sought with short-duration operations; counterterrorism, which refers to all the tactics and techniques used to prevent and respond to terrorist actions; hostage rescue and personnel recovery, the purpose of which is to recover kidnapped civilian personnel in optimal conditions; and finally, air assault, a distinctive capability of the SF, in which they have extensive experience, which consists of employing various techniques to insert units into hostile environments.

With the critical capabilities and distinctive operations of the SF clearly defined, we can now begin to outline the advantages and disadvantages of employing cyber capabilities in Special Forces Operations.

In the organization of the SF units in the National Army, the minimum structure is a direct action detachment, which consists of twelve special operators, or a special reconnaissance detachment, made up of a reconnaissance team of six to eight operators, each with a unique specialty based on the mission. These specialties include weapons, intelligence, communications, explosives, medical, and planning. These specialties are the reason they are called Special Forces. Each operator specializes in one area, and there is a backup for each specialty within the detachment, meaning there is a primary and an alternate.

In this context, cyber operations fall within an intelligence specialist's expertise and are the direct responsibility of the institution's Intelligence branch, as analyzed in the previous sections. However, what must be determined here is the viability of the vast knowledge that a special intelligence operator must acquire to apply it within the Special Operations Forces. Given that cybernetics is a highly technical field and requires extensive experience, this specialist would require significant information, additional courses, and extensive experience in managing technologies and systems. Furthermore, since the priority of the SF is to work together to develop critical capabilities for accomplishing tactical missions, this operator would be in constant training, primarily in how to create networks of informants in the operational environment, how to infiltrate with fronts, and how to use that information to transform it into actionable intelligence. This would be their primary focus as an intelligence operator in the SF. Consequently, it would take too long to train this specialist to have real hacking or cyberattack capabilities.

In the IT world, it is said that to become a successful, mature hacker, one must build a solid foundation of knowledge and develop exceptional computer programming skills to overcome the obstacles they will face. Another of the most important areas these professionals must master is computer networks. Therefore, they must understand how they interconnect and communicate with each other through the internet and internal networks, and be familiar with the current and future protocols on which these networks are built (EUROINNOVA, 2019).

In other words, the focus is not on the special intelligence operator being a hacker; rather, the connection between the SF and cyber operations is based on the network management, programming, and advanced computer systems technology this operator must have, without considering how quickly computer

technology is advancing. The rapid technological evolution of recent years has been overwhelming, challenging even the most basic concepts. In a world that has changed at a pace no one anticipated, it is understandable that even those who consider themselves tech experts or work with technology daily can be confused and fail to grasp the full extent of the ongoing changes (Dans, 2010).

Therefore, this operator must have a minimum of skills that allow him, when necessary, to infect a computer center to destabilize or neutralize some enemy activity. This requires minimal skills to access various systems and, in the event of a blockage, for this specialist to break the encryption and infect the system. This is why it is not feasible for the capabilities of a cyber intelligence specialist to be organic to the SF detachment.

The most suitable and feasible approach, based on an analysis of the various variables, would be to add this pure intelligence capability to the SF detachment. By attaching it to the SO, regardless of the critical capability being used, there would be an intelligence agent with the actual capacity to handle any cyber situation that may occur, whom the organic personnel of the SF unit would protect. A basic level of training in movement techniques, tactical discipline, and general shooting would be required for this intelligence specialist to operate alongside the SF's main effort. Thus, at the critical moment during the operation, he would be able to use his programming, networking, and IT skills to successfully implant the virus into the designated network. After this activity, special operators would extract the unit safely, in accordance with the plan.

Among the advantages of having this hacker attached to the team are the following: technical knowledge of systems, networks, and programming; experience in managing complex systems and their components (encryption, keys, software, etc.); dedication to training in the Intelligence specialty (characterization, network organization, information gathering, etc.). These advantages are crucial during the execution of a Special Operation that requires applying this expertise under pressure—for example, under enemy fire or with limited time to extract personnel safely—and in resolving situations where the computer system is blocked or its cyber defense system is activated. This is when the cyber agent in the special unit must demonstrate their knowledge and experience in managing computer systems and networks.

Therefore, it is recommended that the cyber expert be a member of the Intelligence (CCOCI) attached to the team for the duration of the operational phases, such as planning troop deployment, developing tactical missions, extraction, and,

lastly, the after-action review (AAR), where the feasibility of continuing to combine the specialties of SF and intelligence weapons is determined.

A disadvantage of adding this capability to the SF is that within the detachment, there would be a man who is not trained in developing SO techniques, tactics, and procedures, which are unique within military doctrine and difficult to master given the high level of expertise within the SF. This could lead to delays in progress, the discovery of the assault force, violations of security measures, internal coordination issues among personnel, and other vulnerabilities, potentially resulting in mission failure and human and material losses in the worst-case scenario.

The Colombian SF provides a clear example of these risks, specifically the death of a member of the Technical Investigation Corps (CTI) of the Attorney General's Office during an operation against a FARC leader in Guaviare. After the Colombian Air Force (FAC) delivered weapons, as the CCOES special troops were being inserted into the air assault, an official from the Attorney General's Office had an emergency while rappelling, leading to his fall and subsequent death. He apparently did not follow the required protocol for these procedures. This unfortunate incident caused the operation to change its main objective, shifting focus to finding his body. This example, as argued, shows that integrating non-expert personnel into SO procedures involves significant risks.

Furthermore, the operational scope that cyber operations can offer to SO units may appear in various real-world scenarios. In special warfare and unconventional warfare—activities conducted in conflict environments aimed at gathering intelligence to weaken the adversary's fighting capacity through indirect means—such as actions targeting its resources and critical capabilities with the support of local personnel and logistics (Ejército Nacional de Colombia, 2017d), it is clear that using cyber and SF capabilities abroad, when needed, can produce favorable results when combined.

An example is inserting special troops into dangerous environments across enemy lines to reach a strategic target. Consider the case of a railway network control center, where SF personnel employ all techniques, methods, and tactics to infiltrate. With the support of a cyber-expert agent, they plant a device in their systems to infect them with a virus that would allow, remotely from an allied headquarters, chaos in the operation of train transport. In this scenario, disrupting schedules, routes, railroad directions, and information on the cargo carried by trains, among other actions, would paralyze this means of transport, which in a conflict would be vital for quickly and economically moving troops and heavy military transport vehicles, as well as the logistics for the development of military operations.

This is exactly what occurred during the war between the Russian Federation and Ukraine in Eastern Europe, where a key focus has been enhancing the capabilities of railway troops. Their role is to keep railway lines operational during and in preparation for combat operations, as well as to set up temporary armored vehicle disembarkation points on the battlefield. A past conflict highlighted the need for this reform: during the 2008 Russian-Georgian war, the railway system performed poorly, causing some Russian units to face significant difficulties in delivering drinking water, food, fuel, and ammunition (Montero, 2021). As is evident, railway transportation systems are critical in any conventional conflict.

Continuing with the presentation, another way cyber operations can support the SF in tactical settings is by damaging weapons systems—both ground and air—at a specific military installation. An example might be infiltrating a military installation using SF techniques and, with the help of a hacker, disabling its defenses to allow the entry of infantry, cavalry, or aircraft from the National Army Air Force or the FAC.

Another type of mission where a strategic lethal weapon could be used alongside cyber support is attacking energy sources. Electrical energy is one of the most valuable and widely used strategic resources today, so if this service is disrupted, the use of virtual tools is severely impacted, which in turn leads to decreased productivity and significant monetary losses for some industries and companies (Asociación Colombiana de Ingenieros de Sistemas [ACIS], 2021).

In this context, for example, cyberattacks on a power plant can be used to introduce a virus into its systems and bypass equipment security while special operators conduct security tasks. This could enable the country to be temporarily incapacitated so that conventional forces can perform territorial control, an offensive operation, or an occupation, thus gaining a tactical advantage on the ground. Additionally, since essential services like food, transportation, or public utilities (water, energy, internet, phone, etc.) are vital for the normal functioning of a society, disrupting or affecting these services through an SF operation could cause social disorder and destabilize the opposing government.

In the current, real-life situation in Colombia, where the internal conflict is being waged primarily against various guerrilla organizations, such as the ELN or the RAOG, a direct action special operation such as those described above could also be considered. For example, after a special units attack a specific camp where leader X is located, a cyber agent could be deployed via air raid to access the computers (laptops, USB drives, etc.) located there and hack vital information,

such as email accounts, financial information, locations, contacts, potential future terrorist plans, and more. Thus, in real time, they could penetrate these computer systems and use the information to carry out deception operations, prosecute individuals with terrorist ties, launder bank accounts, seize assets, position units at an advantage in certain regions, conduct counterintelligence, thwart terrorist attacks, and other actions that law enforcement and other agencies responsible for state security can carry out.

These and many other examples illustrate the infinite operational scope of cyber operations in conjunction with special operations units in tactical environments. This type of operation would be an Achilles' heel for the enemy in a given situation, whether at home or abroad.

The use of these capabilities is common in current global conflicts, where hard and soft power merge across multiple fronts. This is examined through the Gerasimov doctrine, which outlines a new type of warfare involving economic retaliation, propaganda, political subversion, and psychological operations. To secure victory, gaining dominance in managing information and strategic communication is essential (Kowalski, 2021). This is precisely the environment where cyber capabilities can offer tactical support to SO units, allowing them, when combined, to serve as a spearhead for the National Government in security and defense matters.

Conclusions

The analysis demonstrates the importance of cyber operations today. Like their role in modern warfare, they are vital in both a country's defense and offense. A clear example is the conflict between Russia and Ukraine, where the use of these capabilities by both sides has shaped the course of the war. Disinformation spread to the global population; Ukrainian government officials' information was compromised; and sophisticated Russian techniques were used to spread propaganda and justify the invasion of Ukraine. These actions exemplify the wide range of damage cyber actors can cause.

The SF have been vital in the conduct of wars from ancient times—when they were not identified as such, even when carrying out typical SF actions—to the modern era, where they have neutralized internationally renowned terrorists such as Osama Bin Laden. These units will enable any State to achieve strategic military

objectives that are difficult to attain under the most adverse conditions, thanks to their inherent capabilities.

The combination of these two capabilities—cyber and SF—enhances the likelihood of success a commander needs at the strategic level. As shown in earlier sections, this combination provides many benefits for specific missions but also has some disadvantages, as is common with any integration. However, if used separately, it would not be feasible to develop these critical missions. Therefore, it can be concluded that, in certain cases, the support cyber operations offer to SF in tactical environments is essential. Disabling security systems, controlling communications, providing vital energy to a specific region, extracting information for later use, deception operations, among others, are the various ways a commander at the strategic level can leverage this pairing at the tactical level.

The importance of joint training between Intelligence (cyber) and the SF lies in reducing the disadvantages associated with these actions. This coordination between the cyber agent and the special operators enhances the success factors of the mission, since the alternative—having an Intelligence specialist as a key member of the direct action detachment or within the special reconnaissance team—requires extensive training time, which is essential for the SF.

In this regard, further study of this topic strengthens Colombia's strategic capabilities, which include its intelligence, cyber defense, and special forces. Therefore, it is crucial for special forces and intelligence agencies to develop a doctrine for jointly using these capabilities through practical planning and exercises. This approach would help us start to accomplish military objectives in a potential scenario of external or internal conflict, ensuring that, over time and if needed, Colombia can respond effectively by integrating these strategic strengths to counter a looming threat to the nation.

In the current tense environment in the region, where the use of all means of combat, including hybrid warfare, is possible, it is necessary for Colombia to keep this cyber + SF capability on alert so it can be deployed at any time and used in tactical missions for strategic purposes. Given the current conditions of uncertainty and volatility, it is not unreasonable to think that a scenario could arise where it would be necessary to use it.

References

Aharonian, A. (2018, September 4). *La guerra de quinta generación.* https://tinyurl.com/3k284r38

Asociación Colombiana de Ingenieros de Sistemas [ACIS]. (2021, September 13). *La importancia de garantizar la continuidad del servicio de energía en las industrias.* https://tinyurl.com/78z8nr5j

Azabal, G. (2021, November 25). *Guerras híbridas: cuando los conflictos se modernizan pero nada cambia.* https://tinyurl.com/yvdtfhyp

Blue Radio. (2021, June 11). *La historia detrás del hackeo más grande contra las Fuerzas Militares de Colombia* [Video]. https://tinyurl.com/kahps392

Castells, M. (2000). *Internet y la sociedad red* [Inaugural lecture]. Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento, Universitat Oberta de Catalunya, 1999. https://tinyurl.com/mpnphpx3

Centro de Doctrina del Ejército [CEDOE]. (2016). *Manual Fundamental del Ejército MFE 3-07 Estabilidad [Public].* Publicaciones Ejército. https://tinyurl.com/3bdvy9cd

Comando General de las Fuerzas Militares [CGFM]. (2016). *Manual de Ciberdefensa Conjunta para las Fuerzas Militares [Restricted].* Imprenta y Publicaciones de las Fuerzas Militares.

Comando General de las Fuerzas Militares [CGFM]. (2018). *Manual Fundamental Conjunto MFC 1-0 Doctrina Conjunta.* Imprenta y Publicaciones de las Fuerzas Militares. https://doi.org/10.25062/MFC10

Dans, E. (2010). La evolución de la tecnología: del ordenador a la nube. In *Todo va a cambiar: Tecnología y evolución: Adaptarse o desaparecer* (pp. 191–206). Ediciones Deusto.

EcuRed. (2012, March 30). *Ciberespacio.* https://tinyurl.com/4pvs267y

Ejército Nacional de Colombia. (2017a). *Manual Fundamental de Referencia del Ejército MFRE 3-07 Estabilidad [Public].* Imprenta Ejército. https://tinyurl.com/yfp4rmfv

Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 3-05 Operaciones Especiales [Public].* Imprenta Ejército. https://tinyurl.com/32dbw83e

Ejército Nacional de Colombia. (2017c). *Manual Fundamental del Ejército MFE 1-01 Doctrina [Public].* Imprenta Militar del Ejército. https://tinyurl.com/h8ywavpv

Ejército Nacional de Colombia. (2017d). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones* [Public]. Imprenta Ejército. https://tinyurl.com/ducm7tje

Ejército Nacional de Colombia. (2021). *Manual de Campaña del Ejército MCE 3-12 Operaciones del Ciberespacio [Restricted].* Publicaciones Ejército.

EUROINNOVA. (2019, January 21). *¿Quieres saber qué estudiar para ser hacker? Euroinnova te lo cuenta.* https://tinyurl.com/2fd5xe3n

Fink, K. D., Jordan, J. D., & Wells, J. E. (2014). Consideraciones para las operaciones ciberespaciales ofensivas. *Revista Military Review,* (May-August), 24–33. https://tinyurl.com/52sh3hrk

Instituto de Seguridad y Bienestar Laboral [ISBL]. (2023). *¿Qué son las infraestructuras críticas?* https://tinyurl.com/3hrsjv5x

Kardoudi, O. (2022, March 17). El primer "deep fake" usado en un conflicto armado muestra a Zelenski rindiéndose. *El Confidencial.* https://tinyurl.com/yuu3d6y5

Kowalski, M. (2021, July 10). *Conflictos híbridos y la doctrina Gerasimov.* https://tinyurl.com/3f8debrj

La Vanguardia. (2018, December 18). *La interferencia rusa en las elecciones de EE.UU. fue dirigida a los afroamericanos.* https://tinyurl.com/mvcr7fuh

Ledo, I. N. (2011). Las redes sociales [Editorial]. *Revista Venezolana de Oncología, 23*(3), 133. https://tinyurl.com/4v46bv4s

Martínez, J. C. (2021, August 30). *Qué diferencia hay entre un cracker y un hacker*. https://tinyurl.com/3kmy78u9

Montero, A. (2021, May 30). Análisis de la guerra en Ucrania desde la logística militar [Video]. *YouTube.* https://www.youtube.com/watch?v=2HT_7Is1sGw

Real Academia Española de la Lengua. (2022). Tecnología. *Diccionario de la Lengua Española.* https://tinyurl.com/2pedndwd

Rodríguez, R., & Jordan, J. (2015). La importancia creciente de las Fuerzas de Operaciones Especiales. *Revista UNISCI,* (38), 107–123. https://tinyurl.com/ud5jn5fm

Rytewiki. (2021, February 1). *Hacker.* https://tinyurl.com/56kj348u

Salazar, S. (2020, December 9). *¿Qué es la doctrina militar y por qué es importante?* https://tinyurl.com/6dryzn3k

Sánchez Medero, G. (2009). Internet: una herramienta para las guerras en el siglo XXI. *Revista Política y Estrategia,* (114), 224–242. https://tinyurl.com/23979csn

Today's Military. (2022). *Especialistas en seguridad cibernética.* https://tinyurl.com/59m488kb

EDITORIAL ESDEG

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 disinformer (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/4bjcbn52

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/44vvvcmt

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/mzvtnc43

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/zbdcynur

EDITORIAL ESDEG

Chapter 9

Limits of Artificial Intelligence and Big Data Technology in Intelligence Analysis*

DOI: https://doi.org/10.25062/9786287818408.09

Jaime Andrés Naranjo Ardila
Jorge Luis Mejía Rosas
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Artificial intelligence (AI) and big data create a teaching and learning environment for processing information in intelligence analysis. This technology introduces new scenarios in the geopolitical, security, and defense sectors, with features that help define boundaries that national security agencies will examine. In this context, it is important to trace the development of AI, as scientific and technological advances are rapidly progressing. This trend is vital for those involved in processing information, as easy access makes it crucial to follow legal guidelines for protecting personal data. Additionally, the challenges posed by AI foster innovation in the legal protection of personal data and application use.

Keywords: analysis; artificial; intelligence; limits; technology.

* 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.

Jaime Andrés Naranjo Ardila

Lieutenant Colonel in the Colombian National Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Leadership and Management of Military Units and Specialization in Military Resources Administration for National Defense, National Army Arms and Services College, Colombia. Diploma in Leadership with an Emphasis on Administration and Diploma in Administrative and Disciplinary Expertise. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: **jaime.naranjoar@buzonejercito.mil.co**

Jorge Luis Mejía Rosas

Retired Colonel of the Colombian National Army. Specialization in Military Intelligence, Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano," Colombia. Specialization in Military Resources Administration, Arms and Services College, and Specialization in University Teaching, Universidad Militar Nueva Granada, Colombia. Bachelor's in Military Sciences and Bachelor's in Business Administration, Escuela Militar de Cadetes "General José María Córdova," Colombia. **https://orcid.org/0000-0003-3233-4948**
Email: **jorge.mejia@esdeg.edu.co**

APA Citation: Naranjo Ardila, J. A., & Mejía Rosas, J. L. (2025). Limits of Artificial Intelligence and Big Data Technology in Intelligence Analysis. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 189-208). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.09

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

It is no secret that over the last decade, there has been a significant technological shift in habits, preferences, and how products and services are acquired. As part of these advances, there are currently technological innovations that can be applied in the field of military intelligence, such as artificial intelligence (AI), the Internet of Things (IoT), virtual reality, blockchain, apps, e-commerce, and big data, focused on customer needs, but which until now have not been fully utilized. Indeed, AI enhances information collection processes by creating a comprehensive data control system, which improves organizational performance and allows the Force to develop various skills, agreements, and commitments based on the science of military intelligence.

This chapter aims to analyze how AI and big data technology are used in military intelligence for planning in Special Operations (SO). First, it examines the technological advancements impacting Military Intelligence and Special Forces (SF), highlighting that innovation enables secure data collection through cryptographic codes that have not been breached so far. The chapter emphasizes the need to develop a plan that promotes the adoption of proactive measures to avoid improvisation when facing high-risk threats. Therefore, the use of big data and AI is seen as contributing to prevention, control, and mitigation efforts, while also ensuring the anonymization of personal data.

This process must include "data mining and big data" because if the variables and expectations of all stakeholders the organization interacts with are not considered, it will not be able to achieve its objectives and goals. Therefore, it is essential to perform control and monitoring at this stage to ensure the plan is practical and achievable.

Second, it connects AI and big data technology to human intelligence in SO. Based on the analysis, it is recommended that implementing processes and procedures is necessary to help the organization position itself effectively. To achieve this goal, AI is a practical option, as it allows the integration of all automated processes, creating a model that produces efficient results and, therefore, improves the information collection process. This enables the identification of the characteristics, customs, preferences, procedures, behaviors, and development of people and organizations.

Finally, the role of big data technology in ongoing improvement is analyzed as a global trend, suggesting that all kinds of good management practices should be examined.

Background

The first mobile apps date back to the late 1990s, when they were already embedded in computers. A clear example is the calendar in Windows 95, which initially started as an app that sent alert signals, or arcade games, a trend at the time, whose producers found a niche market (Bonami et al., 2020).

According to Ahedo and Danvila (2014), the evolution of apps continued with ringtone editors, which performed very basic functions and had a fairly simple design. From this point on, app development accelerated thanks to technological innovations, supported by significant advances in cell phones, as companies that produced them developed competitive advantage practices.

Actually, a revolution has started in the creation of apps, games, news, design, art, photography, and medicine, all in the hands of users, thanks to the rapid innovation processes of mobile applications (Fernández, 2020). At the same time, the internet has produced numerous high-quality tools aimed at fostering innovation through information and communication technologies (ICTs), providing personalized access to data and allowing citizens to identify the strengths and weaknesses of public administration.

This was evident during the handling of the coronavirus pandemic (Fernández, 2020), when it was publicly discussed that these innovations could violate rules regarding the right to *habeas data*, as they collect and centralize user information by locating personal data. Although used solely for health statistics, this data is centralized only for informational purposes (Navarro, 2014).

Therefore, while this information can be used to verify it with information centers, it can also be exploited to locate a person in real time for criminal purposes. Therefore, as Daza (2020) points out,

> it is crucial not to oversimplify, polarize, or reduce the issue to just a renunciation of privacy to protect life or health, or to avoid lockdowns and other restrictions on our freedoms. Privacy violations, like those during the coronavirus pandemic, are often not recognized or felt until it is too late. Therefore, if the debate is framed in these extreme terms, no one would prioritize privacy. (p. 12)

Learning is another area where AI makes sense, as there are currently applications that, for example, convert maps into three-dimensional (3D) scenarios when viewed with a mobile device or webcam. Although these applications respond to the need to determine people's health status, identify risks, and include alarms or alerts, it is clear that these technological advances lead to a scenario that goes beyond the information level, as they deploy functionalities with invasive characteristics (Orozco, 2003).

Evolution in the Conception and Planning of Contemporary Hybrid War Scenarios or Confrontations

Currently, the evolution of conflicts in the international system has made adversaries invisible due to the widespread use of technology, creating many challenges for modern societies. This is especially clear when it comes to developing security and defense strategies, as well as public policies that can protect national interests, given the various risks to peace and harmonious coexistence. The importance of this issue is clear, especially with the emergence of new actors capable of destabilizing institutions in pursuit of their interests, which are often protected within the illegal economy and override the State's goals (Valencia et al., 2019).

In this context, the evolution of technology has enabled advancements in AI, which has achieved notable results across various fields of society. This has improved the ability to make informed decisions amid unexpected events by analyzing data processed by machines. However, this also creates high-risk scenarios for humanity's survival, as countries like the United States, Russia,

and China have revamped their national security strategies using AI resources to defend their interests during conflicts or peacekeeping missions.

Historically, globalization has gradually transformed the way a national security strategy is defined, leading to the creation of crisis, normalization, and stabilization zones, all aimed at fostering peace. State security has evolved over time and made a significant leap forward after the September 11, 2001, attacks on the Twin Towers in New York. This event revealed the rise of new threats to global security, which used different methods of action and attack. Consequently, state intelligence agencies adapted and prepared, leveraging technology to accomplish their goals.

Indeed, it is clear that the main advancements in AI are occurring in world power States, both in their security and defense strategies and in the implementation of their strategic plans. However, the fact that this technology is used in a wide variety of scenarios introduces the risk of serious threats emerging, some of which are technological and others human-related. Experts warn that two major threats linked to AI are that it could become self-sufficient or superintelligent, surpassing human abilities, and that it could be used for lethal or malicious purposes against other countries or non-state actors.

The self-sufficiency of AI, meaning when it surpasses humans in all understandable aspects, has already been considered by science and is called "the technological singularity." Stephen Hawking argued this point, openly saying that such technology could spell the end of humanity. Meanwhile, Nick Bostrom (2016), a professor at the University of Oxford, believes that AI can, to some extent, replace human intellectual work, such as by providing better analysis. He emphasizes that this kind of technology must include human values and work in harmony with all society's actors to produce positive outcomes; otherwise, Bostrom (2016) warns, the scenario could be catastrophic and irreversible for humanity.

From a more moderate perspective, Dr. Ramón López, director of AI in Spain, states that super AI is still far from reality, and therefore, the idea that this kind of technology could dominate the world lacks scientific foundation, since the necessary technological evolution is required to achieve the singularity (Pérez, 2023). Other experts point out that even if an AI with a higher intellectual level existed, it would never be superior to humans, as it does not interact with the environment in a human-like manner. However, these reflections make it clear that all types of ethical dilemmas must be thoroughly examined, especially regarding the use of autonomous weapons (Valls, 2018).

However, regarding AI used for criminal activities, Sonia Pacheco (as cited in Rubio, 2018), director of the Business World Congress, points out that it can have a significant impact due to the risks it poses to a State's security and defense. In this context, it is important to distinguish between the "unintentional" misuse of AI and its "intentional" misuse, such as using drones for terrorist purposes or manipulating electoral contests with accounts that use algorithms on social media to automate messages, known as bots, which perform repetitive tasks 24 hours a day. An example of this malicious use of AI is the attack on military bases in Syria by non-state actors or the development of autonomous weapons that are lethal (Rubio, 2018).

AI, a Strategic Component of a State's Defense

AI is a technology that can be viewed either as a destabilizing factor in military force deployment or as a disruptive tool across all sectors of society's economy, industry, and social activities. The geoeconomic and geopolitical capabilities produced by this technology directly influence the international strategic landscape, as they support informed decision-making and the development of national security strategies, allowing for the consideration of the most critical variables to choose the best course of action. While its use depends on the capabilities of individual States, it is currently a mechanism that major powers such as the United States and Russia have adopted.

Therefore, the development of AI is a crucial element of national security, helping shape domestic policies that align with international community considerations. This technology has gained widespread acceptance, with China in 2017 launching an ambitious state plan with a future-focused technological program (2030) aiming to become a global leader in AI applications. As a result, a worldwide race for dominance in this field started, according to a 2018 World Economic Forum report, which estimated that investment in AI will reach $127 billion by 2025.

It is crucial to analyze the strategic idea of AI and the reasons for governments' substantial investments. Specifically, the current world is constantly changing, with major powers competing for technological and military dominance, vying for international influence, and aiming to protect their national interests.

Indeed, States that use AI should develop a multilateral foreign policy, considering the various threats in the global environment, such as climate change, the spread of weapons of mass destruction, financial crises, and pandemics. The

need to create and implement cooperation mechanisms that can unify efforts across multiple dimensions is clear.

Similarly, the use of AI is important for, for example, fighting pandemics and multidimensional poverty, or strengthening international commitments aimed at improving transportation infrastructure. Greater economic and social development boosts people's quality of life and raises the demand for better environmental protection, which in turn increases their participation in the global trade dynamics.

In this context, it is important to recognize that blockchain enhances AI processes in national security and defense, supporting better management of information aligned with national interests. Additionally, it aids in applying accounting methods in organizational performance, fostering the development of skills, agreements, and commitments in these technological areas, although it always faces limitations related to data protection, confidentiality, and privacy (Martínez, 2019).

In turn, this blockchain trend enables secure data storage using a cryptographic code that has not been compromised so far. Mechanisms for managing such information are evolving within a framework of globalization and technological progress surrounding the global village, showing that companies face specific risks that can affect their sustainability and profitability.

Means Used in Planning and Executing Contemporary Hybrid War Scenarios or Confrontations

Planning involves various methodologies that consist of systematic, step-by-step procedures leading to a series of decisions that can produce results in the military field. Specifically, the desired end states are defined through a study of the operational environment, with a focus on utilizing the capabilities of military units, including AI optimization, to attain a position of relative advantage over the adversary and other threats. These tasks are based on decisive action and promote offensive maneuvers (Bonami & Dala, 2020).

Considering the new security and defense challenges, the Joint Force is called upon to perform all types of activities using AI, in conjunction with the development of military operations, to create a strategic advantage and capability that will enable it to be more effective against current threats and trends in global security (Hueso, 2019).

Therefore, the use of AI technologies is not only important for movement and maneuver, as they improve the integration of the country's security and defense to achieve a unified effort in consolidating territories, but also in military operations, which aim to gain a relative advantage against any threat that endangers the lives and dignity of Colombians (Bravo, 2010).

The use of AI also makes it possible to neutralize the main structures of Organized Armed Groups (OAG) through aerial reconnaissance to identify the positions of mobile columns and through intelligence work (human and technical) on the enemy. This enabled the Government to effectively reduce activities such as kidnapping, homicides, and all types of illicit acts between 2018 and 2022. This state policy, as it has become, demonstrates the importance of institutions "occupying" all national regions and contributes to society's performance in eradicating the social inequalities the country faces (Galindo, 2005).

Indeed, planning involves the continuous and simultaneous coordination of military forces' activities, and in doctrine, it serves as one of the fundamental components of capabilities. This reflects the transformation of the institution's new organizational structures in pursuit of strategies for change and renewal, as well as the new vision, awakening, and potential transformation in training and capacity building. In this context, Unified Land Operations (ULO) enable initiative and provide an advantageous position against various sources of violence through a series of offensive and defensive operations, as well as collaboration from inter-institutional or international perspectives.

Military professionals utilize the art of movement and maneuver through training and tactics, guided by the commander's intent, by selecting among interconnected options.

- Types of offensive or defensive tasks that describe the maneuvers and tactical mission tasks
- Combat organization of available forces, including the distribution of limited resources
- Fundamental choice of control measures
- Time (before, during, and after) of the operation
- Challenges the commander is willing to take on (Vigevano, 2021)

This element is crucial for strengthening cooperation between Colombia and its allies, given that State Strategic Intelligence and Counterintelligence are key factors in decision-making. Additionally, it is important to consider that external factors directly influence Colombian foreign policy, and this element will help in achieving the State's main objectives.

- From a strategic point of view, the relationships between Colombian intelligence agencies and their allies can be strengthened by developing strategic intelligence and counterintelligence activities to protect national interests and gain greater control over transnational crimes.
- From an operational perspective, military intelligence can enhance its capabilities and resources with the main goal of conducting coordinated operations that directly target illegal armed groups operating in border regions.

In this context, the intelligence cycle within a hybrid warfare setting can be defined as the set of skills and abilities that, through the use of AI, enable the analysis of economic, political, and social factors. These components, working in an integrated manner, enhance combat effectiveness with the goal of gaining a military advantage and initiative to counter all types of threats to a State's sovereignty and policies. Currently, the implementation of all interventions relies on conflict-sensitive program management and a cross-cutting approach to equity issues. Special attention is also given to developing sustainable solutions and intervention methods, one of which is military intelligence, involving the broadest possible participation.

Hybrid Confrontation Scenarios Applied to Colombia in the Context of a Hegemonic and Regional Confrontation

Currently, there is an arms race to achieve global dominance, with the United States, China, and Russia as the main competitors. These countries understand the importance of enhancing their AI technologies to serve their national interests, a development the academic community calls the "AI Cold War." For example, China has invested about $150 billion in technology as part of its development plans. This is why they are adopting proactive strategies to become world leaders in AI and establish themselves as the center of global innovation in the near future.

Undoubtedly, compared to previous economic and social revolutions, the development of AI is both dynamic and universal, as it ensures continuous and simultaneous connections that form the basis of so-called globalization. It influences economic, commercial, political, and social activities, capital accumulation, the creation and sharing of knowledge, and information management worldwide.

Similarly, following the Industrial Revolution and the advent of mass production, automation, and robotics, "Industry 4.0" is already considered the "Fourth Industrial Revolution" due to its potential and benefits related to integration, innovation, and process autonomy. The concepts of Industry 4.0 and smart manufacturing are relatively new and contemplate the introduction of digital technologies in the manufacturing industry; that is, the incorporation of technologies such as IoT, mobile computing, cloud computing, big data, wireless sensor networks, embedded systems, and mobile devices (Valencia et al., 2019).

However, some objectives help enhance information processes through open sources. A clear example is that these technologies encourage situations where individuals can share their collaborative skills, join groups, and build a sense of teamwork to gather useful information from large data flows. As shown, these technological features support long-term education.

In this context, for AI's information process to be thorough, specific specialties are needed—such as identity profiling, systemic situational analysis, and foresight—that help create a unique representation of humans. These specialties determine qualities of unification, consolidation, communication, and decisive actions, enabling controlled integration of AI and intelligence. Blockchain aids in distributing, but not copying, digital information. A simple example illustrates this: a spreadsheet duplicated thousands of times across a computer network. The network then updates this spreadsheet regularly, forming the basis of a blockchain (Palomo-Zurdo, 2018, pp. 11–23).

Currently, there is a wide range of information collection programs in the cyber environment, not only for academic purposes but also for obtaining precise data for a State's public services. As a result, there are programs that organize people's information based on their employer, home location, interests or preferences, and other relevant details to gather important data (Navarro, 2014). Some of the most commonly used open-source programs are:

- *Shodan:* This search engine locates computers, webcams, printers, and various electronic devices
- *Namechk:* It shows whether a username is available on more than 150 online services.
- *Tineye*: It is a search engine that, based on a picture, shows which websites it is on (Navarro, 2014).
- *Pipl:* This search engine connects people to different social networks and online links.

- *Domaintools:* This service identifies, monitors, searches, and analyzes a domain name.
- *Tagboard:* It analyzes different Twitter (now X) hashtags.
- *Twopcharts:* This tool analyzes everything posted on Twitter, allowing you to view likes, the timeline, and the history of posts, lists, and relevant content.
- *Foca:* This program extracts and analyzes metadata from different types of documents (Arcos, 2015). By understanding the metadata, you can determine who created or modified it, the type of software used to generate it, and other relevant information about the file (Rosales, 2005).
- *Metapicz:* It extracts metadata from photographs and thus reveals various types of information, such as the camera, software, dates, and phone used.

In this respect, the reality is that organizations cannot afford to wait that long in an era where cybersecurity breaches happen quickly, as an organization's security relies on rapid identification and response. This raises the question: How can a country like England, with strong information security processes, enhance its ability to detect "advanced adversaries" in systems and networks? The answer is that organizations have recently sought to proactively develop various processes, while simultaneously optimizing their cyber and AI infrastructures and institutions (Chipuxi & Paucar, 2020).

The Role of Special Forces in Using AI as a Strategic Tool

The process of automation and monitoring through sensors plays a vital and essential role for SF soldiers in today's operational environment. AI is increasingly advancing in gathering all types of meteorological data, as well as information on the physical and health status of personnel, and on a soldier's capabilities, in real-time to enable optimal decision-making. Additionally, regarding the enemy, it helps understand their weapons, identify their strategies, and analyze their courses of action to attack or defend based on patterns provided by large servers, among other highly relevant aspects.

Therefore, to fully develop AI's potential, interconnection is vital—i.e., the constant exchange of information between different systems, enabling each to

respond to potential threats. However, to accomplish this, access protocols for such data must be strong, ensuring no loss and preventing enemy interference.

In turn, AI enhances decision-making by allowing sensors to be placed on soldiers to monitor their physical and emotional states, as well as on vehicles and systems, and by utilizing aerial photography and audio and video recordings of the operational environment, providing a wealth of valuable information. Typically, 90 percent of SO involves planning and establishing strategies, control points, enemy locations, and other critical aspects. According to General Clarke, Commander of the U.S. Special Operations Command, most military leaders, especially those in the SF, spend the majority of their time on planning (Barceló, 2001).

Therefore, modern armies with SF must create new organizational structures that include AI technology to scan all types of computers and cell phones; gather and counter messages left by adversaries on social media and analyze their trends; examine in detail the situation and the enemy's interests or objectives; and establish an operations center to combat all forms of fanaticism and violent extremism that aim to destabilize government entities (Palomo-Zurdo, 2018).

In turn, AI must assist in detecting electromagnetic threats. For instance, drones equipped with this technology and autonomous learning capabilities can select targets and carry out direct fire actions. These operations must be overseen by an operational legal advisor to ensure the best legal decisions are made, always safeguarding the integrity of law enforcement officials. In this context, human control over these machines is essential to ensure humanitarian protection and proper legal oversight.

In this regard, it should be noted that the U.S. Department of Defense, in Directive No. 3000.09 of November 12, 2012, defines an autonomous weapon system as

> A weapon system that, once activated, can select and engage targets without further intervention by an operator. This includes, but is not limited to, operator-supervised autonomous weapon systems that are designed to allow operators to override operation of the weapon system, but can select and engage targets without further operator input after activation. (U.S. Department of Defense, 2012, p. 21)

Autonomous weapons systems without human control are tools that select and attack targets based on criteria set by programming engineers and operational rules. However, they cannot be stopped by human intervention once the attack has

been initiated. It is also important to note that there are currently over 380 semi-autonomous weapons developed by Israel, China, the United States, and other countries (Sossa & Reyes, 2021).

Although they have not yet been used in armed conflicts, they are expected to be deployed soon as robotics and AI advance. To this end, developed countries, especially major powers, are investing substantial financial resources into the military sector, making the replacement of soldiers with technology appear not to be a distant possibility (Acosta, 2020).

Not every automatic weapons system is fully autonomous, as human intervention in programming must comply with all legal parameters, which means it requires an operator. Currently, many military weapons feature high levels of automation and can also operate semi-automatically. Drones, for example, can perform tasks like taking off and landing automatically, without human control, thanks to routes programmed with the Global Positioning System (GPS).

In the United States, a large part of its defense budget is allocated to developing AI, giving it a significant edge over China, its main rival. Specifically, these technologies are connected to the following areas:

- *Unmanned operations:* Includes aerial, land, and marine systems, both surface and submerged, with unmanned and increasingly autonomous systems.
- *Long-range naval and air operations:* Utilizing floating expeditionary bases or unmanned tanker aircraft, which greatly extend the reach of U.S. Forces aircraft without depending on unreliable allies (Vigevano, 2021).
- *Unobservable operations:* Includes stealth technologies that go far beyond radar "invisibility." Aspects such as material composition, paint, and infrared emissions complicate invisibility to unimaginable levels (Gutiérrez, 2014).
- *Submarine warfare:* This is another field dominated by the United States, but China is building unmanned submarines that would be capable of carrying out kamikaze-style attacks against enemy vessels.
- *Systems engineering and integration:* This is the key to the entire U.S. military architecture. It consists of a system of systems, focused on new levels of inter-arms cooperation within each army and across the armed forces as a whole, enabling greater control over the battlefield.

Therefore, it is important that many countries have established various legal frameworks to regulate the protection of personal data. With the rise of AI and the availability of big data, there is a risk of personal information being compromised,

such as through impersonation or the creation of detailed profiles used for extortion, illegal political activities, or what is called cognitive warfare. *Cognitive warfare* involves manipulating the masses into believing a series of catastrophic events caused by their leaders' decisions, often without any clear criteria or objectivity.

In short, the United States' strategy aims to outpace Chinese advances to protect human combatants. It is developing remotely operated and autonomous unmanned aerial, naval, and ground systems capable of surprise attacks and striking anywhere, anytime, based on a global observation and attack network (Acosta et al., 2020).

In this context, new technological developments have shown that privacy and personal data protection can be compromised in various ways. This issue affects not only one country but millions of people worldwide, crossing borders, as recently exemplified by the Cambridge Analytica scandal in the geopolitical electoral arena. This company specializes in conducting tests on large populations to send personalized messages aimed at influencing their purchasing decisions in both commercial and electoral areas, encouraging citizens to buy certain products or align their voting intentions with specific candidates. The most notable case was during the United States presidential election that resulted in Donald Trump's victory (Hill & Dance, 2020). These events highlight the importance of establishing limits that security agencies must consider.

AI technologies are another resource available to personnel responsible for analyzing and processing information, facilitating the collective creation of knowledge through their easy access. However, it is crucial to establish guidelines to legally protect personal data, ensuring that the results of these analyses do not fall into the wrong hands of criminals or corporations that blatantly misuse it for electoral or commercial purposes. In this way, AI and big data can offer a teaching and learning environment for analyzing the information used in intelligence processes.

Ultimately, new AI challenges drive innovation and shape trends. In the military sector, AI and big data connect user information databases to analyze data and determine solutions or corrective actions, including monitoring what was planned versus what was actually executed to ensure goals are reached. Therefore, establishing guidelines for the legal protection of personal data in apps becomes increasingly important.

Conclusions

AI and big data technology in information analysis are essential concepts in the intelligence process. This must be considered at various levels of strategic planning, as using these capabilities can influence the operational environment and decision-making, especially in developing grand strategies. Likewise, the use of AI and big data continually refines and enhances intelligence capabilities to conduct analyses that closely mirror reality, enabling the creation of more accurate future scenarios in response to this new challenge.

Likewise, it is important to identify the variables and expectations of all involved parties to verify their honesty and credibility. This allows for the clear definition of objectives and helps determine which goals are most likely to be achieved. Therefore, developing more effective control and monitoring systems is necessary to ensure that planning aligns more accurately with reality.

With the advancement of innovation and technology, AI and big data can serve either positive or negative purposes; they might be used to create advantages that leverage favorable situations based on truth or deception. In this context, the use of AI and big data technology in the planning and execution of modern war scenarios or hybrid conflicts is critically important for decision-making, as these are carried out as a series of interconnected tasks and strategies that involve deploying forces and various spheres of power to gain a relative advantage over the adversary, threats, and instability factors.

In this context, Military Intelligence becomes more effective when it enhances its capabilities and resources to gather more intelligence. By conducting a more comprehensive analysis with these tools, decision-makers can create more effective plans for coordinated operations that support mission success and achieve the desired end state in various theaters or areas of internal and external operations.

For this reason, we need to recognize the revolution that these technologies are creating. For instance, if they are used to develop AI that identifies the adversary's center of gravity, it can greatly increase the advantage, making operational decisions more efficient and reducing human resource interventions, thus making them more lethal. Similarly, weapons technologies, no matter how advanced, become vulnerable if a State's strengths are significantly impacted, turning them into a disadvantage in the area of influence or within their own territory.

Currently, the world is focused on technological developments of all kinds. Crises have transformed it, and therefore, it has had to innovate to survive. This

makes it necessary, for better or worse, to change the way of thinking because the real world is transitioning into the virtual world. From a strategic perspective, AI and big data technologies will enhance relationships between intelligence agencies, enabling them to develop strategic intelligence and counterintelligence tasks that neutralize common threats and protect national interests, thereby increasing control. Regarding operational issues, military intelligence must establish agreements to strengthen its capabilities and resources, aiming to carry out coordinated operations that directly target illegal armed organizations operating within the national territory.

However, it should be noted that without a legal regulation for the use and development of AI, a dangerous gateway could open to a range of criminal activities and serious human rights violations. In this context, it is important to distinguish between the "unintentional" misuse of AI and the "intentional" misuse, such as for terrorist purposes, which threatens national security and defense (Romero, 2019). Therefore, establishing a binding international legal framework to regulate this technology is crucial to mitigate these threats.

In the current landscape of hybrid warfare, using AI to analyze economic, political, and social factors that directly boost combat power will facilitate the comprehensive execution of tasks, help gain a military edge, and therefore neutralize all kinds of threats to sovereignty and national policies. Thus, having these tools enables a cross-cutting approach to operational development that emphasizes the participation of military intelligence.

Finally, AI and big data are instruments that must always depend on the analysis and control of a person, who must determine what is useful and what is not in planning. Therefore, it is also essential that a legal framework be in place to regulate them and provide appropriate advice to safeguard all decisions made when incorporating these technologies.

References

Acosta, A., Aguilar-Esteva, V., Carreño, R., Patiño, M., Patiño, J., & Martínez, M. (2020). Nuevas tecnologías como factor de cambio ante los retos de la inteligencia artificial y la sociedad del conocimiento. *Revista Espacios, 41*(05), 25–32. https://tinyurl.com/35dm93jd

Ahedo Ruiz, J., & Danvila del Valle, I. (2014). Las nuevas tecnologías como herramientas que facilitan la educación. In J. Días-Cuesta (Ed.), *Estrategias innovadoras para la docencia dialógica y virtual* (pp. 25–40). ACCI.

Arcos, R. (2015). Reservas de inteligencia: una comunidad ampliada de inteligencia. *Inteligencia y Seguridad*, (8), 11–38. https://tinyurl.com/yc77ra2d

Barceló, M. (2001). A.I. (inteligencia artificial). *Byte España,* (78), 98–99. https://tinyurl.com/32x36khf

Bonami, P., Piazentini, L., & Dala-Possa, A. (2020). Educación, big data e inteligencia artificial: metodologías mixtas en plataformas digitales. *Comunicar, 65*(25), 43–52. https://doi.org/10.3916/C65-2020-04

Bostrom, N. (2016). *Superinteligencia: caminos, peligros, estrategias*. Teell.

Bravo, G. (2010). El proceso de inteligencia, vigilancia, adquisición de blancos y reconocimiento. *Revismar,* (1), 58–64. https://tinyurl.com/3w85djeu

Chipuxi, V., & Paucar, J. (2020). *Propuesta de un modelo de cadena de suministro basado en tecnología Blockchain* [Bachelor's thesis, Universidad Central del Ecuador]. Repositorio UCE. https://tinyurl.com/yc6t2h4b

Daza, M. (2020). *Grado de conocimiento y nivel de implementación de la tecnología Blockchain en empresas colombianas* [Master's thesis, Pontificia Universidad Javeriana]. Repositorio PUJ. https://tinyurl.com/bdv3w9ys

Fernández, M. (2020). *Tecnología Blockchain en la logística portuaria* [Bachelor's thesis, Universidad de Cantabria]. Repositorio UNICAN. https://tinyurl.com/vhh4ztb3

Galindo, C. (2005). De la seguridad nacional a la seguridad democrática: nuevos problemas, viejos esquemas. *Estudios Socio-Jurídicos,* (7), 496–543. https://tinyurl.com/2vh6a55c

Gutiérrez Abarzúa, H. (2014). El concepto ISTAR: ¿Una herramienta válida para la función de inteligencia de las Fuerzas Militares del siglo XXI? *Revista Fuerzas Armadas*, (230), 55–63. https://doi.org/10.25062/0120-0631.859

Hill, K., & Dance, G. (2020, February 10). Una aplicación de reconocimiento facial ha identificado a víctimas de abuso infantil. *The New York Times.* https://tinyurl.com/2m3tj3yd

Hueso, L. (2019). Riesgos e impactos del big data, la inteligencia artificial y la robótica: Enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo*, (50), 1–37.

Martínez Devia, A. (2019). La inteligencia artificial, el big data y la era digital: ¿Una amenaza para los datos personales? *Revista La Propiedad Inmaterial,* (27), 5–23. https://doi.org/10.18601/16571959.n27.01.

Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Investigación, desarrollo e innovación. *Ciberseguridad,* 10–12. https://tinyurl.com/5xkx5k6b

Navarro Bonilla, D. (2014). El ciclo de inteligencia y sus límites: producción de información. *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol,* (48), 51–65. https://tinyurl.com/58yw8ncj

Orozco, L. E. (2003). *La calidad de la universidad: más allá de toda ambigüedad*. https://tinyurl.com/9rsx47tj

Palomo-Zurdo, R. J. (2018). Blockchain: la descentralización del poder y su aplicación en la defensa. *Boletín IEEE,* (10), 885–904. https://tinyurl.com/2s43yc2y

Pashchuk, Y. (2013). *Medios de implementación de Instar en el sistema de Inteligencia de las Fuerzas de Ucrania*. Universidad Nacional de la Fuerza Aérea (KNAFU). https://tinyurl.com/y5d6ujv8

Pérez, J. (2023). Ramón López de Mántaras, experto en inteligencia artificial: "La IA sola no resolverá absolutamente nada. Serán los humanos". *Diario El País,* https://tinyurl.com/52vwc9m2

Romero, S. (2019). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. *Revista de la Escuela Superior de Guerra Naval del Perú ESUP, 16*(1). https://tinyurl.com/56a4vwah

Rosales Pardo, I. R. (2005). La inteligencia en los procesos de toma de decisiones en la seguridad y defensa. *Cuadernos de Estrategia,* (130), 39–64. https://tinyurl.com/2u9yczne

Rubio, I. (2018, November 15). Necesitamos la inteligencia artificial para sobrevivir como especie. *El país*. https://tinyurl.com/4yy47rz2

Sarda, J. M. (2016, September 22). *En la inteligencia de un Estado se pueden mostrar varios tipos de amenazas a las estructuras organizacionales del mismo que pueden afectar los procesos de información. Toma de decisiones y manejo de amenazas*. Universidad de Valencia.

Sossa Azuela, H., & Reyes Cortés, F. (2021). *Inteligencia artificial aplicada a robótica y automatización*. Marcombo; Alfaomega.

U.S. Department of Defense. (2012). *DOD Directive 3000.09, "Autonomy in Weapon System"*. https://tinyurl.com/466nkb9b

Valencia Bermúdez, M. P., Puerta Bohada, J. S., Collazos Ballén, N., Urrea, D., & Cañas C. (2019). Influencia de la cuarta revolución industrial en Colombia. *Punto de Vista, 10*(16), 1-18 https://doi.org/10.15765/pdv.v11i16.1419

Valls, M. (2018). La inteligencia artificial y su encaje en las estrategias de seguridad nacional. *Boletín IEEE*, (12), 472–485. https://tinyurl.com/4y38fw4c

Vigevano, M. (2021). Inteligencia artificial aplicable a los conflictos armados: Límites jurídicos y éticos. *Arbor, 197*(800), Artículo e600. https://tinyurl.com/s73rua84

EDITORIAL ESDEG

Chapter 10

The Geopolitics of Organized Crime in World Order 2.0: A Case Study*

DOI: https://doi.org/10.25062/9786287818408.10

Pedro Alexis Ortiz Celis
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Fabio Albergaria
Escola Superior de Defesa

Abstract: This chapter aims to provide a broad analysis of the actors and factors involved in instability operations in World Order 2.0. It also examines and identifies specific characteristics and elements that contribute to the development of instability operations, especially those originating in the Northern Andean Security Subcomplex, and how their externalities affect the international system at a regional level. To achieve this, transnational illicit activities are contextualized as a factor that generates instability, and the role of the Andean-Amazonian region in these dynamics is also explored.

Palabras clave: threats; instability factors; transnational illicit activities; instability operations; security.

* 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.

Pedro Alexis Ortiz Celis
Lieutenant Colonel in the Colombian National Army. Master's in Strategy and Geopolitics, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Master's in Military Arts and Sciences, WHINSEC, USA. Specialization in Management and Leadership of Military Units, National Army Arms and Services College. Specialization in Military Resources Administration for National Defense, Army Logistics College. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: **pedro.ortizce@buzonejercito.mil.co**

Fabio Albergaria
PhD and postdoctoral fellow in International Relations and postdoctoral fellow in Latin American Studies, University of Brasilia. Master's in Sustainable Development. Assistant professor, Escola Superior de Defesa (ESD), Brazil. Email: **fabio.queiroz@defesa.gov.br**

APA Citation: Ortiz Celis, P. A., & Albergaria, F. (2025). The Geopolitics of Organized Crime in World Order 2.0: A Case Study. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 209-232). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.10

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

In the traditional sense, the international system refers to the collection of political entities that maintain regular relations with each other and are ultimately vulnerable to involvement in a widespread war (Aron, 1963). However, nearly thirty years after the end of the Cold War and the bipolar rigidity, many uncertainties still exist about the nature of the current international system.

Therefore, in this complex system where the fates of its actors are interconnected within a context conducive to diverse connections, we are led to a scenario that remains unpredictable and open to new possibilities. Among these is the task of establishing a security agenda better suited to the new times and priorities of international relations, even in South America.

In other words, as Queiroz (2022) points out, overlapping threats from both outside and within a region require coordinated responses to safeguard the interests of those affected by externalities caused by issues like environmental degradation, climate change, conflict-induced forced displacement, radicalization and terrorist financing, large-scale cyberattacks, deliberate violence by non-state actors, and, for this research, the spread of failed States and organized crime.

This interpretation is based on Haass (2008), who describes the current international system as "the age of nonpolarity," a world where no single group of States dominates. Instead, numerous actors, many non-state and possessing substantial power, influence the global landscape. In this context, Haass characterizes nonpolarity—evident in this spread of power—as the defining feature of the 21st-century international system; he describes it as a major shift away from the traditional systemic views of the recent past.

In Haass's nonpolar system, state power is weakened as cross-border flows of various kinds (drugs, information, weapons, goods, people) happen beyond

the government's knowledge and control. As a result, these flows enable other actors to take actions in spaces that were once the exclusive domain of the State. Therefore, the nonpolar world could lead to a dangerous situation, prone to "nonpolar disorder," with growing threats and vulnerabilities.

From another perspective, Viola and Leis (2007) argue that we have lived within what they call an international system dominated by market democracies, and that its core structural force is globalization, characterized by the shift from an industrial society to a knowledge-based, information-driven society.

In this scenario, the main state actors that connect free-market economies and democratic regimes define their foreign and defense policies so that they do not pose, relative to any other country in this context, threats to their vital interests. Therefore, it is important to highlight that Viola and Leis (2007) define democratic regimes as those characterized by the existence of the rule of law, free and competitive elections, clear differentiation between government and opposition, alternation in power, individual rights and guarantees vis-à-vis the State, separation of powers, constitutional guarantees for minorities, and protection of society against the possible excessive appropriation of resources by the political class.

Based on this, the authors identify the main threats to the current international security system as: 1) transnational terrorism linked to Islamic radicalism; 2) the proliferation of weapons of mass destruction; 3) States that actively challenge this security framework, such as Iran and North Korea; 4) States that partially challenge this system and have significant power resources, like China and Russia; and 5) transnational crime.

In turn, Zakaria (2008) emphasizes that the dynamics of the international system are shaped by what he calls the "rise of the rest." While, in his view, the world remains unipolar at the political-military level under American dominance, there is a notable shift in other areas—industrial, economic, financial, social, and cultural—favoring other powers, especially China and India, as well as non-state actors. This suggests an overlap of elements of unipolarity and multipolarity.

In short, these readings confirm the conclusions of a 2004 report by a commission of experts appointed by Kofi Annan, then Secretary-General of the United Nations (UN), which identified six main sources of threats or challenges to the contemporary security agenda: 1) wars between States; 2) violence within States, civil wars, large-scale human rights violations, and genocide; 3) poverty, infectious diseases, and environmental degradation; 4) nuclear, radiological, chemical, and biological weapons; 5) terrorism; and 6) transnational organized crime (TOC).

These approaches, which represent only a small sample of the efforts to interpret international relations in the first decade of the 21st century, indicate the reorganization of forces in the modern international system at various levels of analysis, from the systemic to the regional. And, within that system, transnational crime, as we have seen, helps create scenarios of instability whose external impacts are not fully understood in terms of their ability to cause disruptions.

In other words, as Zakaria (2008) rightly observes, this new global reality, profoundly changed by the inclusion of unconventional issues on the international security agenda and the increasing involvement of non-state actors, emphasizes the urgent need "to construct a new approach for a new era, one that responds to a global system in which power is far more diffuse than ever before and in which everyone feels empowered." We are moving away from a bipolar and dangerous, yet predictable, world based on the known risk of a contest between two adversaries, toward a different one with unclear boundaries. This new world presents old risks but also offers unprecedented opportunities (Queiroz, 2013). It is World Order 2.0!

The above becomes clearer when we also consider the perspective of Buzan and Waever (2003), who state that, in the post-Cold War era, the regional sphere is the space where the dynamics of insecurity—resulting from the interactions between various actors and sectors—are most clearly and immediately evident. Regarding South America, the same authors note that while the Southern Cone has pursued integration and strengthened mutual trust with Mercosur as its foundation since the 1990s, the Andean-Amazonian North—our area of focus—still carries lingering remnants of past conflicts and rivalries, in a scenario worsened by endemic structural issues.

Thus, in a time of increasing instability and many uncertainties about the future of the global order, we uphold this direct relational hypothesis: the more transnational the illicit activities are, the higher the chance that the so-called Northern Andean Security Subcomplex, especially the Andean-Amazonian area, will become a dangerous zone characterized by fragility in the rule of law and the economy of illegal activities.

Methodology

To gather the data needed to test the hypothesis, we used desk research, a method that involves a thorough review of published materials related to the study subject. For this purpose, we examined documents from relevant official public sources

(such as ministries, Armed Forces, and intelligence agencies) as well as media outlets like newspapers, magazines, and specialized websites.

Regarding the research ontology, we selected instability dynamics within the framework of World Order 2.0 as a key parameter to define the universe of analysis. Additionally, we employed the descriptive model of Regional Security Complexes (RSCs) in general and Regional Security Subcomplexes (RSSs) in particular, which are explained in the section dedicated to the conceptual framework.

Therefore, this case study employed a qualitative methodology to answer the research questions. An analysis was conducted to provide descriptive (how) and causal (why) inferences about the geopolitics of organized crime in the northern tri-border region (Brazil-Colombia-Peru), which we understand as part of an ongoing Andean-Amazonian Instability Arc.

This work is also an exploratory study, given the nature of the research subject, which is a rare topic in the literature, especially in its interpretation through the chosen conceptual frameworks.

Finally, to answer the research question and determine whether the proposed hypothesis is supported or refuted, a causal chain is used that outlines the variables chosen for the study, which are: 1) the independent variables, those that influence other variables and are useful for explaining the characteristics or behavior of the study object; 2) the dependent variable, which the researcher aims to explain based on the influence of one or more independent variables; and 3) the intervening variable, which, in a causal sequence, is positioned between the independent and dependent variables, helping to explain how the former affects the latter.

World Order 2.0

According to Richard Haass (2017), we no longer live in World Order 1.0, which was based on the exclusive protection and privileges of States since the Peace of Westphalia (1648), but instead in an integrated and interdependent world, or, in other words, World Order 2.0. In this scenario, nearly everything—including threats and people—can reach anywhere, creating complex interdependent relationships. Therefore, in World Order 2.0, "what goes on inside a country can no longer be considered the concern of that country alone" (Haass, 2017, p. 2), meaning that overlapping threats from outside and within a given region or country require coordinated responses to protect the interests of those affected by the externalities.

The situation involves illicit activities infiltrating numerous state institutions, including those in South America, facilitated by TOC. This phenomenon is supported by some elements that define World Order 2.0, such as trade liberalization, the movement of goods and people, technological progress, and the transit of non-state actors who promote these products—factors that create cycles of instability and pose challenges to the rule of law, as discussed in the following section.

The international landscape is shaped by interdependence, a phenomenon that has been critically reflected in the various threats currently facing nations. As noted, although war in its traditional Westphalian form is declining, it has not prevented terrorist acts such as the attacks in New York and Washington, D.C., on September 11, 2001, from happening. This shows "a growing deterritorialization of violence and a significant secularization of the international agenda. It has also gained renewed importance with the large terrorist activities carried out by the Islamic State in the Middle East and, most notably, in Europe" (Riquelme et al., 2019).

It is important to remember that traditional and interstate conflicts still exist in the global environment, phenomena that are examined through various security dilemmas in Asia and the Middle East, such as the unstable and complex situations involving the two Koreas, Japan and China, China and Russia, Pakistan and India, and India and China (Tokatlian, 2012). These conflicts are also evident in the current complex and critical crisis between Russia and Ukraine, which began on the morning of February 24, 2022, when Russian President Vladimir Putin ordered his troops to bomb and invade the neighboring country.

In this environment of interdependence between regional frameworks, it has been observed that state and non-state actors face numerous difficulties in addressing the wide range of demands and challenges brought about by globalization, especially regarding security issues. It is important to note that new threats are emerging, with transnational illicit groups, environmental degradation, and natural disasters becoming increasingly significant. In Latin America, security remains a top priority for both societies and governments, which is why studying and analyzing TOC in this region is considered so important.

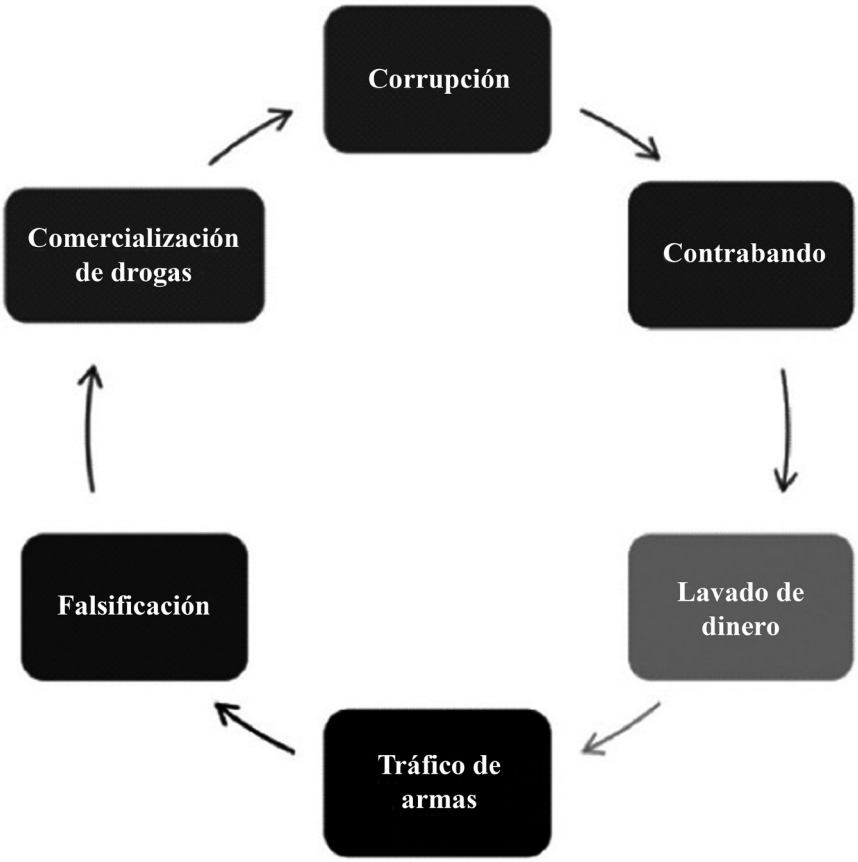
Transnational Organized Crime in World Order 2.0

Organized crime is involved in various aspects of society. We suggest that these relationships extend beyond citizens and the government, even across borders, and have a significant impact on security. As the Organization of American States points out (OEA, 2003),

> […] the concept of security, which was once framed primarily in conventional military terms, has now had to broaden its framework and take into account a variety of threats: international terrorism, drug and illegal arms trafficking, human trafficking, money laundering, institutional corruption, and organized crime. In some countries, poverty, disease, and environmental degradation contribute to the deterioration of human security. (p. 106)

This happens through the creation of a vicious circle, as Cuervo (2018) suggests, which forms networks of interdependence capable of structurally undermining countries and/or regions (Figure 1).

Figure 1. *The Modus Operandi of Transnational Crimes*



Source: Cuervo (2018).

Certainly, the instability caused by organized crime, which still persists, is a major concern for political development, especially when society believes that worsening security is only due to economic decline (Wielandt, 2007).

The actions of organized crime do not distinguish between national political systems, between actors and their relationships, much less do they recognize or take into account an international political system, where the variety of actors, the lack of laws regulating their interactions, the significant asymmetry of power, and the transnational nature of their actions tend to increase and become harder to interpret. To support this view, it should be noted that the world order and its actors, mechanisms, and systems can seem somewhat abstract if they are not analyzed from a global perspective, and a causal analysis is not constructed in a way that bridges the gaps between nations involved in developing illicit activities (Parrao, 2018).

Transnational crime usually involves organizations or individuals that operate sporadically and use self-regulating mechanisms. In his article, Szeinfeld (2012) states that the goal of this type of threat is to make money or gain commercial profit through partly or fully illegal means.

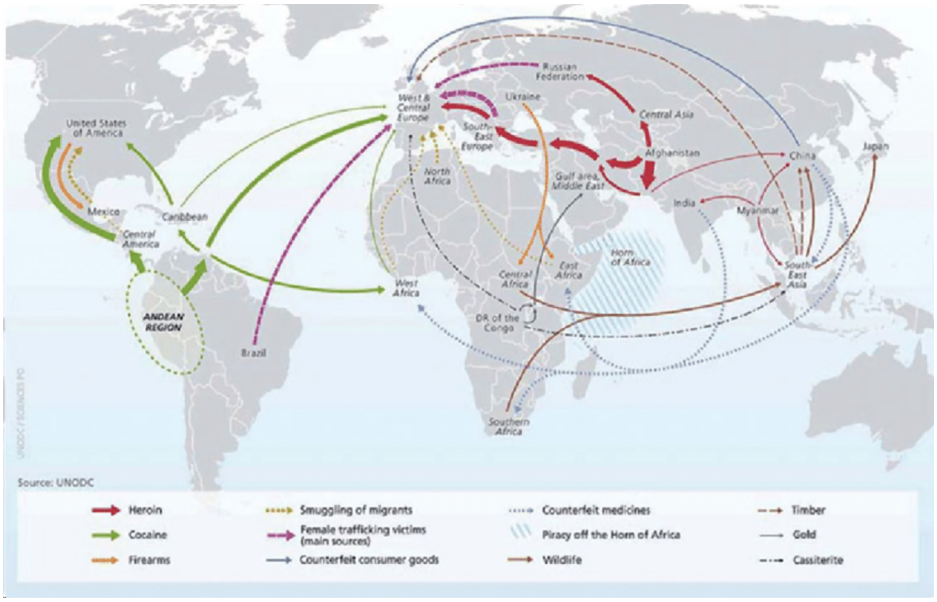
Therefore, William Werner (2009) categorizes TOC from three perspectives: 1) political, which views organized crime as a result of weakened state structures; 2) social, which emphasizes sociocultural factors as determinants of TOC methods; and 3) economic, which explains the methods based on the demand for illegal goods and services.

In its own turn, World Order 2.0 emerged at the end of the last decade of the 20th century, a period when new ideas and technologies were introduced into politics, commerce, and the global economy. In this context, a new organized crime structure has emerged in cyberspace, an electronic marketplace where illicit goods and services are sold, and sometimes businesses are infiltrated, all without physical contact between supplier and customer. This dynamic, in turn, makes fighting criminal networks a more complex task, especially in regions like the Andean-Amazonian area, where notable state weaknesses threaten regional stability (Figure 2).

Therefore, in World Order 2.0, responses must be coordinated and integrated across the broadest range of action spheres, at both the intra- and inter-state levels, to maximize the ability to create lasting impacts in pursuit of: 1) efforts to modernize and fight corruption; 2) reducing illicit finance; 3) strengthening regional multilateral anti-corruption frameworks; and 4) enhancing diplomatic

engagement to achieve anti-corruption policy goals, which will only be feasible through intersectoral governance, as we suggest below.

Figure 2. *Transnational Organized Crime Market Flows*



Source: United Nations Office on Drugs and Crime (2010, p. 2).

These events, along with many others that will be analyzed later, have led criminal actors to adopt this development and escalate their actions, making it clear that the history of crime, like that of politics and the economy, has evolved.

Considering the challenges arising from the new world order, the reconfiguration of threats, and the ongoing conflicts in South America due to the instability caused by TOC, it is essential to analyze which actors are primarily responsible for these threats, to eventually identify them and develop the most effective strategy to counter them.

Research Universe and the Theory of Regional Security Complexes

In today's world, the issue of international security has become more significant globally, not just in politics but also within various academic circles, which have

called for expanding and deepening it to better suit the complex nature of an order filled with many uncertainties. In this context, the Copenhagen Peace Research Institute (COPRI), established in 1985, stands out. It has contributed significantly by introducing the concept of *securitization,* which expands the idea of security and is based on the premise that threats are not only military but also can originate from political, environmental, economic, and social spheres, each with its own unique dynamics.

For the Institute's experts, the regional level has greater visibility because, beyond the bipolar rivalry context, local powers have more room to maneuver, and regional differences—particularly States' concerns about their neighbors' interests and intentions—have become easier to distinguish from the systemic security agenda of the Cold War.

In this regard, another original and important contribution of this Institute is the descriptive model of RSCs. Its basic premise, as stated, is that, in the post-Cold War world, international relations in the field of security lead to greater autonomy and importance of the dynamics occurring on a regional scale.

The main idea is that an RSC exists when perceptions and concerns about the security of people within a geographically connected area are so linked that these issues cannot easily be analyzed or solved separately. According to Buzan and Waever (2003), South America fits this situation, and for this research, the Andean-Amazonian arc is also relevant.

Thus, RSCs are social constructs based on the interdependence relationships established between their units through interactions of material variables and ideas, such as beliefs, identities, material capabilities, borders, power distribution/perception, and anarchy. These factors give the model greater analytical depth. Within this framework, South America has two subregional structures: the Southern Cone Security Subcomplex, which includes Argentina, Bolivia, Brazil, Chile, Paraguay, and Uruguay, and the Northern Andean Security Subcomplex, comprising Peru, Ecuador, Colombia, Venezuela, and Guyana. In this context, Brazil acts indirectly as a connecting country between the two subcomplexes because of its size and because it is both Amazonian and Andean.

The South American Regional Security Complex

South America has advanced in its security cooperation efforts through the creation of the Union of South American Nations (UNASUR), which now forms a regional bloc including all South American countries. Key reasons for its

establishment include the gradual decline in the effectiveness and consensus of the current inter-American system, as well as the significant weakening of traditional regional integration centers in South America: the Andean Community (CAN) and the Southern Common Market (MERCOSUR) (Cujabante, 2012).

Thus, South America looked for multilateral regional options to fight and counter transnational criminal groups while also strengthening unity and cooperation among countries, as was shown on other continents. UNASUR gained the reputation of a new regionalism, setting itself apart from those that appeared in the 1970s. In this regard,

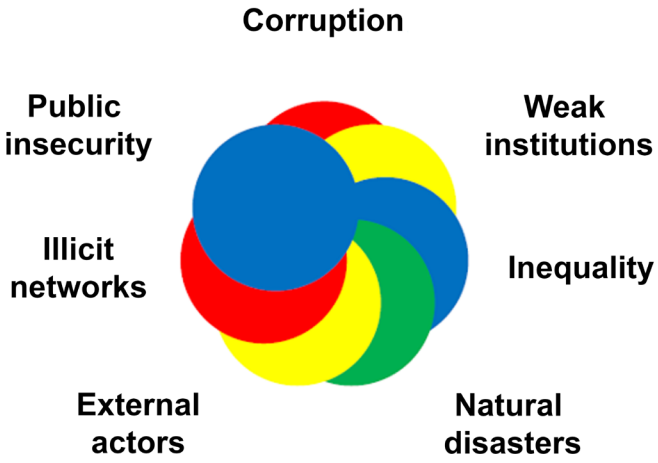
> […] On December 8, 2004, the South American Community was established. Following the Margarita Island Summit in April 2007, its name was changed to its current name, UNASUR, which was formalized in the Treaty of Brasilia, signed on May 23, 2008. (Cujabante, 2012, p. 70)

UNASUR plays a vital role in regional security, as shown by an analysis of the security threat actors present in this geographic area since the end of the Cold War. In this context, as noted in the definition of World Order 2.0, South America is immersed in an environment where States no longer act alone, and the influence of multiple transnational actors is clear. In response to these global changes, the concept of security has evolved in at least three ways (Hurrell, 1998, as cited in Cujabante, 2012):

> 1) The State is no longer the only reference point for security; instead, it must include individuals, communities, humanity as a whole, people in general, the biosphere, and others. 2) Any meaningful analysis of security must consider a wider range of threats, including those from environmental destruction, economic vulnerabilities, and the breakdown of social cohesion. 3) The responsibility for providing security falls not only on the State but also on international institutions and non-governmental organizations. (p. 26)

Therefore, it is evident that among the factors contributing to violence and territorial instability—such as terrorism, organized crime, drug trafficking, corruption, arms trafficking, extreme poverty, and natural disasters—these are beginning to become more prominent, especially in what we refer to as the Andean-Amazonian Arc of Instability. Consequently, the subregion faces a series of interconnected factors that form a vicious cycle, as shown in Figure 3.

Figure 3. *Vicious Cycle of Andean-Amazonian Threats*



Source: Own elaboration.

Therefore, regarding the specific issue of South America, the threats that arise are shaped by particular geographic conditions, natural resources, the political environment, and, in some cases, historical processes, among other factors. In short, new actors are committing crimes in border areas and transnationalizing their actions, for example, through transnational migrations driven by violence and the illegal trade of weapons, drugs, people, environmental resources, and more.

The actions of illicit groups along the northern tri-border (Colombia, Brazil, and Peru)—which we recognize as a key part of the Andean-Amazonian Arc of Instability—have been changing over time. At first, they only aimed to show local control. But as they grew, they first demonstrated their strength and took on more aggressive territorial control within these countries. Eventually, they moved into a realm of criminal transnationalization, occupying large cross-border areas, as is the case now.

Identifying these criminal groups was challenging because the State showed little interest in the issue; it was not a priority in its government policies, and it was believed they did not threaten its stability. As a result, TOC became rooted in gray areas like the Amazonian Trapeze, where government neglect created empty spaces that allowed their expansion and growth in power. To achieve this, these criminal organizations infiltrate institutional structures to control border crossings and strengthen their influence. The truth is, as Procópio (2007), Cuervo (2018), and Queiroz (2022) pointed out, that the Andean-Amazonian region has increasingly

played a significant role in the network of exchanges and cooperation among organized crime groups.

The Northern Andean Security Subcomplex

While the Southern Cone has chosen the path of integration and building mutual trust, the Northern Andean Security Subcomplex, in contrast, still carries underlying remnants of a history of conflict and rivalry. This situation is worsened by structural issues that go beyond the borders of the Subcomplex. Resentments from territorial disputes of the 19th and 20th centuries involving Peru, Bolivia, Chile, Venezuela, Colombia, Guyana, and Ecuador still linger (Buzan & Waever, 2003).

Furthermore, the significant political and institutional weaknesses present in the Subcomplex are among the main reasons for the power vacuum that characterizes the region. This vacuum has been filled by organized crime networks, which are responsible for the subregion's integration into the competitive global illicit market. Therefore, given the systemic weaknesses common to the Andean States, the state-building process is a vital aspect of security, an essential element for maintaining regional order in a context where the presence of weak or failed States increasingly plays a dominant role in security and defense.

This pattern of endemic instability was also emphasized by the Regional Security Cooperation Program (RSCP), which in a study identified it as one of the serious problems the region faces and one that requires special attention, since "the Andean States have experienced [...] processes of deinstitutionalization, rampant government corruption, weak economic growth, political irrationality, centrifugal tendencies, and even the weakening of national viability" (Programa de Cooperación en Seguridad Regional [PCSR] & Friedrich Ebert Foundation, 2007, p. 3).

As is typical in Latin America, transnational crime is heavily involved in the North Andean RSC and, therefore, in the Andean-Amazonian Arc. The CRS serves as a route for production, consumption, and transit that has contributed to the development of strategic points used by criminal gangs, aiding their operations and hindering efforts to reach them through legal means.

This causes instability across various areas of state action, including the political, military, economic, environmental, and social spheres. In this context, it is worth noting the thesis by Meneses Castillo (2016), which discusses the main transnational crimes and their classifications. It also provides representative scenarios, with a focus on South American countries, where common factors

include the presence of gray areas, extensive borders, and weak security and defense systems.

Then, as researchers point out, the threats and vulnerabilities in the Andean-Amazonian Arc form a complex and widespread agenda, marked both by transnational issues related to the endemic practice of illegal activities and by internal problems stemming from deep structural weaknesses in the region's countries. Some of these are prototypes of failed States, where "institutions have ceased to function or have been co-opted to serve private, often illicit, interests" (Naim, 2005, p. 57).

Transnational Crimes in the Northern Andean Security Subcomplex: An Arc of Instability Based on Organized Crime Networks?

Security in the Northern Andean Security Subcomplex is a top priority for the societies and governments of the Amazon Basin countries. It is a key topic of study and concern due to the ongoing development of TOC, which is seen as an illegal activity that causes instability and is connected to offenses committed in more than one country, as well as offenses that happen in one country but are carried out by groups operating across multiple nations (Riquelme et al., 2019, p. 10).

In the region, new transnational actors involved in extensive TOC networks are actively engaged. Lucía Dammert (2012) observes that "in matters related to public security—such as the perception of crime, the occurrence of violent crimes, easy access to weapons, violent protests, and assessments of the police—the region is characterized by a sense of insecurity" (p. 14). Consequently, criminal violence has become one of the most significant challenges confronting governments in the area.

These links with international illicit networks and internal co-optation in border cities, for example, facilitate the formation of multiple symbioses between the contraband economy and organized crime culture, harming human security in Amazonian democracies. Because of this, from a public security perspective, the Northern Andean Security Subcomplex is one of the most violent regions worldwide, representing a major challenge for Latin American democracies.

These concerns become clear when understanding that this geographic region has large areas of porous borders, a situation that encourages organized crime, especially related to drug trafficking, arms smuggling, human trafficking, and illegal immigration. This also explains certain bilateral tensions (Riquelme et al., 2019).

Murillo (2016, as cited in Rodríguez & Nieto, 2020) examines and analyzes how organized crime groups impact the political dynamics of countries in the region, providing evidence that illicit activities have directly influenced the exercise of political power. This phenomenon is reinforced by the lack of governability, which is reflected in the fragility and weakness of various affected States, which "have ceased to address the needs of many social sectors. These criminal groups have exploited this situation to gain legitimacy among these sectors of society" (Rodríguez & Nieto, 2020, p. 265).

One of the biggest transnational crimes in the Northern Andean Security Subcomplex is drug trafficking, which is why this scourge should be considered the main—though not the only—source of income for these organizations. In this regard, it is perhaps the most serious threat to security, the principles of the State, and the relations between affected nations. It is important to note that the activities of these criminal groups have significant consequences, including environmental damage, institutional corruption, and societal decline (Rodríguez & Nieto, 2020).

In this regard, Tokatlian (2014) notes that an important work by Edwin H. Stier and Peter R. Richards from 1987 (*Strategic Decision Making in Organized Crime Control: The Need for a Broadened Perspective*) offers a clear framework for observing and assessing how organized crime develops through three distinct phases: predatory, parasitic, and symbiotic. In the "predatory" phase, territory and control are essential. TOC must influence and dominate one or more illicit goods within a secure physical space; it must identify routes for transporting these goods; have access to markets to sell its products; and ensure personal protection.

In the "parasitic" phase, the political and economic influence of crime grows significantly. This stage not only shows the increased reach of organized crime but also three concerning trends: its legitimization, proliferation, and democratization. The author emphasizes that during this phase, organized crime shows notable corruption in both the public and private sectors. In the "symbiotic" phase, the power of criminal activity becomes more evident, while the political and economic systems become as dependent on organized crime as they are on the established structure. The line between what is lawful and unlawful, what is legitimate and illegitimate, becomes unclear, and the rule of law itself is weakened (Tokatlian, 2014).

This analysis indicates that in the Northern Andean Security Subcomplex, where the TOC is highly developed, these stages must be identified and analyzed separately to guide intervention and the development of policies and practices aimed at reducing organized crime. Neglecting to do so will allow the next phase to progress. This is crucial for understanding issues such as drug trafficking.

The Andean-Amazonian Arc of Instability: A Case Study of the Northern Tri-Border Between Brazil, Colombia, and Peru

The premises presented so far suggest that, regarding the Andean-Amazonian Arc, international drug trafficking flows across the weak borders characteristic of World Order 2.0. This shows that the fragility of the rule of law is a major cause, with the rise in local social violence being one of its effects (Pinto & Rodríguez, 2020; Procópio, 2010; Queiroz, 2022). As will be discussed later, the tri-border or Amazonian Trapeze—the area formed by the cities of Tabatinga (Brazil), Leticia (Colombia), and Santa Rosa de Javari (Peru)—serves as a key distribution route for various illicit drugs used in global trafficking networks.

In addition to what has been mentioned, it is important to note that the Brazilian part of the region is strategically close to drug-producing areas in Colombia and Peru. This makes it vulnerable to the influence of drug cartels, mainly Colombian, which aim to move their production to supply both national and international routes along the Solimões River to Manaus, and from there to other parts of the country and the world (Araújo, 2018).

The northern tri-border area between Colombia, Brazil, and Peru, therefore, presents numerous issues related to fighting crime, where TOC is widespread. In this context, the idea that, in this region, TOC undermines the political and economic foundations of States is relevant, "fueling vicious cycles of insecurity, as members of criminal networks can cooperate with corrupt governments, paramilitary groups, or terrorist organizations" (Gobierno de España, n.d., p. 1, as cited in Rodríguez & Nieto, 2020, p. 266).

This situation results in a population that generally struggles to meet basic needs due to the fragility of the region's institutional structures, which led Rebeca Steiman (2002) to describe the northern tri-border area as the "periphery of the periphery."

This is an area where TOC, as we have repeatedly stated, emerges, marked by insecurity, unrest, and societal decline, demonstrating the convergence of multiple institutional failures. Therefore, "the permanent presence of illegal armed actors in this border region is largely due to the absence and weak presence of the Colombian State in its peripheries" (Trejos, 2015, p. 1), as well as the States of Brazil and Peru in these three main "twin cities": municipalities divided by a border—whether a river or territory—that are closely linked through daily economic and cultural activities. For these reasons, this interaction can have practical

consequences for the sovereignty of States over their territories, a situation worsened by the rise of a drug financial market controlled by trafficking networks, which significantly impacts the financial and social life of the Amazonian Trapeze (Pinto & Rodríguez, 2020; Steiman, 2002).

It must be recognized that the large size of the northern tri-border area makes it hard for the government to effectively oversee, control, and manage both the cross-border flows and the movements within the country. This creates opportunities for crime, which manifests as the political and social decline of institutions in the region, covering an area of 1,632 km² (Figure 4).

Figure 4. *The Northern Tri-Border between Colombia, Peru, and Brazil*

Source: Instituto Mayor Campesino (2015).

Besides what has been mentioned, Fernández (2016, as cited in Sampó, 2018) points out that a true network of illegal groups with advanced logistics and operations has emerged, amplifying effects never seen before. This is due to the strong ability of these groups to control and manage in the region, along with the lack of equipment and personnel from States to effectively enforce their sovereignty.

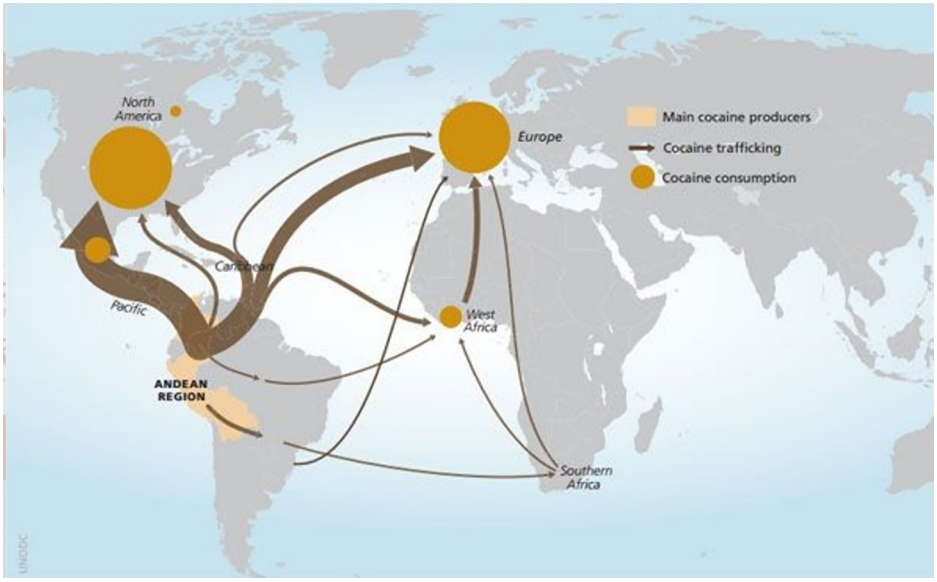
The most significant and largest crime in the tri-border region, as the data indicates, is drug trafficking. It is an area where international illegal networks centered on drug trafficking exist and continue to expand, mainly due to the lack of state presence and, certainly, law enforcement (Trejos, 2015). Therefore, the Amazon is considered crucial for drug trafficking because of its numerous waterways, most of which flow into the Amazon River in Brazil and from there into the rest of the world.

According to data from the United Nations Office on Drugs and Crime (UNODC) *World Drug Report,* published in 2019, the cocaine market functions as an economic engine for the Amazonian Trapeze, with Colombia and Peru as its main producers. Together, these countries experienced a 78.8% increase from 2010 to 2017 (UNODC, 2019, p. 76). Besides reaffirming that the Solimões River route is one of its key outlets for production, it states that Brazil has become a major consumer market in recent decades, not just a transit route for this cocaine.

As Cuervo (2018) notes, this is because of the lack of alternative instruments and insufficient control in the border area, since the three countries do not have the necessary security cooperation to stop or reduce illicit activities. It is troubling that smuggled goods can cross borders freely via roads, boats, planes, and other transportation methods.

This confirms that the Andean-Amazonian region, located on the northern tri-border, is a dangerous zone of instability experiencing rapid development within the framework of World Order 2.0 (Figure 5). It is also known as a route for illicit goods, particularly cocaine, a key Amazonian product with high added value, which remains one of the most urgent challenges for strengthening governance in security and defense.

Figure 5. *Cocaine Flow Routes from the Northern Tri-Border*



Source: O Estado Net (2017).

Conclusions

World Order 2.0 is a tangible and recognizable reality, just like all the external factors caused by complex interdependence relationships, which are seen as potential sources of regional instability. While globalization has undeniably brought benefits such as improved information exchange, more connections, and expanded trade opportunities, criminal networks have exploited this situation to reproduce illicit trafficking chains involving arms, people, and drugs, mainly (Pinto & Rodríguez, 2020). As a result, the illegal economy has become a challenge that surpasses the capacity of the States within the South American Security Complex and is viewed as a shared problem that all must confront.

Specifically, this chapter examined the Northern Andean Security Subcomplex overall, and more specifically, the Andean-Amazonian Arc of Instability, which is emerging to strengthen organized crime networks in the northern tri-border area between Brazil, Peru, and Colombia.

Before drawing conclusions, it is crucial to consider the methodological limitations of this study. On one hand, the lack of data, especially quantitative data, has prevented us from establishing definitive correlations related to the hypothesis. On the other hand, the qualitative inferences collected suggest causal relationships between the variables examined: the dynamics of instability in the tri-border (dependent variable), the levels of fragility of the rule of law, and the geopolitics of the criminal networks operating within the Security Subcomplex linked to the illicit economy (independent variables).

So, what do the descriptive (how) and/or causal (why) inferences demonstrate? The exponential rise in illicit activities in this region, driven and fueled by organized crime, has negatively affected the relationship between Colombia, Peru, and Brazil across multiple sectors, from the economy to security and defense, creating vicious cycles of systemic instability.

Thus, it is important to emphasize the following partial conclusion: the extent of transnational crime development in the local context of the northern tri-border region promotes the growth of the illegal economy. Since many people seek their livelihoods in the informal sector, there is direct recognition and even sympathy for those involved in illegal and informal economies. This has implications for global illegal activity networks reaching parts of Asia, Africa, and Europe, considering the strategic geographic position of the Andean-Amazonian Arc.

With transnational illicit activities confirmed as direct causes of disruptive externalities, it is important to strengthen coordinated, polycentric cooperation between neighboring countries to address this threat and disrupt production and consumption chains, thereby countering the sources of instability that challenge, among other actors, the Armed Forces.

Although the rule of law is fragile, partly due to an economy increasingly based on illicit activities—as this case study suggests—collaborative efforts are expected to encourage interactions among multiple government agencies and civil society to establish and enforce rules in this specific area. In other words, we see polycentric governance mechanisms as some of the best ways to achieve collective and effective responses to the harmful disruptions caused by organized crime.

Finally, the analysis supports the direct relational hypothesis that the more transnational the activities of illicit operations, the higher the likelihood that the Northern Andean Security Subcomplex, particularly the Andean-Amazonian area, will structurally develop into an arc of instability due to the weakness of the rule of law and the economy of illicit activities.

References

Araújo, T. (2018, October 3). Terra sem lei: Como abandono da Tríplice Fronteira amazônica ajuda o narcotráfico no país. *Sputniknews.* https://tinyurl.com/yc3kz3pr

Aron, R. (1963). *Paz y guerra entre las naciones.* Revista de Occidente.

Buzan, B., & Waeber, O. (2003). *Regions and powers: The structure of international security.* Cambridge University Press.

Cuervo Ceballos, G. (2018). El crimen organizado transnacional como una amenaza híbrida para la Triple Frontera (Argentina, Paraguay y Brasil). *Revista Científica General José María Córdova, 16*(23), 43–61. https://doi.org/10.21830/19006586.304

Cujabante Villamil, X. A. (2012). Unasur: ¿Hacia la consolidación de un complejo regional de seguridad? *Revista Científica de Estudios en Seguridad y Defensa, 7*(14), 78–16. https://doi.org/10.25062/1900-8325.191

Dammert, L. (2012). *Seguridad ciudadana en el Perú: las cifras del desconcierto.* Corporación Andina de Fomento.

Haass, R. (2008). The age of nonpolarity: What will follow U.S. dominance. *Foreign Affairs, 87*(3), 44–56. https://tinyurl.com/3mj4xz6b

Haass, R. (2017). World order 2.0: The case for sovereign obligation. *Foreign Affairs, 96*(1), 2–9. https://tinyurl.com/mphmmfr2

Instituto Mayor Campesino (2015). *Migrantes forzados en la Amazonía: una selva que refugia.* IMCA https://tinyurl.com/z8rac2dw

Meneses Castillo, A. L. (2016). *Crimen transnacional en América del Sur y Unasur* [Master's thesis, Universidad Militar Nueva Granada]. Repositorio UNIMILITAR. https://tinyurl.com/37beadt2

Naim, M. (2005). *Ilícito: Cómo el contrabando, los narcotraficantes y la piratería desafían la economía global.* Debate.

O Estado Net. (2017, April 1). *O narcotrafico ameacador.* https://tinyurl.com/mzetx69j

Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC]. (2019). *Informe Mundial sobre las Drogas 2019*. https://tinyurl.com/yzjvhcem

Organización de Estados Americanos [OEA]. (2003). *Conferencia Especial sobre Seguridad* [Report of the Rapporteur of the Special Conference on Security]. https://tinyurl.com/4w5w6tff

Parrao, I. (2018). El orden mundial: Cuatro perspectivas teóricas y sus implicancias en el estudio de la realidad contemporánea. *Artigos Estratégicos, 4*(1), 33–44. https://tinyurl.com/3n8y2tet

Pinto, E. M., & Rodríguez, D. (Eds.). (2020). *Crimen organizado transnacional: Fronteras y actores en el hemisferio.* Sello Editorial ESDEG; Planeta. https://doi.org/10.25062/9789584288936

Procópio, A. (2007). *Subdesenvolvimento sustentável.* Juruá.

Procópio, A. (2010). *Diplomacia e desigualdade.* Juruá.

Programa de Cooperación en Seguridad Regional [PCRS] & Fundación Friedrich Ebert. (2007). *Integración, seguridad y conflictos en la subregión andina.* ILDIS-FES.

Queiroz, F. (2013). Revisitando o conceito clássico de segurança: Dinâmicas, atores e validade analítica. *Intellector, 9*(19), 1–34. https://tinyurl.com/msxu62uf

Queiroz, F. (2022). *La Organización del Tratado de Cooperación Amazónica (OTCA) como herramienta de combate al crimen organizado transnacional en el orden mundial 2.0.* William J. Perry Center for Hemispheric Defense Studies; National Defense University.

Riquelme-Rivera, J., Salinas-Cañas, S., & Franco-Severino, P. (2019). El crimen organizado transnacional (COT) en América del Sur: respuestas regionales. *Estudios Internacionales, 51*(192), 9–33. https://doi.org/10.5354/0719-3769.2019.52781

Rodríguez, A., & Nieto, E. (2020). Estrategia contra el crimen transnacional organizado en la triple frontera Brasil-Perú-Colombia desde la atención social integral de sus habitantes. In O. M. Ramírez-Villegas, H. Cancelado-Franco, & N. R. Cárdenas-Rodríguez (Eds.), *Nuevas amenazas en el siglo XXI: Fronteras y Derechos Humanos* (pp. 261–298). Sello Editorial ESDEG. https://doi.org/10.25062/9789584288950.09

Sampó, C. (2018). Brasil: La re-significación de la violencia como resultado del avance de organizaciones criminales. *Revista de Estudios en Seguridad Internacional, 4*(1), 127–146. http://dx.doi.org/10.18847/1.7.8

Steiman, R. (2002). *A geografia das cidades de fronteira: Um estudo de caso de Tabatinga (Brasil) e Letícia (Colômbia)* [Master's thesis, Universidad Federal do Rio de Janeiro]. UFRJ. https://tinyurl.com/25we5tdk

Szeinfeld, J. (2012). Análisis de las organizaciones criminales trasnacionales en la región. *Revista do Laboratório de Estudos da Violência da UNESP/Marília,* (9), 58–68. https://tinyurl.com/4rw6m4h4

Tokatlian, J. G. (2012). El entorno global. In K Derghougassian (Comp.), *La defensa en el siglo XXI: Argentina y la seguridad regional* (pp. 95–118). Capital Intelectual.

Tokatlian, J. G. (2014, February 11). La Argentina y las etapas del narcotráfico. *La Nación.* https://tinyurl.com/59jdwewy

Trejos, L. (2015). El lado colombiano de la frontera colombo-brasilera: una aproximación desde la categoría de área sin ley. *Estudios Fronterizos, 16*(31), 39–64. https://tinyurl.com/24wyd6ab

United Nations Office on Drugs and Crime (2010). La medición de los mercados y los flujos de productos. https://tinyurl.com/mvjtnu44

Viola, E., & Leis, H. R. (2007). *Sistema internacional com hegemonia das democracias de mercado: Desafios de Brasil e Argentina*. Insular.

Werner, G. C. (2009). *O Crime Organizado Transnacional e as redes criminosas: Presença e influência nas relações internacionais contemporâneas* [Doctoral dissertation, Universidade de São Paulo]. Repositorio USP. https://tinyurl.com/m4c5zut4

Wielandt, G., & Artigas, C. (2007). *La corrupción y la impunidad en el marco del desarrollo en América Latina y el Caribe: un enfoque centrado en derechos desde la perspectiva de las Naciones Unidas* [Serie Políticas Sociales, No. 139]. Organización de las Naciones Unidas. https://tinyurl.com/bded4ksp

Zakaria, F. (2008). *The Post-American World.* W. W. Norton & Company.

Chapter 11

Intelligence Operations and Gray-Zone Wars*

DOI: https://doi.org/10.25062/9786287818408.11

Oscar Fernando Rubio Ramírez
Jesús María Díaz Jaimes
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This article addresses intelligence operations and gray zone warfare, a recent topic in strategic studies of new wars. First, it outlines the concepts and characteristics of the terms discussed. Second, it frames gray-zone conflict or war—an ambiguous and difficult-to-understand term—found in many countries and criminal organizations at both regional and global levels. Finally, it analyzes the challenges, opportunities, and operational and strategic scope of military intelligence in contemporary gray-zone war scenarios and conflicts. It thus seeks strategies that generate effective tools for addressing these conflicts on both the national and international stages.

Keywords: ambiguity; conflict; hybrid warfare; intelligence operations; gray zone.

* 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 Fernando Rubio Ramírez
Lieutenant Colonel in the Colombian National Army. Master's in Strategy and Geopolitics, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Diploma in Oceanopolitics, Spanish Army War College, Spain. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: **oscar.rubio@buzonejercito.mil.co**

Jesús María Díaz Jaimes
Retired Lieutenant Colonel of the Colombian National Army. Master's in Strategy and Geopolitics, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Political Science, Universidad Autónoma de Bucaramanga, Colombia. Specialization in Management, Universidad Militar Nueva Granada, Colombia.
https://orcid.org/0000-0001-6595-8277 - Email: **jesus.diaz@esdeg.edu.co**

APA Citation: Rubio Ramírez, O. F., & Díaz Jaimes, J. M. (2025). Intelligence Operations and Gray-Zone Wars. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 233-258). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.11

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

Armed conflicts, such as world wars, have experienced major changes on the battlefield, especially from the late 14th century to today. Starting with first-generation warfare, which includes European wars fought by Napoleonic armies in the 19th century to gain or defend territorial sovereignty, a key feature was the widespread use of firearms until the 20th century (Aznar, 2015). The typical scene in World War I involved large armies facing each other directly, which led to the development of new concepts, such as "indirect warfare" by military thinker Liddell Hart, who inspired the German army's mobile or lightning warfare (*blitzkrieg*) in World War II (Del Rey & Canales, 2012). The main features of this type of warfare are industrialization and mechanization, with one of its core elements being the ability to mobilize large armies and use war machinery, resulting in the development of new technologies for weapons and doctrines.

Furthermore, following the United Nations Charter of June 26, 1945, and the Geneva Conventions of August 12, 1949 (which introduced the highly material concept of *armed conflict*), new rules and duties were created that States must follow during conflicts between or within States, as applicable (Raggio, 2019). These regulations marked many conflicts of the second half of the 20th century, in what became known as the Cold War, in which the two dominant superpowers of the time participated: on one side, the Union of Soviet Socialist Republics (USSR), which represented the communist development model, and, on the other, the United States of America (USA), which led the capitalist-liberal model. Although this conflict was characterized mainly by the absence of direct military confrontations, both powers actively expanded their influence in third-party countries across all continents to weaken each other's political, economic, or military dominance.

This situation led to the escalation of numerous internal conflicts in many countries, including Vietnam, Nicaragua, Laos, Afghanistan, and the Congo, where many irregular groups were armed and trained to overthrow the State they fought against. In this context, the concept of *asymmetric warfare* emerged, referring to the use of unconventional methods, including terrorism, political warfare, dirty wars, counterinsurgency, and disinformation (Cuneo, 2019). These tactics compensated for the unequal military force, enabling the achievement of political goals. Because these conditions created a new form of warfare that was very hard for States to face within the framework of International Humanitarian Law (IHL), many human rights were violated, and several dictatorships of different kinds were established or strengthened around the world during the Cold War.

When the USSR collapsed in 1991 due to the failure of its economic and political systems, it led to the disintegration of its member States, especially in Eastern Europe, and the loss of its sphere of influence around the world. This ushered in a new era of internal conflict and the rise of radical Muslim religious groups, which caused the deadliest terrorist attack of the early 21st century: two commercial airplanes crashed into the Twin Towers in New York City. This attack sparked a new war, this time against terrorism, led by the Bush administration (Correa, 2017).

In response, the U.S. government directly intervened in several countries to target the military cells of armed groups that use Islamic terrorism, known as jihadists. One example is Al Qaeda, which had training bases in Afghanistan and Iraq aimed at overthrowing Saddam Hussein. These conflicts led to a significant increase in civilian casualties due to the indiscriminate use of terrorist tactics such as car bombs and suicide attacks, which are difficult for regular armies to combat.

As a result of the chaotic security situation and the proliferation of multiple irregular groups in Iraq, the jihadist group Daesh—the self-proclaimed Islamic State, also known as ISIS or ISIL—emerged in 2014 after the U.S. invasion. It adheres to the most traditional and orthodox branch of Islam, Sunni Islam, and displaced Al-Qaeda and Al-Nusra from the scene (Muñoz, 2018). This led to a direct confrontation with the Iraqi and Syrian armies, resulting in the seizure of large areas of each country and the declaration of a new caliphate.

The consequences of these events led to a large-scale regional war in the Arabian Peninsula, where the use of media and social media took on a new role, becoming indispensable in recruiting and spreading their ideology worldwide. The result was multiple terrorist attacks in Europe and the United States by so-called *lone wolves* (Cuneo, 2019), individuals recruited through social media to carry out high-profile terrorist attacks and boost the group's global presence. However,

thanks to the military campaign conducted by NATO forces, Russia, and Iran, which supported the local authorities in Iraq and Syria with military and financial aid, Daesh was militarily defeated in 2017, allowing these forces to protect their strategic interests in the region.

Regarding the regional environment of the American continent, it is important to note that in the central and southern hemispheres, armed groups use terrorist tactics to achieve their objectives, as seen with the Zetas and the Sinaloa Cartel in Mexico. These drug trafficking organizations possess substantial economic power derived from the drug trade, have established large armies equipped with military arsenals from the United States, and maintain full control in certain states where they are legally protected. Through intimidation and targeted assassinations, these groups achieve co-governance and actively participate in the development of regional policies (Zavala, 2018) to further their own interests. Faced with this situation, the Mexican State, led by its Armed Forces, has waged a frontal battle against these organizations and has strengthened its operational and intelligence capabilities, which resulted in the capture of the leader of the Sinaloa Cartel, known by the alias "El Chapo" Guzmán, in 2016.

Regarding Colombia, several armed groups have been identified, some of which have existed for more than fifty years, such as the National Liberation Army (ELN). Other groups formed through the demobilization of former armed organizations include Clan del Golfo, which absorbed some former members of the United Self-Defense Forces of Colombia (AUC) and its areas of influence (Bolaños, 2018). Another example is the peace process between the Colombian government and the Revolutionary Armed Forces of Colombia (FARC), which led to the emergence of several factions or groups, such as FARC Residual, Segunda Marquetalia, and Comandos de la Frontera.

In this context, intelligence operations have been the spearhead of all state intelligence agencies to dismantle these organizations, where ingenuity and deception are crucial. For example, we can mention Operation "Jaque," carried out on July 2, 2018, in which members of Military Intelligence used a fake identity and story to pose as a non-governmental organization (NGO) that was supposedly planning to collect fifteen hostages held by the FARC, including former presidential candidate Ingrid Betancourt, kidnapped since 2002 (Bolaños, 2018). These individuals were released after boarding a helicopter that was supposedly taking them to the location of Guillermo León Sáenz Vargas, aka *Alfonso Cano*, the organization's main leader at the time. During this operation, two leaders of the First Front, Gerardo Aguilar, aka *César,* and Alexander Farfán, aka *Enrique Gafas,* were captured without firing a shot.

It should be noted that this intelligence operation sets a global standard for achieving strategic results with significant national impact without using firearms. The key lesson is that understanding and analyzing how an organization, criminal group, or enemy force operates or commits crimes enables us to identify and leverage its weaknesses while neutralizing its strengths to fulfill our objectives.

As a result, the Colombian military and police forces have undergone a transformation in their training and doctrine to address the various threats they face. In this context, intelligence operations refer to the tasks carried out by military intelligence units and combat units to gather information that meets the commander's critical needs (Schachtner, 2018). Specifically, intelligence personnel are responsible for planning and executing operations against threats and armed groups that commit crimes in their areas of operation.

In short, warfare has evolved along with human development in a globalized world. The nature of conflicts has changed significantly, especially since the Cold War ended. As a result, conflicts between the armies of nation-states are less common, with the notable exception of the current war between Russia and Ukraine. Instead, armed confrontations now mainly focus on internal or civil wars, as well as the rise of radical groups that seek to achieve political objectives through unconventional methods, including terrorism. These features create a non-physical spectrum known as the *gray zone*.

Within this gray zone of war, political, economic, legal, conventional, and unconventional actions dominate, aiming to weaken the adversary's motivation or desire for confrontation so that it aligns with the State's goals. The key is to avoid directly compromising the actions of the nation's regular forces, as this could lead to increased diplomatic tension or, ultimately, an armed confrontation.

The Concepts of "Intelligence Operations" and "Grey Zone" in Contemporary Wars

Intelligence Operation

Intelligence, according to NATO's definition, in a broad sense and within the military context, is the result of gathering and analyzing knowledge about the terrain, weather, activities, capabilities, and/or intentions of a current or potential enemy (Sainz, 1991). It seeks to understand the behavior of the threat by obtaining

comprehensive and detailed information on how it acts or commits crimes. It is also regarded as a discipline that follows a logical process—a sequence of steps that lead to a final product or information useful for operational command decision-making.

In this context, an intelligence operation involves tasks or actions performed by trained and qualified personnel to gather information about an enemy or threat, which varies depending on the country's military doctrine (Quiñónez, 2012). Usually, concepts are developed based on experiences from various wars in which the enemy is involved, as well as the type of warfare, whether conventional or irregular/unconventional. It is important to note that these activities are planned and executed by personnel specifically trained for such missions, commonly known as intelligence agents. They must meet special requirements and conditions set by the relevant authorities of a State or nation.

Intelligence agents have a specific profile, including physical and psychological traits that adapt to their operational environment. These agents must be capable of executing the intelligence cycle, especially in planning and gathering information, to produce accurate analysis and use information effectively, aligned with the objectives and scope of the mission. Most secret agents are quiet and highly discreet, able to infiltrate high-level diplomatic, governmental, or business circles without drawing suspicion (Swenson & Sancho, 2015), as they master the art of camouflage by skillfully using a facade or fictitious story that enhances security against detection by the enemy.

Likewise, there are at least three main types of intelligence that address different needs: military intelligence, strategic intelligence, and police or criminal intelligence (Swenson & Sancho, 2015). Depending on the situation, agents conduct intelligence activities or operations to prevent, detect, and neutralize threats or crimes that pose a risk to a country's security and defense environment. These needs can vary depending on the national and geopolitical interests involved in any domain, whether land, sea, air, cyber, logistical, or biological (Méndez et al., 2019).

In this context, intelligence operations are carried out based on the information needs or gaps identified by the command to support its planning efforts. As explained in the following sections, intelligence operations are divided into six categories: espionage, sabotage, deception, psychological operations, information-gathering operations, and neutralization.

Espionage

Since ancient times, the main role of any intelligence agency has been to gather information on the strengths and weaknesses of rival States and plan their attacks accordingly. Espionage is a covert activity used to obtain classified information through spies for the benefit of an organization or nation. As a result, a spy must be a highly trained individual skilled in collecting classified information related to political, economic, psychosocial, or military matters using clandestine or covert methods (Llop et al., 2013).

According to Gamboa (2016), the old idea of *intelligence/espionage*, which focused only on informational tasks related to "secrets," has long been replaced by a more open-minded approach that requires greater integration to perform new and complex tasks, develop them scientifically, and adapt to the collection and processing of information from many new fields (Gamboa, 2016).

Similarly, depending on its needs and the assigned mission, espionage uses different sources of information, such as recruiting people with access to information, gaining relevant documentation, technically transmitting information, leveraging the agent's or spy's activities, utilizing physical infrastructure for intelligence operations, handling materials or equipment, and studying the natural environment, which involves examining the physical surroundings where espionage activities take place (Llop et al., 2013).

With the globalization of information through the internet, it is very easy to access "open source intelligence" (OSINT), which provides large volumes of data that are difficult to properly select, compare, and analyze. Therefore, the widespread use of new technologies that can assist in the search and tracking of information of national interest is necessary.

The world's advanced intelligence agencies have adapted to the new globalized international landscape and are now taking advantage of opportunities offered by information and communication technologies (ICTs). Finally, it is worth noting that attacks by States, groups, or individuals aimed at obtaining information to gain strategic, political, or economic advantages have been a constant throughout history and continue to pose a significant threat to security (Gamboa, 2016).

Sabotage

Also known as *subversion*, it involves covert acts of physical violence directed at material assets, whether they are owned individually, collectively, or publicly. These acts range from simple modifications of their function to total destruction (Llop

et al., 2013). Generally, the goal of sabotage is to destabilize the State in any of its areas—economic, political, social, or military—to gain tactical advantages that ultimately lead to strategic consequences.

This activity is connected to conducting military operations that, in a conventional war, aim to achieve the objectives set by the State against a threat or enemy. Unlike unconventional warfare, military operations are not necessarily conducted to directly influence the enemy or attain these goals. Carrying out any sabotage action requires information to understand the specific and technical features of the target to be sabotaged, so that the enemy or other adversaries—whether internal or external—will focus their efforts on fulfilling these information needs (Llop et al., 2013).

The objectives achievable through sabotage depend on the ability of the State or organization to access the enemy's material assets or computer networks. This determines whether it has the necessary conditions to impact important documentation, critical infrastructure, the enemy's military equipment, the computer infrastructure, or websites of government agencies, and the natural or geographic environment that could provide a tactical or strategic advantage (Llop et al., 2013). For this reason, incendiary sabotage is used, which involves explosives, especially against critical infrastructure. Mechanical sabotage targets enemy military equipment and capabilities. The most common method today is computer sabotage, which involves stealing information and disrupting or neutralizing the enemy's computer systems.

Deception

These operations are used for military deception or disinformation, which, according to Andrade et al. (2011), are actions carried out with the goal of misleading adversaries about the capabilities, intentions, and operations of one's own military forces. These actions promote incorrect analysis and cause the adversary to draw false conclusions. The aim is to gain an advantage in military or intelligence efforts and to reduce the negative impact of enemy actions on national interests.

Another goal of deception operations is to weaken the credibility of enemy individuals or organizations in their decision-making by altering their perception of reality. The purpose is to buy time and disrupt the unity of military command or the enemy's policies, all without deploying a large number of troops or military equipment for strategic gains. In intelligence operations, this kind of deception is used against both human and technical intelligence, as well as enemy communications and their computer systems.

Psychological Operations

They refer to the planned and directed strategy of using a set of elements, such as propaganda, the media, and other forms of psychological actions—employed by any of the forces involved in conflict—with the goal of influencing the will, attitude, and behavior of troops, population groups, and members of hostile organizations (Andrade et al., 2011) to gain strategic advantages and succeed in warfare.

Since psychological operations are meant to support military efforts, they cannot be conducted by independent forces. They are categorized into three types: strategic, tactical, and consolidation, based on the geographic features of the operational area, the target audience, and the expected timeframe for implementation. Therefore, consolidation psychological operations are performed in regions already under the control of the State, aiming to establish normalcy and foster support among the civilian population.

In this context, it is essential to employ advanced technology capable of penetrating enemy media, either directly or indirectly, to create a matrix of opinion or perception aligned with established objectives and to force the adversary to engage in our information or disinformation domain. This approach would produce a positive tactical or strategic outcome based on the mission's goals.

Likewise, there are many methods that can be used in psychological operations, depending on various factors and categories, such as radio and television broadcasting; distributing printed materials or pamphlets by air; giving gifts and supplies; rumor campaigns against the enemy; publicizing their military defeats; causing shortages of food, shelter, clothing, or other essential items; creating fragmentation and internal distrust; causing conflicts over the management of economic resources (Andrade et al., 2011). In general, any weakness within the enemy system that reduces their will to fight can be exploited.

Information-Gathering Operations

These are intelligence activities designed to use information to achieve national objectives. Like diplomacy, economic competition, or the use of military force, information itself is an essential part of national power (Andrade et al., 2011); in any case, it can be used both defensively and offensively to carry out the mission, as well as to protect one's own capabilities and systematically attack the threat.

To this end, all available media for information dissemination are utilized: radio, television, print media, social media, and digital media. Additionally, information quality criteria such as accuracy, relevance, timeliness, practicality, completeness,

conciseness, and security must be met to produce an optimal information product for the target audience, ensuring they are neither misinformed nor misled, as appropriate.

The objectives of information-gathering operations are extensive, especially in a society that is currently highly connected through digital and social media. Therefore, intelligence agents must study and plan carefully to effectively influence their target audience by leveraging their emotions, motives, and rational thinking, as well as the behavior of governments, organizations, groups, and individuals (Andrade et al., 2011). The goal is to destroy, disrupt, or deny the adversary's use of information, while also degrading, deceiving, exploiting, influencing, protecting, detecting, restoring, or responding to any enemy information that could undermine the credibility of their own institutions, people, or organizations.

Neutralization

Neutralization operations are those designed to prevent any military or unarmed action that could threaten the integrity or institutions of a State or organization. They aim to counter the intentions, threats, and objectives of adversaries or enemies through "counterintelligence" (Quiñónez, 2012), which involves disrupting the adversary's command and control capabilities, for example, by eliminating enemy unit commanders using unconventional methods or military operations with Special Forces units.

They also aim to weaken the logistical or economic capacity of the threat by targeting its critical infrastructure and, most importantly, enemy political or military leaders. An example is the operation carried out by the United States in 2020 to kill Iranian General Qasem Soleimani, commander of the Qods Force in Iraq, who was viewed as a potential threat to that nation's security or legitimacy.

Therefore, it is concluded that intelligence operations should target more than just direct threats. While espionage provides the essential information needed to prevent, detect, and neutralize threats, it also supplies the arguments for proactive planning concerning potential changes in the political, economic, military, or social spheres that could affect the national or strategic interests of the State.

Gray Zone

The concept of the gray zone was recently introduced by geopolitical scholars and adopted by some States, defining it as a spectrum or a new domain of unconventional warfare characterized by ambiguity and lacking a clear physical space. However, it should be noted that some actors do not acknowledge this

zone or include it in their strategic security analyses. Since their strategies have multiple dimensions and facets, creating a rigid overall strategy is challenging. Moreover, even if they attempt to implement such a strategy, it may not achieve the final objectives quickly (Jordán, 2018). Therefore, methods and techniques for targeting the various elements within the gray zone must be developed gradually and precisely.

Characteristics of the Gray Zone

The gray zone describes a broad concept with traits that are hard to notice at first, but that countries and criminal groups create to reach their strategic goals. This spectrum specifically has four traits: ambiguity, gradualism, significant interests involved, and complex strategies, which are explained in the following sections.

Ambiguity

This means that neither peaceful relations nor armed conflict is considered. In a gray-zone conflict, strategic competition between two or more States (with their respective conflicting dyads) occurs below the threshold of political violence, manifesting as a minor armed conflict (Baqués, 2017). That is, a small-scale confrontation where there may be verbal complaints, protests, and the use of the civilian population against authorities, which can lead to a political dispute over time.

Military forces also play a role in this characteristic, which can perform deterrent exercises or show of force in conflict areas or along national borders, while avoiding escalation into open armed conflict. For example, it is worth mentioning the deployment of fighter jets from the People's Republic of China Air Force over Taiwan's territorial waters; this case demonstrates that efforts are being made to avoid crossing red lines that could lead to a military conflict with very high costs and unforeseeable consequences (Mazarr, 2015). In this context, it is crucial for the stronger State to understand its adversary's response capacity to prevent a more powerful and broader military response, which could escalate into a direct war outside the gray zone.

This deliberate ambiguity makes it hard to recognize hostile activities in the gray zone and to coordinate response strategies (Mazarr, 2015). Therefore, it is crucial for intelligence agencies and strategic planning to understand the political goals behind the threat and the methods used in the gray zone, to prevent, identify, and if possible, stop the enemy's intentions or lessen the impact of their actions.

Gradualism

Gradualism emphasizes ambiguity because the importance and connections of various actions are not always clear to the opponent's political decision-makers, allies, or respective public opinions (Mazarr, 2015). This occurs in a context where time is undefined, and desired results or progress happen slowly or gradually. Additionally, this gradual approach maintains the status quo, allowing actions to slowly bring about changes or modifications in gray-zone conflicts. This can lead to a new scenario of hybrid or direct war, depending on the case, or alternatively, produce a fait accompli that allows the strategic goal to be achieved.

Substantial Interests at Stake

This characteristic of gray zone warfare explains why conflict occurs, as the interests and benefits involved often outweigh the risks of exposing them to the enemy or threat. In other words, in this scenario, traditional diplomatic channels are often abandoned in favor of strategies that might cross red lines, which, if uncovered, could result in sanctions or serious diplomatic issues for the country, depending on its geopolitical influence and alliances with actors that could support it.

The influence of asymmetric interests is also evident outside the gray zone, particularly in armed conflicts where the weaker side often defeats the stronger for similar reasons (Mack, 1975). Similarly, in the gray zone, interests may conflict with each other, so the response of alliances will depend on whether the threat directly affects them or if it is merely a conflict between two parties. As a result, they tend to avoid escalating the conflict and aim to stay neutral to safeguard their national interests.

Multidimensional Strategies

Gray-zone warfare refers to a spectrum of actions or strategies that adapt to the type of conflict and goals involved. In this context, these actions may resemble the strategy used in hybrid warfare, which combines various modes of combat such as "conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder" (Hoffman, 2007, p. 8). All of these actions, which can occur "simultaneously and adaptively," constitute a form of multimodal warfare employed by "states or groups that select from the whole menu of tactics and technologies and blend them in innovative ways to meet their own strategic culture, geography, and aims" (Hoffman, 2009, p. 35).

It can be concluded that gray-zone war or conflict involves the deliberate, multidimensional, and integrated use of various instruments of power, including

political, economic, social, informational, diplomatic, and military (Mazarr, 2015). In this scenario, military force is used symbolically and with coercive intent—i.e., to signal, intimidate, and mark territory, or, in some cases, to support other actors who are exercising force. However, it should be emphasized that the key characteristic of gray-zone conflict is the broad and integrated use of unarmed tools. If military force is used to carry out offensive actions, the conflict escalates into open and direct warfare, making it impossible to describe it as part of the gray zone spectrum.

Since these four characteristics are essential in determining whether a gray zone conflict exists, most civilians find it difficult to recognize that a threat could destabilize their way of life. Therefore, seeking public opinion support to legitimize methods or means to attack a threat or enemy becomes an arduous task. It is more practical to form regional alliances that share the same principles or objectives to address these threats, because, as Waltz (2010) said, the international system is shaped by two factors: the first is international anarchy, which is the absence of a supranational authority that effectively guarantees the security of States; and the second is the distribution of relative power among States.

Operational and Strategic Importance of Military Intelligence in Contemporary War Scenarios and Gray-Zone Conflicts at the Global and Regional Levels

It is important to understand the nature of the conflict and the actors involved, as procedures often change depending on the desired impact—whether tactical, operational, or strategic—and in accordance with the directives or intentions of the war's leader, who would be the president or head of the nation. In this scenario, intelligence operations can achieve strategic results of significant national impact without necessarily involving an armed military component in their planning or execution, thereby avoiding the risks associated with armed confrontation, which would be far more severe in a conventional war between two or more countries.

Therefore, military intelligence plays a crucial role in both conventional and unconventional wars—especially in gray-zone warfare—since intelligence operations provide the essential tools to gather information, whether operational or strategic. This information not only helps predict the adversary's intentions or

threats but also supplies the key input needed to develop strategies suited to the enemy's capabilities and the operational and strategic environment where the conflict occurs.

However, it should also be noted that there is a significant element of deceit or fraudulent intent in the actions taken by the actor in the gray-zone war, as it violates the principle of good faith upheld by States in international relations (Baqués, 2017). Therefore, intelligence operations conducted in the gray zone must be kept compartmentalized and operationally secret, which limits the potential for violating the accepted boundaries of this zone and causing issues that could escalate into direct conflict with the adversary.

Authors such as Baqués (2017) and Jordán (2018) have already been mentioned, who explicitly refer to the violation of the principle of good faith that should govern international relations as a key element of the concept. Therefore, actions in the gray area, while attempting to avoid crossing established boundaries at all costs, cannot be classified as ordinary, regular, and legitimate manifestations of international relations because they violate the good faith principle that defines them.

Opportunities for Intelligence Operations and Their Use in Gray Zones amid Contemporary Wars

Gray-zone conflict or war presents a range of possibilities for conducting intelligence operations that are commensurate with the capabilities and training of intelligence agencies. Furthermore, the economic factor plays a crucial role, as financial resources determine the duration and continuity of intelligence activities, regardless of the type of operation being carried out.

Specifically, there are several opportunities or mechanisms available in the gray zone, some of which are outlined in the following sections.

Operations to Influence the Adversary's Public Opinion and International Public Opinion

These actions can be classified as psychological or information intelligence operations, where narratives are created or constructed to be spread through one's own or enemy media outlets. In this way, news stories or messages are generated that reinforce one's own perspective and discredit the adversary's narrative. To

accomplish this, it is crucial to leverage all types of social media accessible to the target audience.

Currently, several companies create trends on social media using web or information warehouses. Many people operate computers with multiple fake profiles across different platforms, such as Facebook, Twitter (now X), TikTok, and Instagram, to coordinate trends or spread information based on the needs of the client. These warehouses, also known as "troll and click farms," are common in some countries, particularly Russia, and have influenced electoral processes in Europe and the United States. They also use fake news, which is very prevalent on social media—what some now refer to as deep fakes—and can even modify highly credible videos to make someone say or do what they need (Marín, 2020). These tools, combined with artificial intelligence, are crucial for producing credible and user-friendly computer content that influences opinions in favor of one's interests.

Similarly, in the regional context, there must be strong and trustworthy media outlets that can function as a platform for the information or news they aim to share. Therefore, they should avoid spreading too much fake news that could harm their reputation. In this regard, the narrative must align with actual facts that are hard for the other party to deny. Lastly, it is important to note that in remote areas, where print or digital media have little to no influence, information often comes through text messages or chains on messaging apps.

In this context, apps like WhatsApp, Telegram, Facebook, Messenger, Signal, and others serve as tools for spreading chain messages, videos, or audios with manipulated information or fake news that help create panic or spread misinformation among enemy forces or affected civilians. For this reason, they are a crucial element in striking the enemy through deception operations that lead to their demobilization from the battlefront or in delivering significant blows to their armed forces through Special Forces units.

Cyberattacks against State and Private Entities

These actions are intended to disrupt the activities or functions carried out by private or public entities of an enemy State or organization. Since it is hard to identify and respond to an attack without risking harm or worsening relations with other States or the opposing party in a conflict (Silva, 2021), the appropriate response from the relevant authorities might be to undermine the credibility or operation of these entities among their civilian population, causing chaos and uncertainty.

Furthermore, these actions aim to steal sensitive information that can provide a strategic advantage over the adversary. This is evident in economic cyberespionage, which can save a country investment in research and development by appropriating technological advances or intellectual property from other companies or States for its own benefit, as China has done in recent years against Western companies.

Political Support for the Opposition of the Adversary

This method is used by state intelligence agencies with government approval to fracture and disrupt the enemy's political environment, thereby weakening its decision-making ability. One of the most well-known domestic cases was the United States' involvement in 1901, when it incited an armed revolt in the Colombian territories of present-day Panama to support its independence and ensure the construction of the Panama Canal and control of the surrounding area (Silva, 2021).

This support includes providing financial aid and the necessary supplies for the opposition's political activities to succeed. To do this, it is crucial to understand how to operate within the gray area of confrontation by leveraging situational ambiguity. Therefore, it is important to avoid leaving traces or clues, such as electronic transactions or meetings between the political opposition and its agents or envoys, in order to prevent enemy intelligence or counterintelligence agencies from gathering evidence of this support. This reduces the risk of it escalating into a larger diplomatic conflict.

The case of Viktor Medvedchuk, a Ukrainian politician from the pro-Russian party Opposition Platform – For Life, is worth mentioning here. He is the godfather of one of Putin's daughters and was actively supported by the Russian intelligence agency FSB to create the political conditions for Russia's invasion of Ukraine in February 2022. While some analysts presented him as the future link between Russia and a defeated Ukraine subjugated to the Kremlin, and in Kyiv, he was called "the prince of darkness," a nickname that indicated his tendency to move in the shadows (Goncharenko, 2022), Ukrainian intelligence agencies were following him for his evident support for the Kremlin. After the failed capture of Kyiv by the Russian army, he went into hiding and attempted to escape to Russia, but was captured by Ukrainian intelligence services in April of the same year.

In other words, only the political strategic leader can risk supporting an adversary's political opposition, but they must do so after analyzing the consequences and, if possible, in a discreet way that allows them to advance toward their goals.

Aggressive Intelligence Actions

Intelligence activities against the enemy in a gray-zone conflict must be conducted aggressively and consistently to infiltrate their secret intelligence services, gather top-secret military information from their forces, or carry out violent actions through recruited agents to target institutions or individuals that pose a threat to their interests.

For instance, Russian intelligence agencies conducted aggressive intelligence activities in Colombia, supporting the 2021 national strike. This was confirmed by the Central Intelligence Agency (CIA) dossier, which shows Russia's involvement in the unrest in Bogotá through funding groups responsible for the riots and damage during protests across the country, including in 2019 (Unidad Investigativa, 2022). This suggests that the distance from the target country does not necessarily hinder engagement in gray-zone conflict and the pursuit of one's interests. In this case, the aim was to weaken the Colombian president's authority, bolster the opposition, and create a more favorable political environment for the Venezuelan regime, which is ultimately Russia's main ally in the region, along with Nicaragua and Cuba.

Faits Accomplis

These involve challenging the deterrence of the opposing actor, whose goal is to provoke it in order to force overreaction, primarily through violence, thereby undermining its internal and external legitimacy and leaving it in a weakened position. Referendums or declarations of independence are good examples (Silva, 2021). For the fait accompli to be effective, the gain must be limited so the victim prefers to let these actions pass rather than escalate and risk armed conflict.

Faits accomplis are a common tactic when occupying disputed territories between two or more States (Jordan, 2018). For example, in the annexation of the Crimean Peninsula, the Russian Federation used a deception operation, took control of the region's power centers with military personnel and intelligence agents, and exiled the Ukrainian authorities. In this way, with minimal force, it achieved a significant territorial gain, creating a fait accompli that Ukraine or NATO could not reverse, as doing so would have led to an escalation of the conflict with severe consequences for all parties.

Proxy Wars

They occur when two or more countries use third parties as substitutes to avoid direct confrontation. A recent example happened at the start of the Cold War, when

the nuclear threat increased the risk of mutually assured destruction, leading to the widespread use of proxy actors among the great powers: the Soviet Union, China, and the United States (Pontijas, 2020). Therefore, a State organized or supported another State, a private army, or a party in a conflict, providing it with weapons, training, military support, financing, and advisors, so it could fight its enemy without deploying its own military forces.

Currently, many countries use proxy warfare to protect their interests, such as the United States, Russia, the United Kingdom, Iran, Turkey, Saudi Arabia, China, and Pakistan. It is also used by non-state actors, including large corporations and businesses, terrorist groups, drug cartels, and others (Pontijas, 2020), with the goal of weakening the enemy's military strength in an armed conflict and thus eroding or dismantling its military power through ongoing military confrontation against its adversary.

In this ambiguous warfare zone, a proxy war is one where the enemy clearly understands its opponent's intentions and goals. It is a form of hybrid warfare, almost a direct confrontation, which could escalate into a full-scale war depending on the weapons and tactics used. This situation could arise in the conflict between Russia and Ukraine, who are engaged in a direct conventional war, with NATO, led by the United States, providing heavy weaponry and substantial financial support to bolster the Ukrainian military's fighting capacity.

This strategy has dealt significant blows to the Russian army, causing the Kremlin to change its initial strategy and objectives. Instead of aiming to occupy Kyiv and install a pro-Russian government, as was initially proposed, its goal shifted to gaining control of the eastern part of the country, the Donbas region, and capturing the Black Sea coast from Ukraine.

This situation could lead to a dangerous escalation of the war, as Russia might interpret NATO's support for Ukraine as an act of aggression, prompting it to launch attacks against Poland or the Baltic States in a direct challenge to the organization's greater military power. As seen in this case, which could escalate into a nuclear conflict, a proxy war aims to provoke a direct clash with the adversary, thereby weakening its military strength and preventing it from securing victories on the battlefield. This strategy also aims to undermine its position in potential negotiations, helping to preserve the political interests and objectives involved.

Economic Coercion

These are robust trade and financial measures implemented against States considered hostile or disruptive to national interests. They aim to weaken their international trade ability and the local purchasing power of their populations. It is worth noting that in this context, support for national, sectoral, individual, or coordinated strikes, along with other actions to exert political coercion and increase political pressure, plays a vital role (Silva, 2021). These economic measures or sanctions need to be strong enough to create sufficient pressure against the opposing government, thereby prompting a shift in its political stance toward one more favorable to the interests of the initiating State.

This is the case of Venezuela, where the United States has imposed several economic and political measures to weaken the regime's power, such as economic sanctions and the non-recognition of its presidency. Although these actions have been ineffective, the Maduro government has been compelled to make limited political concessions and implement economic reforms to maintain control of the country. Specifically, through a process of chaotic economic liberalization, it has tried to give the economy a break, benefiting its elites and groups with access to foreign currency, thereby reducing social tensions. This chaotic transformation, instead of weakening Maduro, has enabled him to strengthen his hold on power (Jiménez, 2022).

Similarly, sanctions against countries like Russia, for its illegal annexation of the Crimean Peninsula in 2014, or Iran in 2018, for its nuclear program, have been ineffective because these countries have found ways to counter external pressures without giving up their achievements and goals. Moreover, their media have used these sanctions as propaganda to denounce a large-scale Western aggression aimed at bringing the government and the nation to their knees. These facts show that, in a gray-zone scenario, economic coercion must be combined with other methods to achieve a strategic advantage over the enemy.

Sliced Salami Tactics

The origins of the term date back at least to the late 1940s, when Hungarian communist leader Mátyás Rákosi claimed to have successfully defeated his internal rivals by inciting them to abandon increasingly large segments of his own party, "cutting them like slices of salami" (Pusztai & Inántsy-Pap, 2016). Also known as incremental gains, this gray-zone warfare mechanism refers to the accumulation of several low-profile actions that provide incremental gains while making it

difficult for the adversary to respond harshly (Mazarr, 2015), since, considered individually, they do not justify the adversary's use of force. This approach creates an opportunity for discussion or diplomatic settlement to find a sensible solution and prevent the conflict from escalating or turning into war.

Therefore, sliced salami tactics occur when multiple faits accomplis are carried out to weaken the enemy's position, thereby boosting our deterrent capability and leverage in potential negotiations. This approach prevents the enemy from responding, as its credibility gets damaged the moment it tries to act, which worsens its situation. For example, Russia has consistently used salami tactics over the past twenty years against its regional neighbors, not only by separating Abkhazia and South Ossetia from Georgia, and Crimea from Ukraine, but also by subtly expanding border fences in Georgia, conducting provocative military flights over Eastern Europe, and moving to control Arctic natural resources (Maass, 2022).

Finally, it should be noted that salami tactics and fait accompli succeed if escalation can be managed and if there are sufficient military capabilities to win at the highest level of conflict.

Military Deterrence

This tool should be viewed as the last deterrent measure, used only after all other options have been exhausted. Its purpose is to carry out military actions that create a psychological impact on the enemy. This involves demonstrating superior military strength to instill fear in the adversary if they attempt to escalate the conflict or engage in gray-zone warfare.

As Jordán (2014) states, deterrence is a process that involves influencing an actor through threats, either tacit or explicit, to prevent them from taking a specific action. Deterrence can be employed before a conflict begins to prevent it, or once hostilities have started, to limit its geographic scope or reduce the intensity of the confrontation (Jordán, 2014). Therefore, the cost-benefit ratio of this action must be assessed objectively and professionally.

Conversely, a thorough understanding of the enemy's military capabilities, whether from a state or non-state actor, is essential for creating effective military deterrence strategies that prevent escalation into direct conflict, which can happen due to a lack of knowledge about the enemy's response protocols. In other words, it is crucial to have a clear understanding of the adversary's doctrine and military capabilities to effectively respond to an attack.

Finally, to conclude this presentation, Figure 1 summarizes the opportunities or mechanisms that can be employed in the gray zone.

Figure 1. *Mechanisms Used in a Gray Zone*

Source: Own elaboration.

Gray Zone in Colombia

Throughout its republican history, Colombia has been marked by struggles against illegal groups, foreign influence, and local communities that aim to exert political, social, and economic control through military or armed force in various illicit activities within the country. As the world's top producer of coca paste, the nation hosts multiple criminal organizations that oversee different stages of drug production, such as the FARC dissidents, ELN, Clan del Golfo, EPL, and regional organized crime groups.

Foreign actors directly or indirectly facilitate the transit of narcotics in exchange for economic benefits, as is the case with the Venezuelan regime, which the international community and multilateral organizations view as the main gateway for drug trafficking from South America to other destinations and continents. Its political, economic, and social conditions, along with corruption, insecurity, impunity, and the decline of security forces and state institutions, have contributed to the rise in both drug trafficking and consumption in the country (Camero, 2017).

Additionally, leaks of confidential documents from the Bolivarian Intelligence Service (SEBÍN) and the Strategic Operational Command of the Bolivarian National Armed Forces (FANB) on August 9, 2019, revealed the presence of FARC dissidents and ELN members in Venezuelan territory, who reportedly enjoy the support of President Nicolás Maduro (López, 2020). This situation creates a serious border security problem with the neighboring country, as irregular groups plan armed

actions against the Armed Forces and attacks on critical state infrastructure from there, aiming to undermine community cohesion and replace state authority. Besides this serious situation, we must also consider the maritime dispute between Colombia and Nicaragua before the International Court of Justice in The Hague over the Caribbean Sea's maritime borders.

This scenario presents significant challenges to the security and defense of Colombian territory, necessitating the exploration of various multidimensional strategies that can be employed against these groups in a gray-zone confrontation. To achieve this, legitimate state actions, such as military or police operations aimed at neutralizing members of the armed groups involved in crimes in Colombian territory, are not enough. The strategy must also focus on delegitimizing these groups' actions in the eyes of the civilian population, who often perceive them as legitimate authorities in their areas.

Therefore, it is possible to evaluate the advisability of using information or psychological operations to impact the border population, and, by extension, targeting members of various armed groups to erode the trust and collaboration that may exist between them. In this way, aggressive actions between these structures could escalate to the point of creating an environment conducive to direct confrontation, which would impact their armed components and their ability to collect the funds they receive from their illicit profits—all this without endangering the safety of members of the state security forces in a potential armed confrontation with these structures.

Now, armed groups are heavily using electronic communication media, such as smart mobile devices, among their armed and logistical components to coordinate the collection of funds and logistical materials for their operations. This situation offers an opportunity to exploit this weakness and acquire new capabilities in electronic warfare equipment, giving the Armed Forces new options like locating and hacking mobile devices. It also allows for cyberattacks to steal data and carry out prosecutions or intelligence operations based on the gathered information.

Since each armed group that commits crimes in the country varies depending on the area it controls, creating its own dynamics of illegal coordination and operations, it is challenging to develop a single strategy to target them uniformly. Therefore, a detailed study of the terrain, population, infrastructure, communication routes, control zones, local legal and illegal economies, regional and national media coverage, internet and mobile connectivity, and other factors is essential. This analysis aims to identify strategies not only to weaken the military capacity

of criminal groups but also to dismantle their support systems, particularly by undermining civilian support and sources of funding.

It is crucial to be clear about the goal expected in a gray-zone conflict against criminal organizations, since there will be no physical victory to gauge the success of the strategy. Instead, in this situation, the aim would be to weaken the strategic capabilities that illegal armed groups possess and their control over areas of Colombian territory and the civilian population living there.

Conclusions

In a gray-zone conflict, it is essential to utilize intelligence operations to achieve established objectives against an adversary State or criminal organization, while aiming to protect national interests as the strategic decision-maker sees them. To accomplish this, espionage, sabotage, deception, psychological operations, neutralization, or information-gathering activities can be employed, all of which can influence the gray zone and deliver significant strategic benefits without resorting to direct armed confrontation.

There are several challenges in the gray zone, as its ambiguity, stakes, and gradualism require the exploration of various multidimensional strategies, which are realized through a careful and comprehensive study of the threat's operational environment. In the case of Colombia, the country faces border security issues with Venezuela and a border dispute with Nicaragua, as well as an internal security problem, as multiple armed groups that commit crimes in different forms coexist. For these reasons, strategies must be implemented to attack their legitimacy as authorities in the areas where they operate, differentially degrade any social support that may exist in their areas of influence, and create conflicts among their members to undermine the command and control of these structures. Furthermore, it is necessary to attack the gray zone with Venezuela and Nicaragua to strengthen Colombia's strategic position vis-à-vis the interests they seek in our nation.

Finally, it must be clear that the war in the gray zone is a conflict involving shadows, which blurs the lines between peace and war among the nations or organizations involved. This escalates into a permanent or long-term conflict that is fought in an ambiguous way. Therefore, victory cannot be measured physically within this spectrum, but rather by the strategic gains achieved in protecting state interests through the accomplishment of objectives.

References

Andrade Rojas, W., Martínez Benavides, J. F., & Pineda Bello, J. C. (2011). *Las operaciones de información en las guerras de información* [Bachelor's thesis, Universidad Piloto de Colombia]. Repositorio UNIPILOTO. https://tinyurl.com/3f7vpwer

Aznar, F. (2015, 25 November). *Las generaciones de guerras: Guerras de primera generación (I)* [Analysis document, No. 54]. Instituto Español de Estudios Estratégicos. https://tinyurl.com/5yca9se5

Baqués, J. (2017). *Hacia una definición del concepto Gray Zone (GZ)* [Research paper, No. 2]. Instituto Español de Estudios Estratégicos. https://tinyurl.com/56aeyjde

Bolaños, L. F. L. (2018). El día que cambió la historia del arma nacional de Inteligencia. *Perspectivas en Inteligencia, 10*(19), 43–55. https://doi.org/10.47961/2145194X.50

Camero, M. (2017). *El tráfico de drogas ilícitas en Venezuela.* Observatorio de Delito Organizado; Asociación Civil Paz Activa.

Correa Martínez, S. L. (2017). *La estrategia antiterrorismo de los EE. UU. en Medio Oriente a partir de los atentados del 11S: Aproximaciones desde el mito político del excepcionalísimo norteamericano* [Bachelor's thesis, Pontificia Universidad Javeriana]. Repositorio PUJ. https://tinyurl.com/4wf8f7dm

Cuneo, P. (2019). *Complejidad y multipolaridad en el Sahel: Nuevas dinámicas relacionales y de intervención en el marco de las relaciones internacionales* [Doctoral dissertation, Universidad Pontificia Comillas]. Repositorio Comillas. https://tinyurl.com/ykknvmpy

Del Rey, V., & Canales Torres, C. (2012). *Blitzkrieg: La victoria alemana en la guerra relámpago* (vol. 1). EDAF.

Gamboa, J. B. S. (2016). Ideas fundamentales sobre inteligencia. In *Inteligencia: Un enfoque integral* (pp. 13–40). Instituto Español de Estudios Estratégicos.

Goncharenko, R. (2022, April 14). Viktor Medvedchuk, el hombre de Putin en Ucrania. *DW.* https://tinyurl.com/2kbh9afu

Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars.* Potomac Institute for Police Studies. https://tinyurl.com/dyc5rmnv

Hoffman, F. (2009). Hybrid warfare and challenges. *Joint Force Quarterly, 52*(1), 34–48. https://tinyurl.com/42ne9y2d

Jiménez, M. (2022). *El difícil camino hacia una democratización en Venezuela* [Working paper, No. 61]. Fundación Carolina; Agenda 2030; Cooperación Española. https://tinyurl.com/yc4f632w

Jordán, J. (2014, June 18). *Gestión de la incertidumbre en las relaciones internacionales: Dilema de seguridad, disuasión y diplomacia coercitiva.* https://tinyurl.com/4aw74fx9

Jordán, J. (2018). El conflicto internacional en la zona gris: Una propuesta teórica desde la perspectiva del realismo ofensivo. *Revista Española de Ciencia Política,* (48), 129–151. https://tinyurl.com/3j5h2j39

Llop Meseguer, S., Martínez Enríquez, L., & Valeriano-Ferrer Gonzales, F. (2013). *Apuntes de inteligencia básica.* División de Publicaciones de la Escuela Superior de Guerra Naval. https://tinyurl.com/4anuvwjy

López, C. (2020). Agencia, actores, escenarios: La tensa calma de la zona gris sudamericana. *Revista de Pensamiento Estratégico y Seguridad CISDE, 5*(2), 25–39. https://tinyurl.com/vybjftfy

Maass, R. W. (2022). Salami tactics: Faits accomplis and international expansion in the shadow of major war. *Texas National Security Review, 5*(1), 33–54. https://tinyurl.com/29bc2jaa

Mack, A. (1975). Why big nations lose small wars: The politics of asymmetric conflict. *World Politics, 27*(2), 175–200. https://doi.org/10.2307/2009880

Mazarr, M. J. (2015, December 22). Struggle in the gray zone and world order. *War on the Rocks.* https://tinyurl.com/5cakh86z

Méndez L. A., Gaitán Vanegas, S., & Fuquen, V. P. (2019). Los dominios de la guerra: Una aproximación al nuevo escenario de la Covid-19. *Estudios en Seguridad y Defensa, 14*(28), 237–257. https://doi.org/10.25062/1900-8325.282

Muñoz Ciro, J. S. (2018). *Causas, proyecto político y medios del Estado Islámico* [Master's thesis, Universidad de Antioquia]. Repositorio UDEA. https://tinyurl.com/5n8uxuvs

Pontijas, J. L. C. (2020). Tendencias en la guerra por delegación (proxy warfare). *Boletín IEEE,* (18), 85–96. https://tinyurl.com/4ytzr357

Pusztai, G., & Inántsy-Pap, Á. (2016). An underground church-run school during the communist rule in Hungary (1948-1990). *Historia y Memoria de la Educación,* (4), 177–213. https://doi.org/10.5944/hme.4.2016.15734

Quiñónez, R. I. G. (2012). *Curso básico de inteligencia.* S. p. i.

Raggio, M. L. (2019). El conflicto en las sombras: Aspectos generales y elementos jurídicos de las operaciones en la zona gris. *Cuadernos de Estrategia,* (201), 17–56. https://tinyurl.com/2yfnn3x

Sainz de la Peña, J. A. S. (1991). Estudio de "Inteligencia operacional". *Cuadernos de Estrategia,* (31), 15–37. https://tinyurl.com/426wst5v

Schachtner, A. J. (2018). *Military intelligence in the gray zone: The strategic role of intelligence in unconventional warfare* [Master's thesis, US Army Command and General Staff College]. Repositorio DTIC. https://tinyurl.com/9ccwwev8

Silva, J. S. (2021). La zona gris, un desafío para la conducción política y estratégica. *Cuaderno de Trabajo,* (6), 1–19. https://tinyurl.com/593hxzm3

Swenson, R. G., & Sancho, C. (Eds.). (2015). *Gestión de inteligencia en las Américas.* National Intelligence University. https://tinyurl.com/y5uxkp2r

Unidad Investigativa. (2022, March 26). El dossier de la CIA que prueba nexo entre rusos y disturbios en Bogotá. *El Tiempo.* https://tinyurl.com/hr7yjwcn

Waltz, K. (2010). *Theory of international politics.* Waveland Press Inc.

Zavala, O. (2018). *Los cárteles no existen: Narcotráfico y cultura en México.* Malpaso Ediciones SL.

Chapter 12

Cyber Capabilities in Contemporary Conflicts*

DOI: https://doi.org/10.25062/9786287818408.12

Juan David Zuleta
Andrés Acosta Muñoz
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Current events show that cyber conflict is already widespread worldwide. This chapter discusses aggressive cyberwarfare strategies and tactics at all stages of national security and defense planning. It concludes that leadership in national security and defense must significantly enhance its understanding of technology, law, ethics, and cyberattacks to address the broader context of multi-domain warfare.

Keywords: defense; strategy; cyberwarfare; intelligence; security.

* 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.

Juan David Zuleta
Lieutenant Colonel in the Colombian National Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Leadership and Management of Military Units, and Specialization in Military Resources Administration for National Defense, National Army Arms and Services College, Colombia. Specialization in Equestrian Administration, National Army Cavalry College. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: **juan.zuleta@buzonejercito.mil.co**

Andrés Acosta Muñoz
Colonel in the Colombian National Army. Master's in Strategy and Geopolitics, and Specialization in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Master's in Security and Defense, Nebrija University, Spain. Specialization in Senior Management, Universidad Militar Nueva Granada, Colombia.
https://orcid.org/0000-0002-2813-5471 - Email: **andres.acosta@esdeg.edu.co**

APA Citation: Zuleta, J. D., & Acosta Muñoz, A. (2025). Cyber Capabilities in Contemporary Conflicts. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 259-278). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818408.12

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

This chapter addresses contemporary conflicts where the capabilities and technological advances of the cyberspace domain are used both offensively and defensively to degrade adversaries' capabilities and create significant destabilization in military actions before, during, and after a conflict. It also analyzes the significant role of Special Forces (SF) and Intelligence units in developing these types of cyber actions and operations, as they are becoming the primary task for States in confronting their threats.

In this regard, it is worth noting that the world is changing by leaps and bounds, and that the development of information and communications technologies (ICTs) is advancing at such an accelerated pace that, in some ways, they are exceeding the expectations of the strategic, operational, and tactical capabilities of Armed Forces around the world. The implementation of new technologies challenges the parameters and factors of conventional warfare, while transforming the strategies that States adopt to confront their adversaries in national, neighboring, regional, continental, hemispheric, and global environments.

Under this criterion, it is possible to identify the main powers in this area, such as the United States, China, Russia, Israel, and Iran, as these countries are belligerents in cyberspace and allocate human, technical, and economic resources to develop their "cyber forces." In general, they act with a dual intention: first, to guarantee the security and defense of their specific cyberspaces, and second, to exert power and influence among their citizens, allies, and potential adversaries (Colom et al., 2013). Ultimately, all of this is intended to prevent and respond to cyberattacks that could jeopardize the continuity and availability of the country's critical services.

However, this is just the tip of the iceberg. Currently, various strategic guidelines have ramifications at both the offensive and defensive levels, which must be addressed to mitigate the different risks and threats in cyberspace. This is especially true in contemporary war scenarios, which often require the intervention of SF units.

Furthermore, this chapter aims to establish the relationship between the new requirements of contemporary wars in terms of operational art and design implementation, as well as identify the center of gravity of cyber threats using strategic intelligence. It is worth clarifying that these initial formulation and logic processes "form the central nervous system of the Colombian National Army's doctrine and address the needs of commanders and staff to resolve situations in volatile, uncertain, complex, and ambiguous operational environments" (Ejército Nacional de Colombia, 2019, p. 19).

The weaknesses of the doctrinal approach to using intelligence and cyber capabilities in modern conflicts are examined through several case studies. This includes analyzing the connection between cyber-based intelligence operations, their success rates in meeting objectives, and the main challenges of using cyber tools in today's scenarios.

Finally, the scope of military intelligence strategies and operations in modern conflicts and wars is analyzed from different perspectives within the cyberspace domain, with the goal of understanding their purposes, features, and outcomes.

Methodology

The research was carried out using tools that allow for a comparative analysis of different theories and related events, which includes a thorough review of the literature on the topic and the cyber capabilities used in modern conflicts. Additionally, documentary research was performed to gather information on strategic guidelines at both the offensive and defensive levels.

In this manner, records were gathered from various bibliographic sources, including journals, scientific articles, books, archival materials, and other academic works. This enabled the development of both a general and a specific understanding of contemporary warfare, as well as the challenges and opportunities facing the SF and Intelligence. While primarily a qualitative study that offers conceptualization, evaluation, and observation, it also incorporates quantitative data to explain the

phenomena observed by collecting digital data, which are analyzed using methods based on mathematical, statistical, or computer techniques.

Afterwards, a comparative and descriptive analysis of each identified scenario is performed, involving the collection of samples to observe how the different variables behave as part of the research problem. Finally, a discourse analysis is conducted on several series of documents, particularly public policies and military doctrines related to cyber capabilities, to elucidate the theoretical framework underlying the concept.

The New Requirements of Contemporary Warfare

In contemporary warfare, various scenarios and events contribute to a nuanced understanding of how armed conflicts are changing. In other words, there are reasons to believe that warfare operates in both physical and virtual domains. This is supported by Patrikarakos (2021), who states that there are two wars: one fought in physical spaces (land, sea, air, and space) and the other occurring in virtual environments (cyberattacks, sabotage, disinformation, and other actions). These factors suggest that a new dynamic is emerging in current conflicts, necessitating innovative approaches to destabilize the enemy during times of war and unrest.

In this scenario, governments worldwide are increasingly focused on shaping social and economic policies through ICTs. As a result, they are beginning to understand the opportunities and challenges of cyberspace while expanding strategies and establishing cyber defense and cybersecurity organizations dedicated to addressing cyber threats. This indicates that nations are only beginning to explore the "Fourth Industrial Revolution" (Connected Industry 4.0), which features a sophisticated integration of production techniques with intelligent systems that connect with organizations and people, while also presenting vulnerabilities that can be exploited to disrupt and harm a nation's critical infrastructure.

In this regard, it is important to note that the needs and specialties of security and defense forces have driven several institutional changes, which have greatly enhanced the protection of critical infrastructure. In other words, cyber capabilities have become an increasingly prominent trend, merging into the unique specialties of each military force. This has led to innovations in their organizations and sparked a positive revolution in managing risks and threats to national security. According to

Kenneth Geers (2009), "Practically everything that happens in the real world is mirrored in cyberspace. For national security planners, this includes propaganda, espionage, reconnaissance, targeting, and—to an unknown extent—warfare itself" (p. 145).

It is worth noting that, according to Geers (2009), five common tactics are used in cyberwarfare: espionage, propaganda, denial-of-service (DoS) attacks, data modification, and infrastructure manipulation. In this context, it can be argued that cyberspace is, ultimately, the "new arena of confrontation" between States, nations, democracies, dictatorships, criminal organizations, and terrorists, among others.

As a result, there is competition between powers and developing countries to establish new enabling structures and organizations that, on the one hand, protect their own cyber capabilities and, on the other, conduct cyber operations with various objectives, primarily aimed at influencing the capabilities of potential threats. Therefore, at this point, cyberwarfare can be said to be emerging.

Based on this overview, the Army Design Methodology (ADM) is outlined below to define how an operational environment (OE) is structured from a systemic perspective during the operational process, especially in relation to cyber capabilities in modern conflicts. To achieve this, a series of network analysis diagrams will be used to visualize and describe the environment. This provides a clear and educational way to display the connections within different networks, helping to understand the OE concerning risks and threats in the cyberspace domain.

It is important to clarify that the OE is defined by the Colombian National Army (Ejército Nacional de Colombia, 2017b) as "the set of conditions, circumstances, and influences that impact the use of capabilities and influence the commander's decisions" (p. 1-2). From this perspective, the following sections outline the operational problem, presenting an overview of key aspects in contemporary conflicts. This will be connected to the strategic guidelines at both the offensive and defensive levels in the cyberspace domain, as well as to the structure of the operational approach.

Strategic Planning Guide 2018–2022

In the *Strategic Plan for the Defense and Security Sector - Strategic Planning Guide 2018–2022* (PES), the Ministry of National Defense (MDN) provided instructions to the Armed Forces to guide the constitutional mission of security forces and to achieve national strategic objectives (MDN, 2018, p. 3). It also sets a roadmap for integrated planning in the defense and security sector over the four-year period, based on an analysis of threats and challenges to national defense and security. Specifically, these were the premises that the MDN (2018) outlined for the Armed Forces:

1. Risks and threats to the State in cyberspace pose a new concern since they can originate from various actors worldwide and aim to achieve objectives linked to different phenomena, such as crime, espionage, sabotage, and terrorism (p. 8).
2. In response to the challenges and threats from the external environment, the PES advocates for defending national interests through a strong strategy that also enhances capabilities in digital security, cyber defense, intelligence, and counterintelligence (p. 9).

General Situation

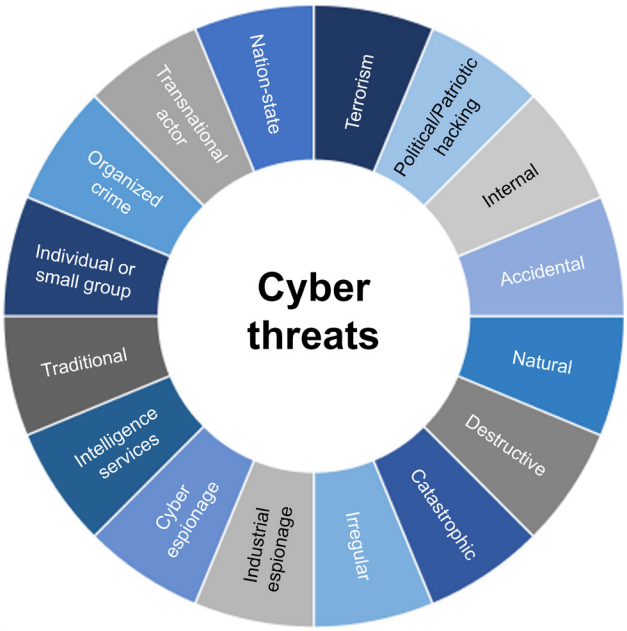
In 1962, the U.S. Department of Defense, through the Advanced Research Projects Agency (ARPA), requested the development of a technology that would enable interconnected communication between different government agencies. Later, in 1969, the message test was successfully completed, creating the first communications network between Stanford University and the University of California, Los Angeles (UCLA).

Then, in 1988, the world saw the emergence of the first malicious code, known as the Morris Worm. As a pioneer in its field, it caused widespread damage to computer networks and systems at the time. It could rapidly self-replicate, directly impacting the internet. Its effects exposed the vulnerabilities within computer systems, highlighting the need for developers to establish security protocols to safeguard against future devastating attacks. Consequently, the events of that year opened new opportunities for creating an enormous variety of malware, which dramatically changed how computer systems could interact. As a result, cyberattacks and cyberespionage came into existence.

In 1990, the European Organization for Nuclear Research (CERN), together with several physicists based in Geneva and Switzerland, developed HTML (Hypertext Markup Language). That same year, the first web client, also known as the World Wide Web (WWW), was created.

However, in the current decade (2020–2030), various threat actors operate in the cyberspace domain (Figure 1), with different types and multiple purposes, including economic, political, intellectual, intelligence, and industrial espionage motives. However, the greatest risk comes from States and intelligence organizations, which, through the manipulation of various structures or groups, carry out their activities in pursuit of specific objectives.

Figure 1. *Cyber Threats*



Source: Own elaboration.

The most common threats in cyberspace can be categorized as follows: nation-state, transnational actor, organized crime, individual or small group, traditional threat, intelligence services, cyberespionage, industrial espionage, irregular threat, catastrophic threat, destructive threat, natural threat, accidental threat, internal threat, political/patriotic hacking, and terrorism.

Structure of the Operational Environment

The new battle typology is set in the post-Cold War era, when computers and online communications were used to address threats through the development and deployment of information aimed at psychological and logistical disruption. It is also marked by the use of information technologies across various organizations at strategic, operational, and tactical levels, involving a wide range of components and resources from armed forces around the world.

In the United States, considered the birthplace of the internet, many thinkers, military personnel, politicians, and others are dedicating time and resources to analyzing the phenomenology of cyber risks and threats, as well as exploring the alternatives needed to sustain leadership in the global cyberspace arena.

For its part, the North Atlantic Treaty Organization (NATO) defines a country's critical infrastructure as consisting of public and private institutions in the agriculture, food, water, public health, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal administration sectors (Geers, 2009).

Furthermore, cyberspace is regarded as the nervous system and control system of a country. It consists of hundreds of thousands of interconnected computers, servers, routers, hubs, and fiber-optic cables that link critical infrastructure. Therefore, the healthy operation of cyberspace is vital to the nation's economy and security.

Problem Identification and Options

The strategic reasons for the rise of cyberwarfare are linked to several key factors. First, the internet is susceptible to cyberattacks. Clearly, no security system offers 100% protection. As a result, there is currently no completely secure system capable of preventing all types of cyberattacks. Besides, the internet's flawed design enables hackers to covertly read, delete, or modify information stored or transmitted between computers. Consequently, attacks armed with constantly evolving malicious code likely have more access points to your network and its secrets than system administrators can effectively defend against.

Second, there is a high return on investment. The goals of cyberwarfare practitioners are clear: stealing research and development data, spying on sensitive communications, and spreading propaganda. What makes hacking stand out is that it can be accomplished at a fraction of the cost and risk associated with other information-gathering or manipulation methods.

Third, cyber defense is inadequate. Cyber defense remains an immature yet constantly evolving field. Traditional law enforcement skills are often insufficient, and it can be difficult to retain personnel with in-demand skills. The global nature of the internet makes cyber investigations even more complex. Lastly, there are no State-sponsored offensive operations in cyberspace, nor is there cooperation between law enforcement agencies.

Fourth, there is plausible deniability. The complex design of the internet gives cyber attackers a high level of anonymity. Savvy hackers can route attacks through countries with which the victim's government has poor diplomatic relations and refuses to cooperate with law enforcement. Even successful investigations often only uncover another hacked computer. Today's governments risk losing a cyber conflict without ever knowing who their real adversary is.

The fifth factor is the involvement of non-state actors. Nation-states strive to maintain as much control as possible over international conflicts; however, globalization and the internet have significantly enhanced everyone's ability to monitor current events and influence them. Transnational subcultures now form spontaneously online and affect numerous political agendas, without answering to any chain of command. In this context, a challenge for national security leaders is that this activity could disrupt delicate diplomacy.

These phenomena seem to confirm that all political and military conflicts have a cyber aspect, the scope and effect of which are hard to predict, as attackers have a wide range of effective cyberwarfare strategies and tactics available to them.

Therefore, the internet is vulnerable to cyberattacks. Its amplifying power means that future victories in cyberspace could result in victories on the ground. Both state and non-state actors see a high return on investment in cyber tactics, from planting carefully crafted propaganda to manipulating an adversary's critical infrastructure.

Weaknesses in the Doctrinal Conception

The doctrinal conception of military forces worldwide regarding these issues is in its early stages, so there is still a long way to go to understand and establish regulations that enable the implementation of strategies, methods, procedures, and tactics to address risks and threats in cyberspace. Consequently, it is necessary to identify and address some key factors in developing a doctrinal approach that enables us to address these challenges. Below, we examine the application of intelligence and cyber capabilities in contemporary conflicts and provide case studies that highlight key aspects to consider in these types of initiatives.

Use of Intelligence

Undoubtedly, the capabilities that cyberwarfare tools give to security and defense forces in intelligence are exceptional. Therefore, it is safe to say that these capabilities continue to offer a significant opportunity to gain a strategic advantage over opponents. Infiltration, penetration, and information gathering are their main strengths, as they ensure the stealthy access points needed for effective intelligence operations.

Cyber Capabilities in Contemporary Conflicts

According to Patrikarakos (2021), "terms like 'hybrid warfare,' 'disinformation,' and 'troll farm'—have all become buzz words of our 'post-truth' age" (p. 3). Furthermore, the possibility of controlling the internet, traffic, mobile phones, and security systems is not a science fiction story, but rather part of the general concept of cyberwarfare. For this reason, "strategists must be aware that part of every political and military conflict will take place on the internet" (Geers, 2009, p. 58).

Cyberattacks have evolved and increased in capacity and complexity; year after year, new viruses, Trojans, or malware emerge. Their ability to disrupt processes, open backdoors, modify code, facilitate information theft, gather data on organizational relationships, and impair systems indicates that the full scope of cyberspace characteristics is still being uncovered.

Therefore, it must be recognized that no software application is completely free of vulnerabilities. In other words, industrial, commercial, military, government, and police systems, among others, will require increased attention, primarily because of the importance of each category and the immediate impact they can have on critical infrastructure. Because of these qualities, they can become targets for various organizations, including hacktivist groups, cybercriminals, cyberterrorists, and nations. It is important to understand that the consequences of these attacks could be devastating to the critical infrastructure of any country.

Case Studies

Below are several case studies related to cyber capabilities in contemporary conflicts, which enable us to identify, evaluate, and analyze the risks and threats that national security and defense institutions face in the general environment of cyberspace.

Chechnya (1994)

In the internet age, unfiltered news from a war zone can arrive instantly. Internet users worldwide play a crucial role in international conflicts by sharing information, whether in text or image form, on websites.

According to Thomas Timothy (2003), since the early days of the World Wide Web, pro-Chechen and pro-Russian forces have conducted a virtual war on the internet, which is happening simultaneously on real battlefields. The Chechen separatist movement, in particular, is seen as a pioneer in using the web to deliver

powerful public relations messages. Skillful placement of propaganda and other types of information, like a bank account number for a war fundraising campaign in Sacramento, California, helped unify the Chechen diaspora.

Furthermore, the most influential information was not pro-Chechen but anti-Russian. Digital images of bloody corpses helped sway public opinion against supposed Russian military excesses. In 1999, while Kremlin officials denied an incident where a Chechen bus was attacked and many passengers were killed, footage of the event appeared online. As technology improved, internet users watched streaming videos showing Chechen military actions favorably, such as ambushes of Russian military convoys (Goble, 1999).

It is worth noting that, according to Goble (1999), the Russian government acknowledged the need to enhance its tactics in cyberspace. In 1999, Vladimir Putin, then Russia's Prime Minister, declared, "We surrendered this terrain some time ago... but now we are entering the game again" (Goble, 1999). Moscow sought Western help in shutting down the prominent pro-Chechen website kavkaz.org and announced "the introduction of centralized military censorship regarding the war in the North Caucasus."

Thus, according to Bullough (2002), during the Second Chechen War (1999–2000), Russian officials were accused of escalating the cyber conflict by hacking Chechen websites. The timing and sophistication of some of the attacks suggested involvement by a nation-state, for example, kavkaz.org, which was hosted in the United States. It was reportedly taken offline at the same time as the assault by Russian special forces, who were conducting a rescue operation inside a Moscow theater besieged by Chechen terrorists.

Kosovo (1999)

In the interconnected conflicts of the internet age, anyone with a computer and an internet connection can become a potential combatant. NATO's first major military engagement took place after the rapid growth of the web in the 1990s. Just as Vietnam was the world's first televised war, Kosovo was its first large-scale internet war.

According to Geers (2020), as NATO planes started bombing Serbia, many pro-Serb (or anti-Western) hacker groups, like the Black Hand, began attacking NATO's internet infrastructure. It is unclear whether any of the hackers directly worked for the Yugoslav military; in any case, their goal was to disrupt NATO military operations.

The Black Hand, which took its name from the Pan-Slavic secret society that helped start World War I, claimed they could identify NATO's "most important" computers and, through hacking, would attempt to "delete the data" they contained. The group reported success in at least some vulnerabilities, particularly in U.S. Navy computers, and said it was subsequently taken offline.

NATO, the U.S., and UK computers were targeted during the war through DoS attacks and virus-infected emails, with 25 different virus strains detected (Geers, 2020). In the U.S., the White House website was defaced, prompting an investigation by the Secret Service. While the U.S. claimed there was "no impact" on the overall war effort, the UK admitted to losing some of its database information.

At NATO headquarters in Belgium, the attacks became a propaganda win for hackers. NATO's public affairs website, which was used to present the organization's side of the conflict through briefings and news updates during the Kosovo war, was nearly inoperable for several days. NATO spokesman Jamie Shea blamed the "line saturation" on "hackers in Belgrade." A simultaneous email flood successfully overwhelmed NATO's email server. As the organization rushed to update nearly all of its computer servers, the network attacks, which initially started in Belgrade, spread worldwide.

Middle East (2000)

During the Cold War, the Middle East often acted as a testing ground for military weapons and tactics. In the internet age, the same has been done with cyberwarfare.

In October 2000, after the kidnapping of three Israeli soldiers, blue and white flags and an audio file playing the Israeli national anthem were placed on a hacked Hezbollah website. Subsequent pro-Israel attacks targeted the official websites of military and political groups seen as hostile to Israel, including the Palestinian National Authority, Hamas, and Iran (Preatoni, 2014).

Retaliation by pro-Palestinian hackers was swift and more varied in scope. Israeli politics, the military, telecommunications, media, and universities all experienced attacks. They also targeted sites of economic importance, including the Bank of Israel, e-commerce platforms, and the Tel Aviv Stock Exchange. At that time, Israel was more connected to the internet than all of its neighbors combined, resulting in numerous targets. The ".il" domain offered a clear list that pro-Palestinian hackers worked through methodically.

As noted, wars often showcase new tools and tactics. Specifically, during this conflict, the DoS program "Defender" was used effectively by both sides,

demonstrating that software can be destabilized more quickly than a tank or a rifle. The defense innovation involved constantly checking the date and time of its simulated web requests, which helped defeat the web caching security mechanisms of the time (Geers, 2004).

Thus, the Middle East cyberwar demonstrated that the internet age and political conflicts can quickly escalate into international conflicts. For example, according to BBC News (2000), the Pakistani "Hackers Club" hacked into the U.S.-based pro-Israel lobby, AIPAC (the American Israel Public Affairs Committee), and published confidential emails, credit card numbers, and contact information of some of its members. Similarly, Page (2000) claimed that "the telecommunications firm AT&T was targeted for providing technical support to the Israeli government during the crisis."

Furthermore, Rebecca Anna Stoil and James Goldstein (2006) asserted that the Middle East cyberwar has generally continued in cyberspace and remains ongoing today. In 2006, as tensions between Israel and Gaza increased, pro-Palestinian hackers shut down about 700 Israeli internet domains, including those of Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel, and McDonald's Israel.

United States and China (2001)

On April 26, 2001, the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC) released Advisory 01-009:

> Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems [...] Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC. (Information Warfare Site [IWS], 2001, p. 86)

Tensions increased sharply between the two nations after the United States bombed the Chinese embassy in Belgrade in 1999, and following the mid-air collision of a U.S. Navy plane and a Chinese fighter jet over the South China Sea in 2001, along with the prolonged detention of the U.S. crew in the People's Republic of China.

According to Jeremy Wagstaff (2001), a reporter for *The Wall Street Journal,* hackers on both sides of the Pacific, such as the China Eagle Alliance and PoizonB0x, started large-scale website defacements and created hacker portals with titles like "USA Kill" and "China Killer." After the cyber skirmishes ended, both sides repeatedly accused each other of defamation and DoS.

In this context, the FBI investigated a 17-day hack of a California power grid test network that started on April 25 (Weisman, 2001). The case was widely dismissed as media hype at the time, but in 2007, the CIA informed industry leaders that not only is a tangible threat from hackers to such critical infrastructure possible, but that it had already occurred (Nakashima & Mufson, 2008).

Estonia (2007)

On April 26, 2007, the Estonian government moved a Soviet World War II memorial from the center of Tallinn, its capital. This action sparked outrage among the public in Russia and among Estonia's Russian minority population.

Starting on April 27, the Estonian government, law enforcement, banking, media, and internet infrastructure faced a series of cyberattacks that lasted three weeks, whose effects continue to attract considerable interest from governments around the world.

Since Estonians perform over 98 % of their banking online, the impact of multiple distributed DoS attacks, which shut down communication with the country's two largest banks for as long as two hours and caused international services to be partially unavailable for days, is understandable.

Less discussed, but likely of greater importance to both national security planners and computer network defense personnel, were the attacks on the internet infrastructure (router) of the Estonian government's ISPs, which reportedly disrupted government communications for at least a "short" period.

On the propaganda front, a hacker defaced the website of the Estonian Prime Minister's political party on April 27, changing the page's text to a purportedly fabricated apology from the government for relocating the statue, along with a promise to return it to its original location.

There was significant diplomatic interest in this cyberattack due in part to the potential reinterpretation of NATO's Article 5, according to which "an armed attack against one [Alliance member] [...] shall be considered an attack against them all" (NATO, 1949, Article 5). It should be noted that Article 5 has only been invoked once, following the terrorist attacks of September 11, 2001. Potentially, it could one day be interpreted to cover cyberattacks as well.

Iran (2010)

One of the most notable cases in the era of cyberwarfare is Iran. Clearly, the development of the Stuxnet worm became a tool capable of seriously impacting

the country's critical infrastructure. Specifically, this attack aimed to disrupt the nuclear activities at the Bushehr reactor. It is worth noting that the goal was successfully accomplished, causing a significant delay in Iran's nuclear program.

The unique characteristics of this case show that its entire execution meets the ideal conditions for cyberwarfare. Therefore, it can be concluded that the creation of this cyberweapon ultimately served as an effective tool that impacted Iran's national interests. Additionally, establishing an infiltration and deception operation to activate it and compromise a country's computer networks—leaving them vulnerable to various types of attacks (Porteus, 2010)—can only be described as clever and innovative.

Ukraine (2014)

Ukraine served as a testing ground for new types of information operations (Patrikarakos, 2021). On November 21, 2013, Mustafa Nayyem, a Ukrainian journalist of Afghan descent, posted on Facebook, urging people to gather at Maidan Nezalezhnosti (Independence Square) in Kyiv. He aimed to protest President Viktor Yanukovych's decision to reverse his commitment to sign an association agreement with the European Union, which would have strengthened their political and economic ties.

On the anniversary of this cyberwar, as companies prepared for another round of hacking, the Chinese government reportedly succeeded in a last-minute withdrawal, implying that Chinese hackers may have a higher level of coordination than their American counterparts (Hess, 2002).

Operational and Strategic Scope of Military Intelligence

The internet is transforming many aspects of life, including how warfare is conducted. Sometimes, cyber tools and tactics favor nations with strong information technology infrastructure. However, the internet is a powerful resource that smaller or weaker groups can use to attack a more powerful traditional enemy. Like terrorism and weapons of mass destruction, the ever-changing, asymmetric nature of cyberattacks prompts questions about all elements of cyber defense—such as detection, analysis, investigation, prosecution, retaliation, and more—for national security and defense planning.

As seen in the case studies, it is clear that the operational and strategic scope of military intelligence can greatly benefit from the use of cyber tools to achieve its goals. There is no question that their potential must be examined from a national security and defense perspective, in accordance with both national and international laws.

Therefore, analyzing, designing, developing, testing, and using cyber weapons in the near future are actions that will shape the next step in the evolution of cyberwarfare. It should be noted that the strategic and operational levels of military intelligence must work together to provide the necessary resources, methods, techniques, tactics, and procedures to accomplish future intelligence missions.

Nevertheless, it is essential not to forget that contemporary war scenarios have limits and gray areas that must be considered.

Contemporary War Scenarios

Patrikarakos (2021) argues that conflict is guided by two principles: first, that force is not always the best way to reach strategic goals, and second, that 20th-century geopolitical and security models are insufficient for today's threats. Therefore, using cyberspace as a new battlefield plays a crucial role in creating the impact needed to meet objectives.

At this point, it is essential to note that several factors suggest that modern war scenarios are increasingly focused on traditional domains of warfare. The areas of knowledge, influence, or activity, and the territory where dominance is exercised, become useful tools that help describe broad areas of understanding and visualize the environment where operations occur (Ejército Nacional de Colombia, 2017b).

Considering that "cyberspace is a global domain within the information environment composed of interdependent networks of information technology infrastructure and data, which include: the Internet, telecommunications, networks, computer systems, and integrated processors and controllers" (Ejército Nacional de Colombia, 2017b, p. 491), its significance in modern conflicts should be emphasized. Consequently, it must be utilized to its fullest potential to gain a strategic advantage against the adversary.

Gray-Zone Conflicts

National and international laws prohibit security and defense agencies from acting irrationally or illegally; therefore, these gray areas are heavily exploited by threats. In other words, the locations, areas, and illegal activities carried out have several

key supports, including secrecy, encryption, geographic sanctuaries, and legal loopholes.

In this regard, it is worth noting that secrecy allows actors considered threats to carry out actions without being identified, and in some cases, it is also impossible to determine why they carry out their plans. Furthermore, encryption enhances this by hindering forensic identification of the criminal network. For its part, geographic sanctuary benefits cybercriminals, as they enjoy protection from other States. Ultimately, loopholes in the law form the foundation of cybersecurity and cyber defense, indicating that without adequate tools, a meaningful response to threats cannot be achieved.

Conclusions

Strategists must recognize that part of every political and military conflict occurs online, and because of its widespread and unpredictable nature, battles fought there can be just as crucial, if not more so, than those on the actual battlefield.

The case studies indicate that it is no longer just hackers who caught national security and defense planners off guard, but rather more complex structures, organizations, and States that need to be examined from a wider perspective.

The landscape of modern warfare has shifted with the rise of cyberspace; therefore, any nation that does not dedicate itself to strengthening its cybersecurity and cyber defense measures today is walking a high wire, partly supported by land, sea, air, and space domains. In essence, they would not be strong enough to compete with cyber threats.

Additionally, the widespread presence of risks in cyberspace necessitates the activation of cyber intelligence at the strategic, operational, and tactical levels, which is essential for identifying, categorizing, and comprehending adversaries in cyber warfare.

Nothing can stop nations or States from building functional cyber capabilities, but ingenuity, expertise, and knowledge are crucial for success in cyberspace operations. Similarly, understanding the overall situation, the structure of the OE, and identifying problems enables the development of operational art options that support better decision-making on the battlefield.

References

BBC. (2000, November 3). *Israel Lobby Group Hakend.* https://tinyurl.com/muukxy4p

Bullough, O. (2002, November 14). Russians wage cyber war on Chechen websites. *InfoSec News.* https://tinyurl.com/44h6c2vt

Colom, P., Coz, J., Fojón, E., & Hernández, A. (2013). Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales. *ARI,* (26), 1–10. https://tinyurl.com/2p8puuvv

Ejército Nacional de Colombia. (2017a). *Manual Fundamental de Referencia del Ejército MFRE 1-01 Doctrina [Public].* Imprenta Ejército. https://tinyurl.com/2vpdpwpn

Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones [Public].* Imprenta Ejército. https://tinyurl.com/ducm7tje

Ejército Nacional de Colombia. (2019). *Manual de Técnicas del Ejército MTE 5-01 Metodología de Diseño del Ejército [Public].* Imprenta Ejército. https://tinyurl.com/3zjfspr2

Geers, K. (2004, April 4). *Cyber Jihad and the globalization of warfare: Computer networks as a battle ground in the Middle East and beyond* [Slide presentation]. https://tinyurl.com/yjabbbax

Geers, K. (2009). *Cyberspace and the changing nature of warfare* [Keynote Speech IST-076/RSY-017]. OTAN. https://tinyurl.com/bddy3pa

Geers, K. (2020). #Cyberwar: International Conflict in Cyberspace. In *Alliance Power for Cybersecurity* (pp. 3–5). Atlantic Council. https://tinyurl.com/y5p2pajx

Goble, P. (1999, October 9). *Russia: Analysis from Washington – A real battle on the virtual front.* https://tinyurl.com/5f798nju

Hess, P. (2002, October 29). *China prevented repeat cyber-attack on US.* https://tinyurl.com/435u3bwz

Information Warfare Site [IWS]. (2001). *The Information Warfare Site.* https://tinyurl.com/ycyzbxu2

Ministerio de Defensa Nacional. (2018). *Plan Estratégico del Sector Defensa y Seguridad. Guía de Planeamiento Estratégico 2018-2022*. https://tinyurl.com/2sh6v5mt

Nakashima, E., & Mufson, S. (2008, January 19). Hackers have attacked foreign utilities, CIA analyst says. *Washington Post.* https://tinyurl.com/43nc2fbm

North Atlantic Treaty Organization [NATO]. (1949, April 4). *The North Atlantic Treaty.* https://tinyurl.com/yc2ujn2t

Page, B. (2000, November 11). Pro-Palestinian Hackers Threaten AT&T. *TechWeb News.* https://tinyurl.com/5n7wnenj

Patrikarakos, D. (2021). *Un muy moderno "niebla de guerra", Ucrania: siete años después.* CHARCR.

Porteus, H. (2010, June 10). *The Stuxnet Worm: ¿Just another computer attack or a game changer?* [In Brief, No. 2010-81-E]. Parliament Information and Research Service of Canada. https://tinyurl.com/2hu9uasw

Preatoni, R. (2014, August 10). *Calling All Hackers*. https://tinyurl.com/29w58ryh

Timothy, T. (2003). Information warfare in the seconds (1999-) Chechen War: Motivator for military reform? In A. C. Aldis & R. N. McDermott (Eds.), *Russian military reform 1992-2002*. Routledge.

Wagstaff, J. (2001, April 30). The internet could be the site of the next China-US Standoff. *The Wall Street Journal*. https://tinyurl.com/yuk6r3j2

Weisman, R. (2001). *California power grid hack underscores threat to U. S. news factor.* https://tinyurl.com/f7nyz54y


EDITORIAL ESDEG

Commandos

Challenges Facing Special Forces and Intelligence in Contemporary Warfare

Contemporary warfare presents unprecedented challenges. Today, armies face more diffuse adversaries, with a mix of traditional and new threats adding to the already complex gray-zone environments. In this context, special operations and intelligence take on a leading role. These highly flexible, adaptive, interoperable, and stealthy units, with their diverse and advanced technological capabilities, are essential for confronting today's adversaries.

However, they need to be reconsidered. The essential capabilities of Special Forces must be reassessed to find new approaches for tackling these challenges. Likewise, intelligence must adapt to increasingly global environments, with tactical and operational intelligence merging with strategic intelligence. Therefore, intelligence and Special Forces must collaborate more deeply than in the past, nearly blurring the line between the two.

This book explores relevant and contemporary debates about the use of Special Forces and Intelligence in modern warfare. It is the outcome of four years of academic reflection and research by the Army Department of the Escuela Superior de Guerra "General Rafael Reyes Prieto." These insights are especially important given the specific nature of the topic and the limited academic research on Special Operations.

EDITORIAL ESDEG

ISBN 978-628-7818-39-2