

Chapter 4

Contemporary Cyber Threats: Challenges for Special Operations in Colombia*

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

José Nicolás Rodríguez Rodríguez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Oscar Garzón

Joint Special Operations Command

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

Keywords: threats; capability; cyber; warfare.

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

José Nicolás Rodríguez Rodríguez

Lieutenant Colonel in the Colombian National Army's Special Forces. Master's (cum laude) in Cyber Defense and Cybersecurity, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Military Unit Leadership and Specialization in National Defense Resource Management, National Army Arms and Services College. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Bachelor's in Business Administration, Universidad Politécnico Gran Colombiano. Email: jose.rodriguezrod1@buzonejercito.mil.co

Oscar Garzón

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

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

COMMANDOS: CHALLENGES FACING SPECIAL FORCES AND INTELLIGENCE IN CONTEMPORARY WARFARE

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

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

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

Security and Defense Collection

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Threats to Colombia's Security and Defense with Cyber Capabilities

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

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

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

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

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

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

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

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

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

Indeed, according to Medina-Ochoa (2019),

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cyber Capabilities in the Special Forces

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

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

Education and Cyber Culture

For Conti and Surdu (2009),

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

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

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

Doctrinal Legitimacy in the Cyber Environment

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

Cyber Special Forces in the National Army

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

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

Cyber Cell Capabilities

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

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

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

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

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

Recruiting Ethical Hackers

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

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

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

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

The Department of Special Operations in Cyberspace

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

Conclusions

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

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

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

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

References

- Aguilar-Antonio, J. M. (2019). Hechos ciberfísicos: Una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (25), 24–40. <https://doi.org/10.17141/urvio.25.2019.4007>
- Arteaga, F. (2019). Disrupción tecnológica y orden global. *Revista UNISCI*, (51), 109–128. <https://tinyurl.com/mrxnrzst>
- Barbe, E. (1987). El papel del realismo en las relaciones internacionales: Teoría de la política internacional de Hans J. Morgenthau. *Revista de Estudios Políticos*, (57), 149–176. <https://tinyurl.com/mpwzp726>
- Bassets, M. (2015, February 8). El más fuerte es el más vulnerable: EE.UU. es víctima y, a la vez, el más poderoso agresor en el 'cibertablero' mundial. *El País*. <https://tinyurl.com/mrx756zy>
- Beleño, B. (2020). *Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam* [Specialization capstone, Universidad Nacional de Colombia Abierta y a Distancia]. Repositorio UNAD. <https://tinyurl.com/2susm9p9>
- Colom, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova*, 10(10), 77–90. <https://doi.org/10.21830/19006586.228>
- Colom, P., Coz, J., Fojón, E., & Hernández, A. (2013). Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales. *ARI*, (26), 1–10. <https://tinyurl.com/2p8puuvv>
- Consejo Nacional de Política Económica y Social [CONPES]. (2016). *Política Nacional de Seguridad Digital, CONPES 3854*. Departamento Nacional de Planeación. <https://tinyurl.com/bdzhjvdy>
- Conti, G., & Surdu, J. (2009). Army, Navy, Air Force, and Cyber: Is it time for a cyberwarfare branch of military? *A Newsletter*, 12(1), 14–18. <https://tinyurl.com/2bscnp7h>
- Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 18(30), 357–377. <https://doi.org/10.21830/19006586.588>
- Ejército Nacional de Colombia. (2018). *Manual de Campaña del Ejército MCE 318 Operaciones de Fuerzas Especiales [Restricted]*. Imprenta Ejército.
- El Tiempo*. (2020, October 25). ¿Quién era y cómo operaba "Uriel", el terror del ELN en Chocó? <https://tinyurl.com/shjz4t8x>
- Espitia, A., Agudelo, J., & Ramírez, T. (2021). Percepciones sobre innovaciones tecnológicas en el Ejército colombiano. *Revista Logos, Ciencia & Tecnología*, 13(2), 85–102. <https://doi.org/10.22335/rict.v13i2.1408>
- García, B. (2022, March 9). Las Fuerzas Especiales de Rusia: ¿Quiénes son los Spetsnaz? *Noticiero Televisa*. <https://tinyurl.com/4d4dxhec>
- González-Martínez, M. A., & Montero-Moncada, L. A. (Eds.) (2020). *El tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder ciber en el siglo XXI*. Sello Editorial ESDEG. <https://doi.org/10.25062/9789584288943>
- Guerrero Vallejo, G. Y. (2022). *Operaciones cibernéticas y seguridad hemisférica en Colombia: Análisis desde la cooperación regional e internacional* [Master's thesis, Universidad Santo Tomás]. Repositorio USTA. <https://tinyurl.com/2s3s5st3>

- Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Potomac Institute for Police Studies. <https://tinyurl.com/dyc5rmnv>
- Inter-American Defense Board. (2020). *Cyber Defense Handbook. Guidelines for the Design, Planning, Implementation and Development of a Military Cyber Defense*. https://jid.org/wp-content/uploads/2022/01/Cyber-defense_handbook_ing.pdf
- Medina-Ochoa, G. (Ed.) (2019). *La seguridad en el ciberespacio, un desafío para Colombia*. Sello Editorial ESDEG. <https://doi.org/10.25062/9789585216549>
- Miguel-Gil, J. (2019). El tratamiento informativo de la guerra híbrida de Rusia. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (25), 108–121. <https://doi.org/10.17141/urvio.25.2019.4006>
- Ministerio de Defensa Nacional. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia*. <https://tinyurl.com/455ky3f2>
- Miranzo, M., & Del Río, C. (2014). La protección de infraestructuras críticas. *UNISCI Discussion Papers*, (35), 339–352. <https://tinyurl.com/36k8z69t>
- Mitaritonna, A. D. (2019). *Empoderamiento de la conciencia situacional en operaciones militares utilizando realidad aumentada* [Doctoral dissertation, Universidad Nacional de La Plata]. Repositorio UNLP. <https://tinyurl.com/yuz3ucke>
- Nieva, M., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *UNISCI Journal*, (42), 47–68. <https://tinyurl.com/mrejyh6a>
- Organization of American States [OAS]. (2019). *Media Literacy and Digital Security: The Importance of Staying Safe and Informed*. <https://www.oas.org/en/sms/cicte/docs/Media-Literacy-and-Digital-Security.pdf>
- Patiño Orozco, G. A. (2019). El sistema internacional cibernético: Elementos de análisis. *Oasis*, (30), 163–186. <https://doi.org/10.18601/16577558.n30.10>
- Pons Gamón, V. (2017). Internet, la nueva era del delito: Cibercrimen, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 80–93. <https://doi.org/10.17141/urvio.20.2017.2563>
- Poveda Criado, M. A., & Torrente Barredo, B. (2016). Redes sociales y ciberterrorismo: las TIC como herramienta terrorista. *Opción*, 32(8), 509–518. <https://tinyurl.com/mr3r78tc>
- Realpe, M. E., & Cano, J. (2020). Amenazas cibernéticas a la seguridad y defensa nacional: reflexiones y perspectivas en Colombia. In V. Gauthier, R. A. Méndez, J. Cano, J. Ramió & L. E. Sánchez (Eds.), *Seguridad informática: X Congreso Iberoamericano, CIBSI 2020* (pp. 105–113). Universidad del Rosario. <https://doi.org/10.12804/si9789587844337.10>
- Sánchez, D. R., & Rodríguez, F. (2010). Seguridad nacional: el realismo y sus contradictores. *Desafíos*, (15), 119–177. <https://tinyurl.com/mu2vbm6>
- Sancho, C. (2017). Ciberseguridad: Presentación del dossier. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 8–15. <https://doi.org/10.17141/urvio.20.2017.2859>
- Vergara, E., & Trama, G. A. (2017). *Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina. <https://tinyurl.com/mr3cyap4>