Cyber Risk Management Associated with the Use of Satellite Antennas in the National Army

Nubia Edith Céspedes Prieto[1], Fabian Esteban Cano Jaime[2]

[1]Escuela de Ingenieros Militares, Ejército Nacional de Colombia, Bogotá 111611, Colombia.
Email: nubia.cespedes@esing.edu.co; necespedesp@unal.edu.co, ORCID: https://orcid.org/0000-0002-5248-3898
[2]Escuela Superior de Guerra "General Rafael Reyes Prieto", Ejército Nacional de Colombia, Bogotá 111611, Colombia., Email: fabian.cano@esdeg.edu.co, ORCID: https://orcid.org/0000-0002-6645-9303

Abstract
Digital connectivity is now essential for efficient and secure military operations. However, the Colombian National Army faces significant challenges due to the limited coverage and low quality of its internal network (INTRANET), forcing personnel to rely on commercial solutions such as satellite antennas. While these alternatives provide advantages like global coverage and high speed, they introduce considerable cyber risks, including communication interception that could compromise national security. This article analyzes SATCOM systems and their role as technological infrastructure within the military, detailing their strategic and tactical applications. It identifies inherent vulnerabilities in these technologies such as jamming, spoofing, or attacks targeting ground segments which highlight the urgency of evaluating and strengthening cyber defense strategies. The adoption of appropriate techniques and standards is crucial to mitigate risks and protect military communications against emerging cyber threats.

Keywords: satellite antenas, cyber risks, cyberspace, cyber defense, cybersecurity.

Introduction

Currently, digital transformation has enhanced the importance of connectivity in the military environment, where efficiency and security depend to a large extent on the ability to maintain stable and secure communications. The Colombian National Army faces the challenge of an institutional network with insufficient coverage and quality, which has led, in practice, to many units opting for commercial solutions such as commercial satellite antennas (Colombian National Army. 2021. Management Report of the Communications and Cyber Defense Operational Support Command (CAOCC)). This choice, while resolving immediate connectivity gaps, includes a range of cyber risks: from information interception and unauthorized access to widespread exposure to threats in cyberspace. As a result of this problem, this article aims to apply a methodology that allows managing and mitigating cyber vulnerabilities and threats derived from the use of commercial satellite antennas in the development of military operations. For this, a mixed methodology was used, combining qualitative and quantitative methods with a projective approach through surveys of military personnel, where the data was analyzed through the application of the JASP statistical tool. (Santamarta, n.d .)

The results obtained show that only 52% of the units have institutional network coverage, while the rest resort to commercial solutions to fulfill their functions. Moreover, about 45% of these alternative connections are used in administrative tasks, 33% in operations and 22% in training, which highlights the associated operational risk. The main reasons for using these external networks are the search for better connectivity (44%), wider coverage (48%) and higher speeds (17%). It is worrying that more than 80% of the staff recommends the use of these solutions and that approximately 60% do not implement any security measures or perceive the risks inherent in the use of commercial networks, a fact that is partly explained by the lack of knowledge or training in cybersecurity and cyber defense. Analyzing the satellite communications market, it was identified that, despite the existence of more than 18 satellite internet providers in Colombia, only four concentrate most of the institutional demand, with SpaceX's Starlink standing out for its advantages in cost, ease of use and coverage. (Shaengchart & Kraiwanit , 2023)

The study highlights the urgency of increasing awareness of cyber risks and improving cyber defense strategies, promoting the adoption of security measures and the development of institutional capabilities to safeguard the integrity of communications and information in military operations.

Methodology

The methodology applied in this research was based on a mixed method, integrating qualitative and quantitative techniques, and was characterized by its projective approach in relation to the management of cyber risks associated with the use of satellite antennas in the operations of the Colombian National Army. First, a survey-type data collection instrument was designed and applied to military personnel present in various areas of the

country, achieving coverage of more than 80%, with the purpose of exploring connectivity conditions, usage practices, security perceptions and protection measures implemented in the management of commercial satellite networks. The questions addressed variables such as institutional coverage, activities related to the use of alternative media, reasons for adopting these solutions, and knowledge about vulnerabilities and threats.
The projective approach allowed the research to be oriented towards the identification of future strategies for the management and mitigation of the risks detected, promoting a proactive vision in institutional decision-making. The collection of information was carried out with an instrument validated by expert peers, under criteria of anonymity and voluntariness, ensuring the validity of the data. The quantitative analysis was developed with the JASP statistical tool, complemented by a qualitative analysis that interpreted the experiences and perceptions of the staff, managing to integrate both perspectives. This methodology made it possible to determine the problem and its operational impact, as well as to propose actions to strengthen the institution's cyber defense and cybersecurity capabilities.

The Reality of Military Communications in Colombia

For several years, the National Army has had to carry out operations in one of the most complex geographical areas. Because of this, for some time now, satellite antennas have become the best allies to guarantee communication and control of military units, allowing those in the most remote areas or in the highest mountains to communicate. Without these tools, it would simply not be possible to carry out the development of the different activities that are carried out on a daily basis. The problem is that, over time, they have come to depend on them for everything, from administrative or logistical processes, training and even in the area of operations, becoming the weak point that enemies know well.
The conflict in which Colombia is currently facing is no longer only about combats in the area of operations, now, the same conflict has evolved along with current technologies, venturing into the domain of cyberspace. Different groups with malicious intent, both from other countries and internally, have the ability to launch cyberattacks against infrastructure. And, as expected, military communications are one of their preferred targets. It is identified that, worldwide, satellite signals can be jammed, receivers can be deceived with false information or, in the worst case, take control of equipment. This new reality shows the weaknesses of how vital tools are being defended.
The Colombian National Army has generated mechanisms for the attention and protection of communication networks and databases, but the results show that for the protection of physical equipment it has been insufficient for the development of the activities required in the service, one of these being satellite antennas. There are protocols for the handling and management of the media as established in Permanent Directive No. 0118000010005/2018 "Guidelines for the Direction of Information Technologies of the Military Forces" is the one that regulates the use of satellite antennas and personal or alternative means of communication for the protection of information. in turn, there is permanent directive 101 of the General Command of the Military Forces "Cybersecurity and Cyber Defense Guidelines for FF.MM." which focuses on policies and guidelines for protection in cyberspace, but does not regulate or detail the physical use of antennas, or alternative or personal means. The current regulations leave a significant gap, in the face of the specific digital risks for devices and new communication alternatives related to 4G and 5G technology, a gap that urgently needs to be closed.
It is precisely for this reason that this research arises. With the purpose of studying what are the vulnerabilities presented by the antennas used daily for the fulfillment of activities, both operational and administrative. The idea is to lay the groundwork for creating a clear and practical plan to make it easier to manage these new risks. The goal is to ensure that communications remain secure and reliable so that the Army can fulfill its mission no matter what challenges arise on the ground or in the cyber world.

The appeal of business solutions

The evolution of new technologies in which different companies have invested billions of dollars makes satellite communication an innovative system with greater capacity and lower latency in terrestrial and aerial networks, optimizing factors such as bandwidth, latency, security and availability, guaranteeing uninterrupted communication even in the most remote areas. (communication via the Internet on the satellite platform, n.d .)
Companies such as SpaceX's Starlink have positioned themselves on the planet for their service and infrastructure, their systems are more advanced, economical and faster than the technology currently available to the Army. It is characterized by its large constellation, which as of July 2025 has 7,885 satellites in orbit (https://www.space.com/spacex-starlink-satellites.html), Musk (2021) had promised global coverage with lower latencies than traditional systems, with a distance of 500 km from the earth's surface with a performance similar to that of fiber optics that would reach an increase of up to 100 times the bandwidth if we compare it to geostationary satellite systems (GEO).
On the other hand, in Colombia companies such as HughesNet, Skynet, GlobalTT among others, use geostationary satellites (GEO), which means that they are 36,000 km away from the earth's surface, which implies greater latency and with it other disadvantages compared to Starlink, not to mention the physical part in terms of its infrastructure and operation.

The ease of use of Starlink antennas as well as portability is also a plus. Well, anyone can learn to operate one of these devices in less than an hour. It does not require years of technical training or training, or specialized knowledge in this type of device. Simply turn on the computer, point it towards the sky and you have internet service. It's as simple as using a cell phone. This operational simplicity contrasts drastically with traditional military systems that require specialized, certified personnel and complex installation and maintenance procedures.

In terms of costs, they also favored these solutions, taking into account that the plans and equipment are economically affordable in the market for these technologies, highlighting that the equipment is owned by the user and does not require a permanence clause (https://www.starlink.com/co/service-plans), all these factors make them more attractive and as a possible more precise alternative to guarantee the quality and connectivity of communications.

Establishing a high-speed internet network means being able to transmit video in real time, download high-resolution satellite images and use modern applications for the development of military operations (Logic Fruit Technologies. (2024). Secured Communication Solutions in Defense & Military). The new capabilities allow for the integration of advanced geographic information systems, multimedia communications and platforms on which operations are planned and executed.

Countries that use StarLink satellites in military operations

Country	**Employment**
Ukraine	As an essential tool for command communications, drone coordination, logistics, internet in forward bases, and backup in areas where conventional infrastructure was destroyed. https://www.dw.com/es/qu%C3%A9-pasar%C3%ADa-si-eeuu-desconectara-starlink-en-ucrania/a-71839124
United States	Support to air and naval bases, connectivity demonstrations, and interoperability tests between command and control systems during maneuvers https://danielmarin.naukas.com/2024/06/30/la-megaconstelacion-militar-starshield-de-spacex-toma-forma/
Brazil	To maintain connectivity in isolated areas, particularly in the Amazon and maritime areas, facilitating patrol exercises, training and logistics operations. https://apublica.org/2024/10/starlink-militares-usam-internet-via-satelite-de-elon-musk-sem-teste-de-seguranca-da-rede/ #

The Hidden Dangers

When Russia attacked Ukraine

The events of February 2022 changed everything. The Russian attacks on Viasat's networks were not accidents or side effects. They were deliberate and well-planned attacks on civilian infrastructure supporting military operations (CISA, 2022). The Russians knew exactly what they were doing: cutting off communications to sow chaos before the invasion. The precision and timing of these strikes demonstrated a level of planning that had been in development for months, possibly years, suggesting that anti-satellite capabilities were integral to modern Russian military doctrine.

Most troubling was the sophistication of the attacks. They were not simple signal blocks. The Russians managed to break into their systems, tamper with the software, and cause permanent damage to thousands of terminals. This showed that they had technical capabilities specifically developed to attack commercial satellite systems. Subsequent analysis revealed that the attackers had studied the specific vulnerabilities of each system in detail, developing custom tools to exploit weaknesses that manufacturers were unaware of. This preparation suggests specialized research programs in anti-satellite warfare that had been operating in secret for years.

Then came the attacks on Starlink. Groups associated with Russian intelligence, especially one known as Secret Blizzard, began targeting Ukrainian military devices that used these antennas (TheSIGN, 2024). They did not attack satellites directly, but used more subtle techniques: infiltrating soldiers' mobile devices, installing malicious software, and stealing information about troops' locations and activities. This indirect approach showed a sophisticated understanding of how modern military operations actually work, where satellite systems are integrated with multiple devices and local networks.

The Security Agency of Ukraine discovered a malicious program specifically designed to attack Starlink systems, which they called "Malware 4.STL" (Cyber Defense Magazine, 2024). This program used soldiers'

phones to gather information about the antennas: where they were located, what kind of data they transmitted, and when they were most active. It was a clever way to attack: instead of blocking signals directly, they gathered intelligence for more effective future attacks. The malware demonstrated detailed knowledge of Starlink's internal communications protocol and the ability to operate undetected for extended periods.

Technical vulnerabilities

Security researchers had been warning about these problems for years. Santamarta (2018) had documented serious vulnerabilities in satellite terminals that included apparent backdoors, fixed passwords in software, and insecure communication protocols. But the industry didn't pay much attention until the actual attacks began. The industry's resistance to implementing security improvements was partially due to cost considerations and the perception that threats were theoretical rather than practical. This situation changed after the events in Ukraine, when it became clear that academic vulnerabilities had become operational attack vectors.

Lennert Wouters, a cybersecurity specialist at KU Leuven University (Leuven), Belgium, demonstrated something particularly alarming at a security conference. With a modified chip that cost just $25, he was able to hack into a StarLink terminal and evade all its security measures. This showed that the attacks did not require huge resources or advanced military technology. A clever attacker with basic knowledge of electronics could compromise these systems. The demonstration was especially impactful because it used commercially available components and techniques documented in academic literature, suggesting that any adversary with modest resources could replicate the attack.

Subsequent investigations were even more troubling. Liu et al. (2024) found evidence that more than 8,675 Starlink terminals had been used for malicious activities, including automated attacks against other systems. This meant that the network was not only vulnerable to external attacks, but could also be used as a platform to attack other targets. The compromised terminals formed a distributed network (botnet) that could be remotely controlled to launch coordinated attacks, turning the communications infrastructure into a cyberweapon directed against other systems.

The study identified more than 8,700 security vulnerabilities in the network, from minor issues to critical flaws that could allow full control of endpoints. Most concerningly, many of these vulnerabilities existed by design: the systems were optimized for ease of use and cost, not military security. The fundamental architecture prioritized accessibility and scalability over protection, reflecting commercial market priorities where military security was not a primary consideration.

Specific Threats

Interception and Espionage

Listening to other people's military conversations is a practice as old as war itself. What has changed is how easy it has become to do so. Graham et al. (2020) explain that anyone with amateur radio equipment can intercept basic satellite signals. Although deciphering content requires more resources, simply knowing when and from where troops are communicating is already valuable information. Traffic analysis techniques make it possible to extract significant intelligence even from encrypted communications, by studying patterns, volumes and synchronization of transmissions. Modern automated interception systems can process thousands of communications simultaneously, identifying patterns that would be impossible to detect through manual analysis.

Communication patterns reveal a lot without needing to understand conversations. If a unit suddenly increases its communications traffic, it's probably planning something important. If communications are concentrated at certain times, that indicates routines that can be exploited. If the volume of data transmitted changes, it may mean that they are receiving new orders. Machine learning algorithms can identify subtle correlations between communication patterns and operational activities, enabling predictions about future operations based solely on traffic metadata (Spanish Ministry of Defense. 2024. Artificial intelligence as a factor in the transformation of military operations at the operational level)

Analysts can track specific terminals and create detailed maps of military movements. Each terminal has unique features, such as an electronic fingerprint, which allows you to follow it through time and space. This is especially dangerous for special units that rely on secrecy for their operations. Electronic fingerprinting techniques have evolved to detect minute differences in hardware components, software configurations, and usage patterns that make each terminal unique. This individualization allows for persistent tracking even when superficial identifiers such as serial numbers or network addresses are changed.

Nogueira et al. (2019) document how this information can be used to anticipate military operations. If the patterns show that a unit is moving into a specific area with intense communications, they are likely planning an operation in that area. Criminal groups can use this information to abandon drug labs, set up ambushes, or simply avoid contact. The predictive capability of these analytics has been significantly improved with the use of artificial intelligence that can correlate multiple sources of information to generate operational predictions with alarming accuracy.

Blocking and Interference

Blocking military communications has been a tactic of war for decades. What's new is how sophisticated these techniques have become. It's no longer simply about transmitting noise to saturate frequencies. Modern systems can adapt their attacks in real-time, track frequency changes, and mimic legitimate signals to confuse receivers. Modern jammers incorporate adaptive tracking algorithms that can automatically identify and counteract the anti-jamming techniques used by target systems. This electronic weapons competition has led to increasingly sophisticated jamming systems that can operate autonomously for extended periods.

Uplink blocking is particularly effective because it can be done from the ground, relatively close to the target troops. A well-positioned jamming transmitter can easily silence a military unit that relies on a low-power satellite terminal. This is especially concerning for small patrols or special units operating far from support. Portable jamming transmitters are now much smaller, allowing some attacking groups to carry them and strategically position them near military units without being detected. Colombia's mountainous geography provides multiple vantage points from which it is possible to launch effective jamming attacks.

In Compliance Magazine (2024) describes adaptive jamming techniques that can automatically follow the system's attempts to change frequencies or protocols. These "smart" systems learn from defense attempts and adapt to maintain effective interference. It's like a game of cat and mouse, but automated and at electronic speed. The most advanced systems incorporate machine learning capabilities that can predict defensive responses and prepare countermeasures before they are implemented, creating a persistent jamming cycle that is extremely difficult to break.

Deception and False Signals

Sending false signals to confuse the enemy is another old tactic that has been modernized considerably. Spoofing attacks can make a military terminal think it is receiving legitimate orders when in fact it is being manipulated by the enemy. Falco and Boschetti (2021) document cases where these attacks have managed to fool even sophisticated military systems. The effectiveness of these attacks has increased dramatically with the development of artificial intelligence systems that can analyze and replicate legitimate communication patterns with extraordinary accuracy.

The most famous case occurred in 2011, when Iran managed to shoot down a U.S. RQ-170 drone using fake GPS signals. The Iranians did not fire any missiles or use traditional jamming. They simply sent fake GPS signals that made the drone think it was flying over Afghanistan when in fact it was over Iranian territory. The drone landed "softly" in Iran, believing it had returned to its base. This incident showed that spoofing attacks could be more effective than traditional countermeasures, as they exploited systems' reliance on their own sensors.

In the context of communications, these attacks can be used to insert false information into military channels. A sophisticated attacker could send fake commands that appear to come from higher commands, modified intelligence reports, or even incorrect coordinates for airstrikes. The key is to make false information convincing enough to go unnoticed. Modern spoofing systems can replicate not only the content of communications but also the technical patterns, transmission times, and signal characteristics that operators use to verify authenticity.

Massimi et al. (2023) explain how these attacks can be combined with social engineering to be more effective. Attackers can use information obtained from open sources (social media, news, etc.) to create false messages that are credible. If they know that a unit is operating in a certain area and that there are reports of enemy activity, they can send false alerts that cause confusion or divert resources. The proliferation of information in open sources has greatly facilitated the construction of convincing hoaxes, as attackers can correlate multiple sources of public information to create false but plausible narratives.

Impact on Military Operations

Losing communications during a military operation is like going blind in the middle of combat. Commanders lose visibility into what's happening on the ground. Units in the area are unable to receive updated orders or report updates in a timely manner. Coordination becomes impossible and each unit has to improvise based on outdated information. This fragmentation of command and control can quickly turn a coordinated operation into multiple independent actions that can interfere with each other or duplicate efforts, markedly diminishing overall effectiveness.

Lewis (2014) describes how manipulating communications can be worse than simply losing them. If commanders receive incorrect but credible information, they can make decisions that actively harm the operation. Units can be sent to the wrong places, resources can be wasted on false targets, and the element of surprise can be completely lost. False information can spread through multiple command levels before being detected, amplifying its destructive effects and creating confusion that can last for hours or days.

Logistical Problems

Modern logistics operations are incredibly complex and rely entirely on reliable communications. Tracking inventories, coordinating supply movements, and managing the supply chain requires constantly updated information. When communications fail, the entire logistics machine can quickly collapse. Automated logistics management systems process thousands of transactions daily, from ammunition requests to equipment

maintenance scheduling. The disruption of these information flows can create cascading effects that extend far beyond the immediately affected units.

Automated fulfillment systems are especially vulnerable because they rely on accurate and up-to-date data. If systems report incorrect supply locations or fake inventories, logistics decisions will be incorrect. Scarce resources can be sent to the wrong places while units that urgently need them are left without support. Automation that makes operations more efficient also creates centralized vulnerabilities where errors or attacks can have multiplied effects throughout the logistics network.

The coordination of medical evacuations represents a particularly critical case. Telemedicine systems that enable remote medical consultations depend on high-quality communications. If these communications are disrupted or compromised during a medical emergency, the consequences can be fatal. Incorrect coordinates for evacuation can send medical helicopters to the wrong places. Medical evacuation protocols in Colombia involve complex coordination between ground units, aviation, field hospitals, and often civilian facilities. The failure of communications at any point in this chain can result in delays that compromise the survival of the injured.

Attacks specifically directed against logistics systems can be used to weaken military capabilities without direct engagement. If the supply of ammunition, fuel or food can be interrupted, troops are forced to reduce operations or abandon positions. It is a form of economic warfare that can be very effective with relatively limited resources. Criminal groups in Colombia have shown an understanding of these principles, frequently targeting motorized movements of supplies and logistical facilities to degrade military capabilities indirectly.

Protection Strategies

The most important lesson is not to rely on a single system for something as critical as military communications. Diversifying means using multiple vendors, different technologies, and various backup methods. If one system fails or is attacked, the others can keep operations running. Real diversification requires a deep understanding of the fundamental architectures of different systems to ensure that they do not share common vulnerabilities that could be exploited simultaneously. Military planners must consider not only technical diversity but also geographical, political, and economic diversity in their communications providers.

This doesn't mean simply buying antennas from different brands. It means using fundamentally different technologies that don't share the same vulnerabilities. Traditional geostationary systems work very differently than constellations like Starlink. Although they may be less modern, they are also less vulnerable to certain types of attacks. Effective technical diversification must include systems that operate in different frequency bands, use different communication protocols, and rely on geographically dispersed terrestrial control infrastructures.

Earth systems are still important as a backup. HF radios may be outdated, but they are independent of space infrastructure that can be attacked. Microwave communications may have limited range, but they are difficult to intercept from afar. Tactical cellular networks may be slow, but they are under national control. Each technology has specific advantages that can be critical in particular circumstances. Effective integration of multiple communication systems requires the development of protocols and procedures that allow for rapid transition between systems when necessary.

Additional Protection

Using trading systems does not mean accepting their trading security levels. Military communications need additional protection that goes beyond what providers offer. This means adding extra layers of encryption, stronger authentication, and continuous monitoring of communications integrity. Commercial systems are designed for typical commercial threats, not for sophisticated adversaries with state resources and specific military or criminal motivations.

Independent encryption is especially important. Rather than relying only on the protection provided by the commercial provider, the Military must add its own encryption before transmitting sensitive information. This means that even if commercial systems are compromised, military information is still protected by systems controlled by the institution. Military encryption systems must use algorithms and keys completely independent of any commercial system, ensuring that the compromise of one system does not affect the security of the other.

Authentication should verify not only who is sending messages, but also that the messages have not been altered in transit. This requires systems that can detect subtle manipulation of communications, not just obvious attacks. Methods should include identity verification of devices in addition to individual users. Authentication protocols for military use must be more robust than commercial standards, incorporating multiple verification factors and continuous validation techniques during communication sessions.

Continuous monitoring should detect anomalies that may indicate attacks in progress. This includes changes in traffic patterns, unusual interference, and strange behavior of systems. Analysts need specialized tools to recognize indicators of attacks against satellite systems specifically. Monitoring systems must incorporate artificial intelligence capable of detecting subtle deviations from normal patterns that could indicate infiltration or manipulation by sophisticated adversaries**.**

Colombia needs to develop internal capacities to understand, evaluate and protect satellite communication systems. This does not necessarily mean building your own satellites immediately, but developing the

knowledge and skills necessary to be less dependent on external suppliers. In-house capacity development should follow a progressive approach that begins with a basic understanding of satellite technologies and gradually evolves into stand-alone design and construction capabilities.

Cyber operations centers need personnel specialized in satellite technologies. This requires specific training that goes beyond traditional cybersecurity. Analysts need to understand how satellite communications work, what types of attacks are possible, and how to detect and respond to specific threats. Training should include technical aspects of satellite systems, but also an understanding of the operational and strategic implications of different types of vulnerabilities.

Research and development programs can create solutions tailored to specific needs. Starting with the Technological Support Command of the National Army, the Colombian Ministry of Defense, in coordination with the Military Forces, promotes the "Innovation Force", a multisectoral national hub for collaboration between the State, universities and the productive sector. Universities can contribute fundamental research, while private industry can develop practical applications. Cooperation with partner nations can accelerate development while maintaining national control over critical technologies. Research programs should focus on specific problems facing Colombia, such as communications in rainforest environments or protection against asymmetric threats from non-state groups.

The development of one's own satellite capabilities should be seen as a long-term investment in technological sovereignty. Although the upfront costs are high, national control over critical communications justifies the investment. A program may start with basic capabilities and gradually expand as economically feasible. Regional cooperation with other Latin American countries can make it more feasible to develop shared satellite capabilities that would be too costly for any individual country.

Practical Recommendations

Moving towards a comprehensive system for risk and incident management that uses artificial intelligence, but from a close and practical perspective: the ideal is to combine intelligent tools that help monitor and protect technological infrastructures and services, quickly detecting any strange behavior to respond without delay. The use of these resources, beyond automation, makes it possible to anticipate problems, document incidents in an orderly manner and make better decisions in the face of crises. Betting on artificial intelligence in this process not only improves the ability to react and protect, but also facilitates people's daily work and provides peace of mind, knowing that they are supported by solutions that adapt and learn from each situation.

Foster innovation and establish cybersecurity centers of excellence to drive the development of new solutions and best practices in digital protection. These centers should be collaborative spaces where experts, academics, and practitioners can work together, share knowledge, and experiment with cutting-edge technologies. Promoting innovation in this area not only strengthens defenses against current threats, but also prepares organizations and the country to face future challenges with creativity and effectiveness. This builds a solid and continuously updated community that provides security, trust and sustainable growth in the digital environment.

Promoting cyber defence through simulations and the use of emerging technologies, based on a practical and close vision, incorporating simulated exercises helps to better prepare people to face real situations, allows us to learn from mistakes in controlled environments and strengthens the reaction to possible threats. Leveraging innovative tools and new technologies such as virtual environments, smart sensors, and advanced analytics helps anticipate risks and tailor responses. In this way, a culture of prevention and continuous improvement is created that facilitates daily work and provides greater confidence, knowing that technological defense is constantly evolving in the face of modern challenges.

Develop and implement an incident management training program designed to strengthen the response capabilities of all those involved. This program should offer clear tools, practical exercises, and collaborative learning spaces, so that each participant knows how to act in unexpected situations and can confidently contribute to problem-solving. Continuous training and awareness-raising, adapting content to real needs and encouraging the exchange of experiences, contributes not only to improving incident handling, but also to creating a safer and more prepared work environment for any digital challenge.

A proposed acquisition of new cloud security portfolios such as the AWS (Amazon Web Service) project, integrates the key principles for the design and operation of a hybrid military-supported spatial architecture in the context of the "AWS KUIPER Project". It lists the four main pillars that must be guaranteed in a satellite and cloud technology solution for military support: security, performance, reliability, and scalability. In essence, this infrastructure prioritizes protection against risks and threats, offering high performance in communications and operations, ensuring that systems operate continuously and reliably, and being prepared to grow and adapt to different needs and volumes of users. These factors are critical in both military environments and critical applications that require secure and robust connectivity, leveraging satellite technologies (such as AWS's Kuiper) and advanced digital platforms**.**

Immediate Actions (First 6 Months)

The Army should immediately begin implementing additional encryption on all sensitive communications. This can be done with portable devices that connect between Starlink terminals and military communication equipment. These devices must use approved algorithms for classified information and must be independent of

any trading system. The implementation should include strict protocols for cryptographic key management and procedures for regular verification of the integrity of encryption systems.
Operational procedures should change to include verification of critical information through independent channels. Important messages should be confirmed using alternative methods such as HF radio or terrestrial communications when possible. This may be slower, but it provides independent verification that the information has not been tampered with. Procedures should specify what types of information require independent verification and establish deadlines for confirmation that do not compromise operational effectiveness.
Staff training should include awareness of specific threats against satellite communications (cybersecurity). Operators must learn to recognize jamming signals, jamming attacks, and anomalous behavior in systems. Reporting procedures should establish clear channels for reporting suspicious incidents quickly. Training should be hands-on and include exercises that simulate different types of attacks so that personnel can practice appropriate responses in controlled environments.
Complete inventories of all satellite terminals in use should be established, including specific locations, configurations, and applications. This information is necessary for risk assessment and incident response planning. Endpoints should be regularly audited for unauthorized modifications or strange behavior. Inventories should also include information on supply chains and maintenance histories to facilitate forensic investigations if compromises are detected.

Medium-term improvements (6 months to 2 years)
Implement cyber operations centers to develop specialized capabilities in monitoring satellite communications. This requires specific equipment for spectrum analysis, personnel trained in satellite technologies, and procedures adapted for threats against space systems. Monitoring capabilities should include interference detection, analysis of anomalies in traffic patterns, and identification of spoofing signals. Centers must establish connections with international organizations that monitor threats against satellite systems to exchange information on emerging threats.
Backup systems need to be significantly improved to provide reliable alternatives when trading systems are not available. This may include upgrading existing radio networks, implementing tactical microwave communications, and developing basic military satellite capabilities. Backup systems should be tested regularly under realistic conditions to ensure that they will work when needed. The transition between primary and backup systems should be practiced frequently to minimize disruptions during emergencies.
Agreements with multiple suppliers must be negotiated to reduce dependence on a single system. These agreements should include guarantees of availability during crises and priority access for military applications. Contracts must specify service levels and penalties for non-compliance. Agreements must also include provisions for access to technical information necessary for independent operation and maintenance of critical systems. Contract negotiation should consider geopolitical implications and include clauses that protect national interests.
Personnel development programs should create experts in satellite technologies and specialized cybersecurity. This may include exchange with international organizations, advanced training, and collaboration with universities. Retention of specialized personnel must be a priority to avoid loss of critical knowledge. Programs should include both technical training and education on the operational and strategic implications of technology decisions. The development of internal expertise must be systematic and sustainable in the long term.

Long-term goals (2 to 5 years)
Consider the development of national or regional satellite capabilities. This does not necessarily mean building and launching satellites immediately, but developing the technical capabilities needed to reduce foreign dependence in the long term. Satellite capacity building requires heavy investment in technical education, industrial development and international cooperation. The long-term benefits of technological independence justify the significant upfront costs.
Regional cooperation may be a more feasible alternative to completely national development. Countries such as Brazil, Mexico and Argentina have experience in satellite technologies. Regional cooperation could create shared capacities that are more effective and cost-effective than isolated national efforts. Regional cooperation must be structured to ensure that Colombia maintains control over critical aspects of national security.
Research and development programs should focus on specific countermeasures against identified threats. This includes anti-interference technologies, attack detection systems, and enhanced authentication and encryption methods. Research must involve research centers, universities, private industry and international cooperation. Research programs must balance fundamental research with the development of practical applications that can be implemented within realistic timeframes.
National regulations must evolve to address emerging threats and new technologies. The legal framework should be flexible enough to adapt to rapid changes in technology and threats, but specific enough to provide clear guidance to users and providers. Regulations should be developed in coordination with relevant stakeholders and should consider economic implications in addition to safety considerations. The regulatory

process should include mechanisms for the periodic updating of standards and requirements based on lessons learned and evolving threats.

Lessons from other countries

International Experiences

The United States learned valuable lessons during conflicts in Iraq and Afghanistan about vulnerabilities in military communications. Military drones in Iraq transmitted video without encryption, allowing insurgents to intercept the transmissions using basic commercial software. This led to significant improvements in safety protocols and operational procedures. U.S. experiences have shown that even systems designed for military use can have serious vulnerabilities when deployed without adequate consideration of threats specific to the operational environment.

NATO has developed specific standards for the use of commercial technologies in military applications. These standards recognize that commercial technologies are unavoidable due to their technical superiority and cost advantages, but they establish minimum safety requirements and risk assessment procedures. NATO standards balanced practical necessity with security requirements, providing a model for other countries facing similar challenges.

Israel has developed a hybrid approach that combines commercial technologies with specialized domestic capabilities. They use commercial systems for non-critical applications but maintain independent national systems for more sensitive communications. This approach allows you to take advantage of business benefits while protecting critical capabilities. The Israeli model demonstrates that it is possible to maintain strategic independence while benefiting from commercial innovation.

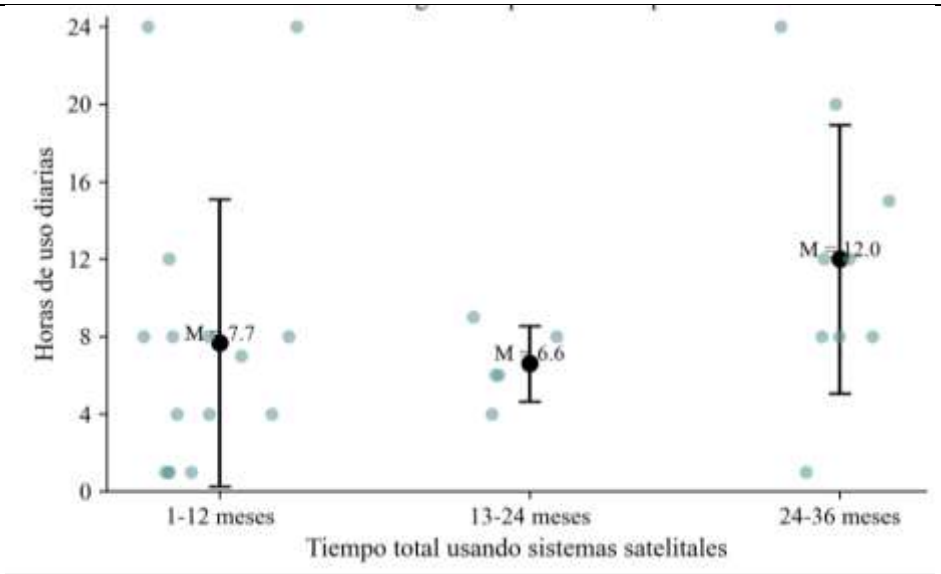
European countries have begun to develop independent satellite capabilities specifically because of security concerns about reliance on U.S. systems. The European Union's IRIS2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite) program seeks to create European alternatives for critical government communications. Casaril and Galletta (2024) analyse how these initiatives balance international cooperation with technological sovereignty. European initiatives show that even close allies may decide that technological independence deserves substantial investment in its development.

Analysis and results

The most important finding according to the study is the increase in the attack surface. A system that is active for 12 hours a day has twice the threat exposure time as one that is active for 6 hours. This means that there is a tendency to be exposed to:

- More opportunities for denial-of-service (DoS) or jamming attacks.
- More time available for an adversary to attempt to exploit vulnerabilities in the satellite network or endpoint.
- Increased likelihood of data being intercepted or malicious code injection attempted.

Figure 1. Frequency of use based on total satellite experience time



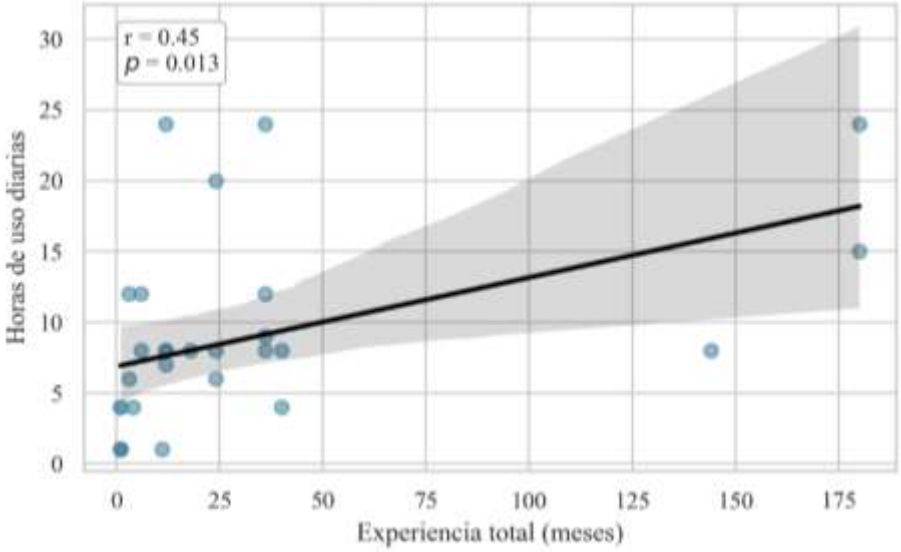
Source: Authors' elaboration based on the data collected by the evaluation instrument

The relationship between the total experience (in months) and the daily frequency of use (in hours) for the units that were part of the study, shows that, although there is a positive trend: the greater the total experience, the more the hours of daily use. This pattern is reflected in the adjusted regression line with an upward slope.

Pearson's correlation coefficient ($r = 0.45$) indicates a moderate and positive correlation between both variables, suggesting that individuals with more months of experience tend to use the system or technology more

frequently on a daily basis. The p-value = 0.013 shows that this association is statistically significant with a trend that represents an increase in confidence and with it a growth in risk.

Figure 2. Relationship between total experience and daily frequency of use



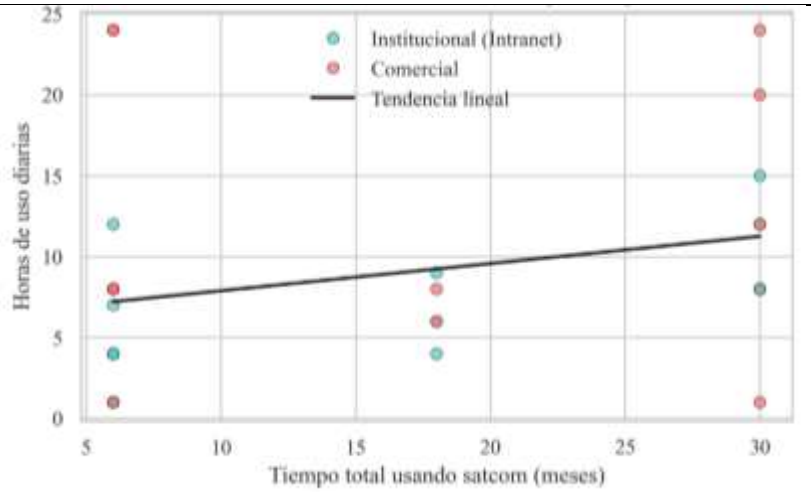
Source: Authors' elaboration based on the data collected by the evaluation instrument

The frequent use of SATCOM systems, both institutional and commercial, at different levels of experience, shows the diversity in the knowledge and compliance with security protocols by users. The results obtained show that even people with significant experience can use commercial networks, which tend to present greater vulnerabilities to interceptions, traffic manipulation and social engineering attacks.

The increase in the frequency of daily use proportionally exposes greater volumes of information, increasing the risk of leaks or compromises of critical data if robust protection and monitoring measures are not adopted. In addition, the alternation between institutional and commercial networks can make it difficult to standardize security policies, generating gaps that can be exploited by malicious actors.

These findings highlight the need to strengthen cybersecurity education, promote SATCOM access and use practices. This involves the development and implementation of risk management strategies, authentication and ongoing training of personnel, along with active monitoring of the networks used in all military operations.

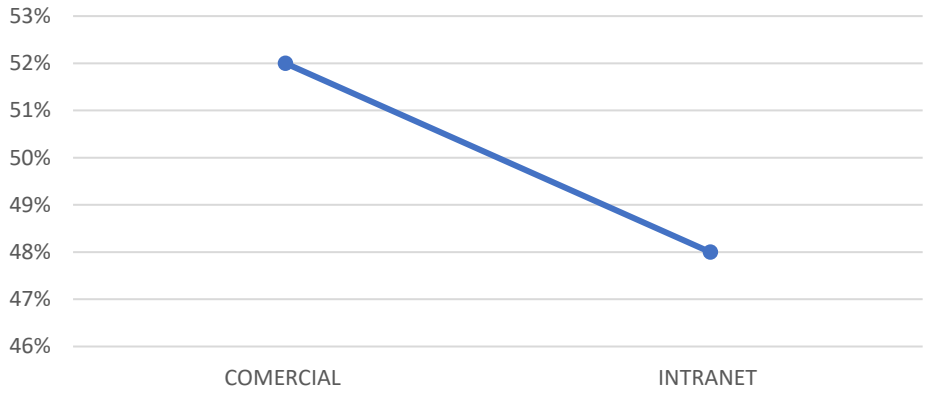
Figure 3. Daily frequency trend vs experience time



Source: Authors' elaboration based on the data collected by the evaluation instrument

It was evidenced that only 48% of the units have an institutional data network (intranet) coverage that allows the execution of the different activities of the force, the remaining 52% corresponds to the personnel who by their means use other commercial means in order to fully comply with the tasks of each official

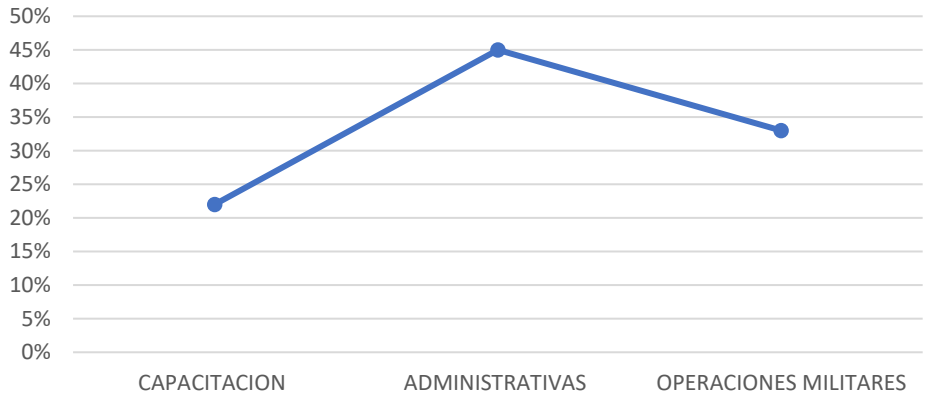
Figure 4. Comparison of data coverage in the units of the National Army



Source: Authors' elaboration based on the data collected by the evaluation instrument

Once it is determined that almost 50% of the units manage data connectivity through other means to institutional ones, it is possible to establish what type of activities they are used for, observing the highest percentage in administrative functions with 45%, 33% in military operations which generates a vulnerability for them and finally 22% are used in training or training processes.

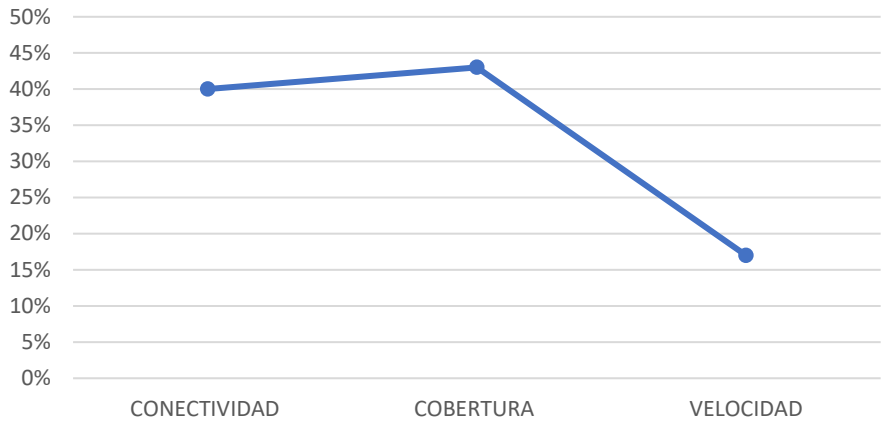
Figure 5. Use of commercial satellite communications in the National Army



Source: Authors' elaboration based on the data collected by the evaluation instrument

The reasons given by the personnel who use commercial communications are related to variables that they do not find in the institutional network, such as connectivity in 40%, coverage in 43% and speed in 17%.

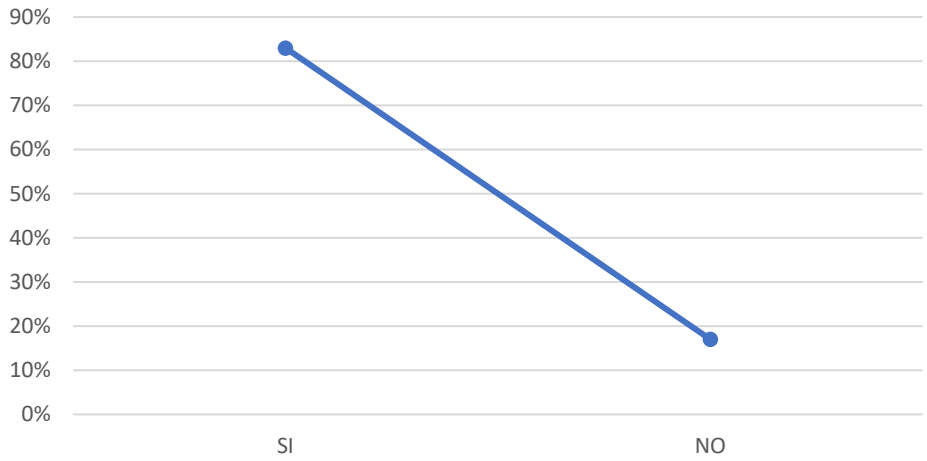
Figure 6. Reasons for the use of commercial satellite antennas



Source: Authors' elaboration based on the data collected by the evaluation instrument

Taking into account the issues analyzed above, it can be seen that a solution applied in an immediate term due to its advantages is the use of alternative means to the institutional ones, and it is marked in the trend of increasing these means through the recommendations made by the personnel who are using them, it was found that more than 80% of the personnel who use them recommend using them as a solution to the connectivity problem.

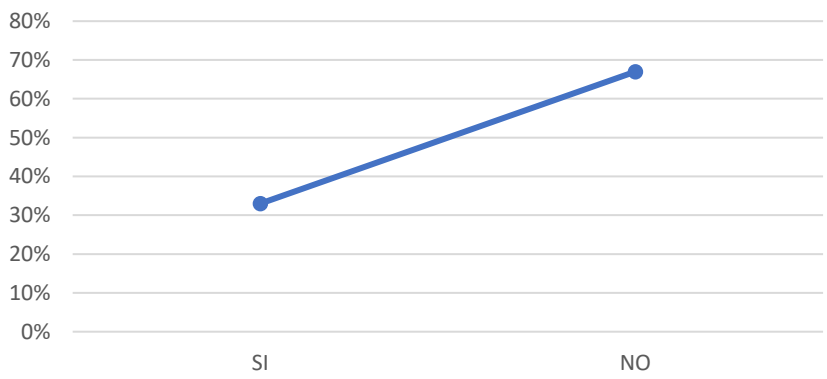
Figure 7. Do you recommend the use of commercial satellite antennas in Army units?



Source: Authors' elaboration based on the data collected by the evaluation instrument

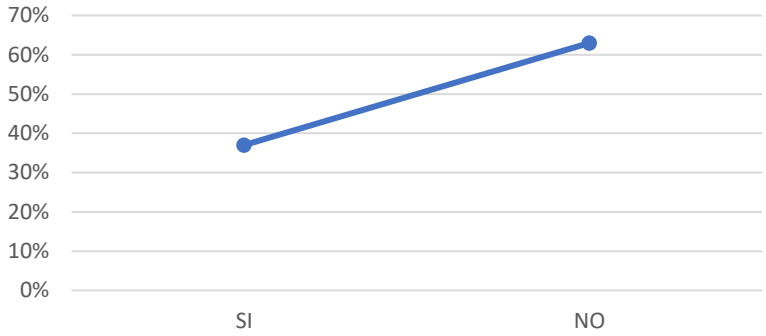
It was found that more than 60% of the personnel who use these alternative means do not apply any security measure in the handling of information, exposing it to a variety of threats of which they can be victims, it could be deduced that this happens due to ignorance of the new threats in the cognitive environment or lack of awareness in the human factor. therefore, it is necessary to develop capacity building measures that impact education, training and awareness among all the institution's staff.

Figure 8. Implement safety measures during the use of commercial satellite antennas



Source: Authors' elaboration based on the data collected by the evaluation instrument

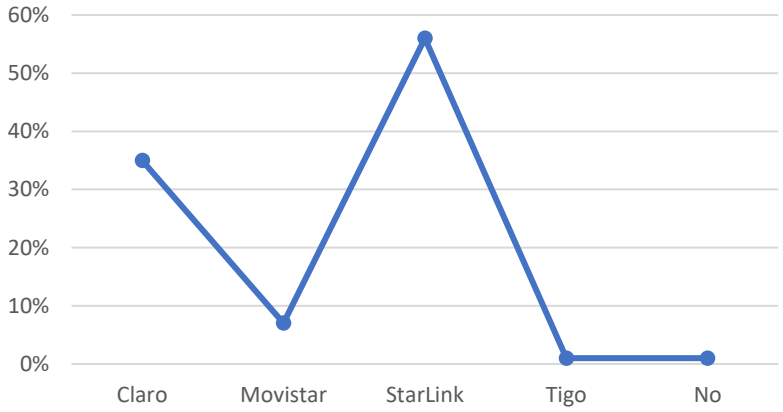
Figure 9. It considers that the use of commercial satellite antennas represents risks



Source: Authors' elaboration based on the data collected by the evaluation instrument

It was found that in Colombia, there are more than 18 satellite internet service providers, noting that only four of them are the most used in the institution for the solution to the problem, highlighting among them that the Starlink company of SpaceX, which presents the highest trend in employment, this is due to several factors such as the acquisition and service values that are cheaper, It is easy to install and operate, its speed and coverage have a greater advantage over others, they are portable devices that are easy to transport and do not require specialized technical personnel for their installation or change of location.

Figure 10. It considers that the use of commercial satellite antennas represents risks



Source: Authors' elaboration based on the data collected by the evaluation instrument

Conclusions

Colombia faces a real dilemma with its military communications. Traditional systems don't work well enough for modern operations, but trading alternatives bring security risks from close attention. There are no perfect solutions, only trade-offs between different types of risks and benefits. The challenge for the Army is to find the optimal balance that maximizes operational capabilities while reducing strategic vulnerabilities. This balance must be continually reassessed as the threat environment and technological capabilities evolve.

International experience, especially documented attacks on satellite systems in Ukraine, demonstrate that these threats are real and current, not theoretical problems for the future. There are groups that have developed specific capabilities to attack commercial systems and have shown a willingness to use them. The evidence from Ukraine should serve as a wake-up call for all military forces that rely on commercial satellite systems, demonstrating that technological superiority does not guarantee protection against determined adversaries. And that the trend of growth in the development of technology within the framework of 5G requires greater preparation and developments that prevent situations that compromise the security of the state.

Armed groups and criminal organizations have reasons to jam military communications, and some have shown increasing technological capabilities. The geography of the country makes satellite communications especially important, but it also creates dependencies that can be exploited. The combination of challenging terrain, adaptive adversaries, and limited resources create an environment that is particularly vulnerable to disruption of communication systems.

The operational benefits of systems like Starlink are undeniable. The Army's communication and coordination capabilities have been significantly improved. The problem is not that these technologies are inherently bad, but that they are vulnerable and must therefore be properly understood, addressed, and mitigated. Recognition of these vulnerabilities should not lead to the abandonment of these technologies, but to a more thoughtful implementation that addresses the associated risks.

The balance between operational benefits and security risks requires continuous evaluation and adjustments based on changing threats and evolving capabilities.

Cybersecurity in satellite systems requires specialized approaches that go beyond traditional computer security. Threats are different, vulnerabilities are different, and countermeasures must be tailored specifically for these unique environments.

Colombia has an opportunity to learn from the experiences of other countries and develop approaches that appropriately balance operational benefits with national security imperatives. The cost of failure to act can be far greater than the cost of implementing appropriate protections.

References

1. Anderson, C., & Johnson, M. (2003). The impressive psychology paper. Lucerne Publishing.
2. Ansong, S., Rankothge, W., & Ghorbani, A. A. (2024). Role of cybersecurity for a secure global communication eco-system: A comprehensive cyber risk assessment for satellite communications. Computers & Security, 128, 103-118.
3. Casaril, F., & Galletta, L. (2024). Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2. Computers & Security, 139, 103-115.
4. Castillo, J. (2018). Technological sovereignty and national security in Latin America. University Press.
5. CISA - Cybersecurity and Infrastructure Security Agency. (2022, March 17). Strengthening cybersecurity of SATCOM network providers and customers. Cybersecurity Advisory AA22-076A.
6. CISA - Cybersecurity and Infrastructure Security Agency. (2022, May 10). U.S. government attributes cyberattacks on SATCOM networks to Russian state-sponsored malicious cyber actors.
7. CONPES 3854. (2016). National Cybersecurity and Cyber Defense Policy. National Council for Economic and Social Policy, Republic of Colombia.
8. Cyber Defense Magazine. (2024, March 23). Cybersecurity threats in global satellite internet.
9. Diálogo Américas. (2022, April 7). Colombia rises to the cyber challenge.
10. Permanent Directive 300-28. (2018). Cybersecurity and Cyber Defense Guidelines for the Military Forces. Ministry of National Defense, Republic of Colombia.
11. Espinosagiralt, J. (2023). Satellite antennas and their applications in critical communications. Journal of Telecommunications Engineering, 45(3), 78-95.
12. Falco, G., & Boschetti, A. (2021). Commercial satellite vulnerabilities: A comprehensive analysis. International Journal of Critical Infrastructure Protection, 32, 100-115.
13. World Economic Forum. (2021). The Global Risks Report 2021. World Economic Forum Press.
14. Graham, J., Smith, L., & Patel, R. (2020). Satellite communications and cybersecurity: Emerging threats. Journal of Space Technology, 45(2), 56-72.
15. Guerrero, R. (2011). Fundamentals of military satellite communications. Editorial Técnica Militar.
16. Guevara Julca, J. Z. (2002). Communications systems aimed at the decentralization of the country's public entities. Universidad Nacional Mayor de San Marcos.
17. Hierro Alcántara, J. L. (2023). Military applications of navigation satellites in the twenty-first century. Journal of Defense and Technology, 48(4), 112-128.
18. Housen-Couriel, D. (2016). Commercial off-the-shelf vulnerabilities in space systems. Space Policy, 38, 128-135.
19. Huidobro, J. M. (2013). Antenna Technology: Principales and Applications. Editorial Ra-Ma.
20. In Compliance Magazine. (2024, March 5). Electronic warfare and cyber defense of satellites.
21. IOActive. (2022, March 25). Missed calls for SATCOM cybersecurity: SATCOM terminal cyberattacks open the war in Ukraine.
22. ISO 27001:2022. (2022). Information security management systems - Requirements. International Organization for Standardization.
23. Kareem, K. M. (2024). Cyber threat landscape analysis for Starlink: Assessing risks and mitigation strategies in the global satellite internet infrastructure. arXiv preprint arXiv:2406.07562.
24. Latina Ecuador Sacristán Romero, M. (2005). Evolution of satellite communications. Central University Press.
25. Lewis, J. A. (2014). Conflict and negotiation in cyberspace. Center for Strategic and International Studies.
26. Liu, Y., Zhang, X., & Wang, L. (2024). Characterizing and analyzing LEO satellite cyber landscape: A Starlink case study. ResearchGate.
27. Llanso, E., & Pearson, M. (2016). Cybersecurity challenges in satellite communications. Communications of the ACM, 59(11), 44-51.
28. Massimi, F., Tedeschi, P., & Di Pietro, R. (2023). Advanced persistent threats in satellite networks. IEEE Network, 37(2), 78-85.
29. MDPI Sensors. (2024). A survey on satellite communication system security. Sensors, 24(9), 2897.
30. MinTIC Colombia. (2022). Regulation of satellite technologies in Colombia. Ministry of Information and Communications Technologies.
31. Morales, P., & Hernández, D. (2021). Satellite Technologies and National Defense: A Legal Analysis. Journal of Space Law, 18(1), 34-49.
32. Musk, E. (2021). Starlink constellation deployment and military applications. Space Technology Review, 28(5), 234-247.

33. NATO STANAG 4774. (2023). Cybersecurity requirements for military communication systems. North Atlantic Treaty Organization.
34. NIST Cybersecurity Framework 2.0. (2024). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, U.S. Department of Commerce.
35. Nogueira, R., Silva, M., & Torres, F. (2019). Cybersecurity challenges in military satellite systems. Defense Systems Journal, 67(4), 89-104.
36. NSA Cybersecurity Advisory. (2022). Protecting VSAT communications. National Security Agency, United States.
37. Pinto, R., Medina, C., & Vargas, L. (2023). Emerging technologies in satellite communications. Engineering and Competitiveness, 25(2), 234-251.
38. Resolution 7870. (2022). Guidelines for cybersecurity in satellite services.
39. Ministry of Information and Communications Technologies, Republic of Colombia.
40. Sacristán, P. (2005). History of space communications. Editorial Espacio.
41. Santamarta, R. (2018). Last call for SATCOM security. Black Hat Technical Conference Proceedings. Las Vegas, NV.
42. Smith, M. (2001). Writing a successful paper. The Trey Research Monthly, 53, 149-150.
43. SpaceX. (2022). Starlink technology overview. Retrieved from www.spacex.com
44. Tedeschi, P., Sciancalepore, S., & Di Pietro, R. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. Computer Networks, 216, 109-125.
45. TheSIGN. (2024). Uncovering potential vulnerabilities in Starlink: Russian hackers' persistent attempts.
46. U.S. Trade.gov. (2024). Colombia - Defense & Security.
47. Wang, K., Li, M., & Chen, S. (2022). Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. Journal of Cybersecurity, 8(1), tyac008.
48. White, J., & Mauldin, K. (2020). Military applications of commercial satellite systems. Defense Technology Quarterly, 33(4), 67-82.
49. Yang, Z., Liu, H., & Zhang, W. (2024). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica, 198, 447-458.
50. Zetter, K. (2023). Geopolitical implications of commercial satellite dependencies. International Security Review, 45(3), 123-145.
51. Zhao, H. (2019). The next generation of satellite services: Challenges and opportunities. Telecommunications Policy, 43(8), 654-668.
52. Spanish Ministry of Defence. 2024. Artificial intelligence as a factor in the transformation of military operations at the operational level.