

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/kahaps392>
- 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/duc7tje>
- 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/3hrsiv5x>
- 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>