

## Chapter 11

# Intelligence Operations and Gray-Zone Wars<sup>\*</sup>

---

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](mailto: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](mailto: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 battlefield 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 & Inántszy-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

| GRAY ZONE                      |        | STRATEGIES  |                                |         | INTELLIGENCE OPERATIONS          |
|--------------------------------|--------|---|--------------------------------|---------|----------------------------------|
| AMBIGUITY                      | IMPACT | Operations influencing international and adversary public opinion |                                | THROUGH | ESPIONAGE                        |
|                                |        |   |                                |         | SABOTAGE                         |
| GRADUALISM                     |        | Economic coercion   | Offensive intelligence actions |         | DECEPTION                        |
| SUBSTANTIAL INTERESTS AT STAKE |        | Proxy wars  | Sliced salami tactics          |         | PSYCHOLOGICAL OPERATIONS         |
|                                |        | Cyberattacks against public and private entities                  |                                |         | INFORMATION GATHERING OPERATIONS |
| MULTIDIMENSIONAL STRATEGIES    |        |   | NEUTRALIZATION                 |         |                                  |

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/3f7vpwr>
- 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/vybjfffy>
- 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., & Inántszy-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 nexos 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.