

Chapter 12

Cyber Capabilities in Contemporary Conflicts*

DOI: <https://doi.org/10.25062/9786287818408.12>

Juan David Zuleta
Andrés Acosta Muñoz

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Current events show that cyber conflict is already widespread worldwide. This chapter discusses aggressive cyberwarfare strategies and tactics at all stages of national security and defense planning. It concludes that leadership in national security and defense must significantly enhance its understanding of technology, law, ethics, and cyberattacks to address the broader context of multi-domain warfare.

Keywords: defense; strategy; cyberwarfare; intelligence; security.

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

Juan David Zuleta

Lieutenant Colonel in the Colombian National Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Leadership and Management of Military Units, and Specialization in Military Resources Administration for National Defense, National Army Arms and Services College, Colombia. Specialization in Equestrian Administration, National Army Cavalry College. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: juan.zuleta@buzonejercito.mil.co

Andrés Acosta Muñoz

Colonel in the Colombian National Army. Master's in Strategy and Geopolitics, and Specialization in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Master's in Security and Defense, Nebrija University, Spain. Specialization in Senior Management, Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0002-2813-5471> - Email: andres.acosta@esdeg.edu.co

APA Citation: Zuleta, J. D., & Acosta Muñoz, A. (2025). Cyber Capabilities in Contemporary Conflicts. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 259-278). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818408.12>

COMMANDOS: CHALLENGES FACING SPECIAL FORCES AND INTELLIGENCE IN CONTEMPORARY WARFARE

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

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

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

Security and Defense Collection

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introduction

This chapter addresses contemporary conflicts where the capabilities and technological advances of the cyberspace domain are used both offensively and defensively to degrade adversaries' capabilities and create significant destabilization in military actions before, during, and after a conflict. It also analyzes the significant role of Special Forces (SF) and Intelligence units in developing these types of cyber actions and operations, as they are becoming the primary task for States in confronting their threats.

In this regard, it is worth noting that the world is changing by leaps and bounds, and that the development of information and communications technologies (ICTs) is advancing at such an accelerated pace that, in some ways, they are exceeding the expectations of the strategic, operational, and tactical capabilities of Armed Forces around the world. The implementation of new technologies challenges the parameters and factors of conventional warfare, while transforming the strategies that States adopt to confront their adversaries in national, neighboring, regional, continental, hemispheric, and global environments.

Under this criterion, it is possible to identify the main powers in this area, such as the United States, China, Russia, Israel, and Iran, as these countries are belligerents in cyberspace and allocate human, technical, and economic resources to develop their "cyber forces." In general, they act with a dual intention: first, to guarantee the security and defense of their specific cyberspaces, and second, to exert power and influence among their citizens, allies, and potential adversaries (Colom et al., 2013). Ultimately, all of this is intended to prevent and respond to cyberattacks that could jeopardize the continuity and availability of the country's critical services.

However, this is just the tip of the iceberg. Currently, various strategic guidelines have ramifications at both the offensive and defensive levels, which must be addressed to mitigate the different risks and threats in cyberspace. This is especially true in contemporary war scenarios, which often require the intervention of SF units.

Furthermore, this chapter aims to establish the relationship between the new requirements of contemporary wars in terms of operational art and design implementation, as well as identify the center of gravity of cyber threats using strategic intelligence. It is worth clarifying that these initial formulation and logic processes “form the central nervous system of the Colombian National Army's doctrine and address the needs of commanders and staff to resolve situations in volatile, uncertain, complex, and ambiguous operational environments” (Ejército Nacional de Colombia, 2019, p. 19).

The weaknesses of the doctrinal approach to using intelligence and cyber capabilities in modern conflicts are examined through several case studies. This includes analyzing the connection between cyber-based intelligence operations, their success rates in meeting objectives, and the main challenges of using cyber tools in today's scenarios.

Finally, the scope of military intelligence strategies and operations in modern conflicts and wars is analyzed from different perspectives within the cyberspace domain, with the goal of understanding their purposes, features, and outcomes.

Methodology

The research was carried out using tools that allow for a comparative analysis of different theories and related events, which includes a thorough review of the literature on the topic and the cyber capabilities used in modern conflicts. Additionally, documentary research was performed to gather information on strategic guidelines at both the offensive and defensive levels.

In this manner, records were gathered from various bibliographic sources, including journals, scientific articles, books, archival materials, and other academic works. This enabled the development of both a general and a specific understanding of contemporary warfare, as well as the challenges and opportunities facing the SF and Intelligence. While primarily a qualitative study that offers conceptualization, evaluation, and observation, it also incorporates quantitative data to explain the

phenomena observed by collecting digital data, which are analyzed using methods based on mathematical, statistical, or computer techniques.

Afterwards, a comparative and descriptive analysis of each identified scenario is performed, involving the collection of samples to observe how the different variables behave as part of the research problem. Finally, a discourse analysis is conducted on several series of documents, particularly public policies and military doctrines related to cyber capabilities, to elucidate the theoretical framework underlying the concept.

The New Requirements of Contemporary Warfare

In contemporary warfare, various scenarios and events contribute to a nuanced understanding of how armed conflicts are changing. In other words, there are reasons to believe that warfare operates in both physical and virtual domains. This is supported by Patrikarakos (2021), who states that there are two wars: one fought in physical spaces (land, sea, air, and space) and the other occurring in virtual environments (cyberattacks, sabotage, disinformation, and other actions). These factors suggest that a new dynamic is emerging in current conflicts, necessitating innovative approaches to destabilize the enemy during times of war and unrest.

In this scenario, governments worldwide are increasingly focused on shaping social and economic policies through ICTs. As a result, they are beginning to understand the opportunities and challenges of cyberspace while expanding strategies and establishing cyber defense and cybersecurity organizations dedicated to addressing cyber threats. This indicates that nations are only beginning to explore the "Fourth Industrial Revolution" (Connected Industry 4.0), which features a sophisticated integration of production techniques with intelligent systems that connect with organizations and people, while also presenting vulnerabilities that can be exploited to disrupt and harm a nation's critical infrastructure.

In this regard, it is important to note that the needs and specialties of security and defense forces have driven several institutional changes, which have greatly enhanced the protection of critical infrastructure. In other words, cyber capabilities have become an increasingly prominent trend, merging into the unique specialties of each military force. This has led to innovations in their organizations and sparked a positive revolution in managing risks and threats to national security. According to

Kenneth Geers (2009), "Practically everything that happens in the real world is mirrored in cyberspace. For national security planners, this includes propaganda, espionage, reconnaissance, targeting, and—to an unknown extent—warfare itself" (p. 145).

It is worth noting that, according to Geers (2009), five common tactics are used in cyberwarfare: espionage, propaganda, denial-of-service (DoS) attacks, data modification, and infrastructure manipulation. In this context, it can be argued that cyberspace is, ultimately, the "new arena of confrontation" between States, nations, democracies, dictatorships, criminal organizations, and terrorists, among others.

As a result, there is competition between powers and developing countries to establish new enabling structures and organizations that, on the one hand, protect their own cyber capabilities and, on the other, conduct cyber operations with various objectives, primarily aimed at influencing the capabilities of potential threats. Therefore, at this point, cyberwarfare can be said to be emerging.

Based on this overview, the Army Design Methodology (ADM) is outlined below to define how an operational environment (OE) is structured from a systemic perspective during the operational process, especially in relation to cyber capabilities in modern conflicts. To achieve this, a series of network analysis diagrams will be used to visualize and describe the environment. This provides a clear and educational way to display the connections within different networks, helping to understand the OE concerning risks and threats in the cyberspace domain.

It is important to clarify that the OE is defined by the Colombian National Army (Ejército Nacional de Colombia, 2017b) as "the set of conditions, circumstances, and influences that impact the use of capabilities and influence the commander's decisions" (p. 1-2). From this perspective, the following sections outline the operational problem, presenting an overview of key aspects in contemporary conflicts. This will be connected to the strategic guidelines at both the offensive and defensive levels in the cyberspace domain, as well as to the structure of the operational approach.

Strategic Planning Guide 2018–2022

In the *Strategic Plan for the Defense and Security Sector - Strategic Planning Guide 2018–2022* (PES), the Ministry of National Defense (MDN) provided instructions to the Armed Forces to guide the constitutional mission of security forces and to achieve national strategic objectives (MDN, 2018, p. 3). It also sets a roadmap for integrated planning in the defense and security sector over the four-year period, based on an analysis of threats and challenges to national defense and security. Specifically, these were the premises that the MDN (2018) outlined for the Armed Forces:

1. Risks and threats to the State in cyberspace pose a new concern since they can originate from various actors worldwide and aim to achieve objectives linked to different phenomena, such as crime, espionage, sabotage, and terrorism (p. 8).
2. In response to the challenges and threats from the external environment, the PES advocates for defending national interests through a strong strategy that also enhances capabilities in digital security, cyber defense, intelligence, and counterintelligence (p. 9).

General Situation

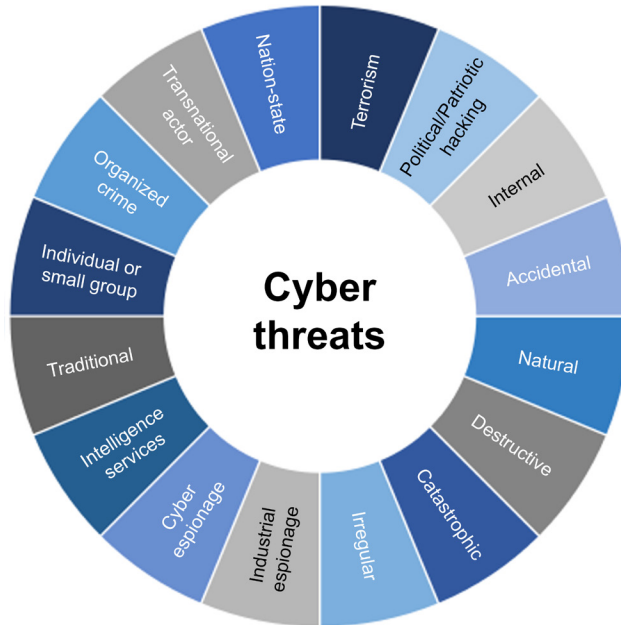
In 1962, the U.S. Department of Defense, through the Advanced Research Projects Agency (ARPA), requested the development of a technology that would enable interconnected communication between different government agencies. Later, in 1969, the message test was successfully completed, creating the first communications network between Stanford University and the University of California, Los Angeles (UCLA).

Then, in 1988, the world saw the emergence of the first malicious code, known as the Morris Worm. As a pioneer in its field, it caused widespread damage to computer networks and systems at the time. It could rapidly self-replicate, directly impacting the internet. Its effects exposed the vulnerabilities within computer systems, highlighting the need for developers to establish security protocols to safeguard against future devastating attacks. Consequently, the events of that year opened new opportunities for creating an enormous variety of malware, which dramatically changed how computer systems could interact. As a result, cyberattacks and cyberespionage came into existence.

In 1990, the European Organization for Nuclear Research (CERN), together with several physicists based in Geneva and Switzerland, developed HTML (Hypertext Markup Language). That same year, the first web client, also known as the World Wide Web (WWW), was created.

However, in the current decade (2020–2030), various threat actors operate in the cyberspace domain (Figure 1), with different types and multiple purposes, including economic, political, intellectual, intelligence, and industrial espionage motives. However, the greatest risk comes from States and intelligence organizations, which, through the manipulation of various structures or groups, carry out their activities in pursuit of specific objectives.

Figure 1. Cyber Threats



Source: Own elaboration.

The most common threats in cyberspace can be categorized as follows: nation-state, transnational actor, organized crime, individual or small group, traditional threat, intelligence services, cyberespionage, industrial espionage, irregular threat, catastrophic threat, destructive threat, natural threat, accidental threat, internal threat, political/patriotic hacking, and terrorism.

Structure of the Operational Environment

The new battle typology is set in the post-Cold War era, when computers and online communications were used to address threats through the development and deployment of information aimed at psychological and logistical disruption. It is also marked by the use of information technologies across various organizations at strategic, operational, and tactical levels, involving a wide range of components and resources from armed forces around the world.

In the United States, considered the birthplace of the internet, many thinkers, military personnel, politicians, and others are dedicating time and resources to analyzing the phenomenology of cyber risks and threats, as well as exploring the alternatives needed to sustain leadership in the global cyberspace arena.

For its part, the North Atlantic Treaty Organization (NATO) defines a country's critical infrastructure as consisting of public and private institutions in the agriculture, food, water, public health, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal administration sectors (Geers, 2009).

Furthermore, cyberspace is regarded as the nervous system and control system of a country. It consists of hundreds of thousands of interconnected computers, servers, routers, hubs, and fiber-optic cables that link critical infrastructure. Therefore, the healthy operation of cyberspace is vital to the nation's economy and security.

Problem Identification and Options

The strategic reasons for the rise of cyberwarfare are linked to several key factors. First, the internet is susceptible to cyberattacks. Clearly, no security system offers 100% protection. As a result, there is currently no completely secure system capable of preventing all types of cyberattacks. Besides, the internet's flawed design enables hackers to covertly read, delete, or modify information stored or transmitted between computers. Consequently, attacks armed with constantly evolving malicious code likely have more access points to your network and its secrets than system administrators can effectively defend against.

Second, there is a high return on investment. The goals of cyberwarfare practitioners are clear: stealing research and development data, spying on sensitive communications, and spreading propaganda. What makes hacking stand out is that it can be accomplished at a fraction of the cost and risk associated with other information-gathering or manipulation methods.

Third, cyber defense is inadequate. Cyber defense remains an immature yet constantly evolving field. Traditional law enforcement skills are often insufficient, and it can be difficult to retain personnel with in-demand skills. The global nature of the internet makes cyber investigations even more complex. Lastly, there are no State-sponsored offensive operations in cyberspace, nor is there cooperation between law enforcement agencies.

Fourth, there is plausible deniability. The complex design of the internet gives cyber attackers a high level of anonymity. Savvy hackers can route attacks through countries with which the victim's government has poor diplomatic relations and refuses to cooperate with law enforcement. Even successful investigations often only uncover another hacked computer. Today's governments risk losing a cyber conflict without ever knowing who their real adversary is.

The fifth factor is the involvement of non-state actors. Nation-states strive to maintain as much control as possible over international conflicts; however, globalization and the internet have significantly enhanced everyone's ability to monitor current events and influence them. Transnational subcultures now form spontaneously online and affect numerous political agendas, without answering to any chain of command. In this context, a challenge for national security leaders is that this activity could disrupt delicate diplomacy.

These phenomena seem to confirm that all political and military conflicts have a cyber aspect, the scope and effect of which are hard to predict, as attackers have a wide range of effective cyberwarfare strategies and tactics available to them.

Therefore, the internet is vulnerable to cyberattacks. Its amplifying power means that future victories in cyberspace could result in victories on the ground. Both state and non-state actors see a high return on investment in cyber tactics, from planting carefully crafted propaganda to manipulating an adversary's critical infrastructure.

Weaknesses in the Doctrinal Conception

The doctrinal conception of military forces worldwide regarding these issues is in its early stages, so there is still a long way to go to understand and establish regulations that enable the implementation of strategies, methods, procedures, and tactics to address risks and threats in cyberspace. Consequently, it is necessary to identify and address some key factors in developing a doctrinal approach that enables us to address these challenges. Below, we examine the application of intelligence and cyber capabilities in contemporary conflicts and provide case studies that highlight key aspects to consider in these types of initiatives.

Use of Intelligence

Undoubtedly, the capabilities that cyberwarfare tools give to security and defense forces in intelligence are exceptional. Therefore, it is safe to say that these capabilities continue to offer a significant opportunity to gain a strategic advantage over opponents. Infiltration, penetration, and information gathering are their main strengths, as they ensure the stealthy access points needed for effective intelligence operations.

Cyber Capabilities in Contemporary Conflicts

According to Patrikarakos (2021), "terms like 'hybrid warfare,' 'disinformation,' and 'troll farm'—have all become buzz words of our 'post-truth' age" (p. 3). Furthermore, the possibility of controlling the internet, traffic, mobile phones, and security systems is not a science fiction story, but rather part of the general concept of cyberwarfare. For this reason, "strategists must be aware that part of every political and military conflict will take place on the internet" (Geers, 2009, p. 58).

Cyberattacks have evolved and increased in capacity and complexity; year after year, new viruses, Trojans, or malware emerge. Their ability to disrupt processes, open backdoors, modify code, facilitate information theft, gather data on organizational relationships, and impair systems indicates that the full scope of cyberspace characteristics is still being uncovered.

Therefore, it must be recognized that no software application is completely free of vulnerabilities. In other words, industrial, commercial, military, government, and police systems, among others, will require increased attention, primarily because of the importance of each category and the immediate impact they can have on critical infrastructure. Because of these qualities, they can become targets for various organizations, including hacktivist groups, cybercriminals, cyberterrorists, and nations. It is important to understand that the consequences of these attacks could be devastating to the critical infrastructure of any country.

Case Studies

Below are several case studies related to cyber capabilities in contemporary conflicts, which enable us to identify, evaluate, and analyze the risks and threats that national security and defense institutions face in the general environment of cyberspace.

Chechnya (1994)

In the internet age, unfiltered news from a war zone can arrive instantly. Internet users worldwide play a crucial role in international conflicts by sharing information, whether in text or image form, on websites.

According to Thomas Timothy (2003), since the early days of the World Wide Web, pro-Chechen and pro-Russian forces have conducted a virtual war on the internet, which is happening simultaneously on real battlefields. The Chechen separatist movement, in particular, is seen as a pioneer in using the web to deliver

powerful public relations messages. Skillful placement of propaganda and other types of information, like a bank account number for a war fundraising campaign in Sacramento, California, helped unify the Chechen diaspora.

Furthermore, the most influential information was not pro-Chechen but anti-Russian. Digital images of bloody corpses helped sway public opinion against supposed Russian military excesses. In 1999, while Kremlin officials denied an incident where a Chechen bus was attacked and many passengers were killed, footage of the event appeared online. As technology improved, internet users watched streaming videos showing Chechen military actions favorably, such as ambushes of Russian military convoys (Goble, 1999).

It is worth noting that, according to Goble (1999), the Russian government acknowledged the need to enhance its tactics in cyberspace. In 1999, Vladimir Putin, then Russia's Prime Minister, declared, "We surrendered this terrain some time ago... but now we are entering the game again" (Goble, 1999). Moscow sought Western help in shutting down the prominent pro-Chechen website *kavkaz.org* and announced "the introduction of centralized military censorship regarding the war in the North Caucasus."

Thus, according to Bullough (2002), during the Second Chechen War (1999–2000), Russian officials were accused of escalating the cyber conflict by hacking Chechen websites. The timing and sophistication of some of the attacks suggested involvement by a nation-state, for example, *kavkaz.org*, which was hosted in the United States. It was reportedly taken offline at the same time as the assault by Russian special forces, who were conducting a rescue operation inside a Moscow theater besieged by Chechen terrorists.

Kosovo (1999)

In the interconnected conflicts of the internet age, anyone with a computer and an internet connection can become a potential combatant. NATO's first major military engagement took place after the rapid growth of the web in the 1990s. Just as Vietnam was the world's first televised war, Kosovo was its first large-scale internet war.

According to Geers (2020), as NATO planes started bombing Serbia, many pro-Serb (or anti-Western) hacker groups, like the Black Hand, began attacking NATO's internet infrastructure. It is unclear whether any of the hackers directly worked for the Yugoslav military; in any case, their goal was to disrupt NATO military operations.

The Black Hand, which took its name from the Pan-Slavic secret society that helped start World War I, claimed they could identify NATO's "most important" computers and, through hacking, would attempt to "delete the data" they contained. The group reported success in at least some vulnerabilities, particularly in U.S. Navy computers, and said it was subsequently taken offline.

NATO, the U.S., and UK computers were targeted during the war through DoS attacks and virus-infected emails, with 25 different virus strains detected (Geers, 2020). In the U.S., the White House website was defaced, prompting an investigation by the Secret Service. While the U.S. claimed there was "no impact" on the overall war effort, the UK admitted to losing some of its database information.

At NATO headquarters in Belgium, the attacks became a propaganda win for hackers. NATO's public affairs website, which was used to present the organization's side of the conflict through briefings and news updates during the Kosovo war, was nearly inoperable for several days. NATO spokesman Jamie Shea blamed the "line saturation" on "hackers in Belgrade." A simultaneous email flood successfully overwhelmed NATO's email server. As the organization rushed to update nearly all of its computer servers, the network attacks, which initially started in Belgrade, spread worldwide.

Middle East (2000)

During the Cold War, the Middle East often acted as a testing ground for military weapons and tactics. In the internet age, the same has been done with cyberwarfare.

In October 2000, after the kidnapping of three Israeli soldiers, blue and white flags and an audio file playing the Israeli national anthem were placed on a hacked Hezbollah website. Subsequent pro-Israel attacks targeted the official websites of military and political groups seen as hostile to Israel, including the Palestinian National Authority, Hamas, and Iran (Preatoni, 2014).

Retaliation by pro-Palestinian hackers was swift and more varied in scope. Israeli politics, the military, telecommunications, media, and universities all experienced attacks. They also targeted sites of economic importance, including the Bank of Israel, e-commerce platforms, and the Tel Aviv Stock Exchange. At that time, Israel was more connected to the internet than all of its neighbors combined, resulting in numerous targets. The ".il" domain offered a clear list that pro-Palestinian hackers worked through methodically.

As noted, wars often showcase new tools and tactics. Specifically, during this conflict, the DoS program "Defender" was used effectively by both sides,

demonstrating that software can be destabilized more quickly than a tank or a rifle. The defense innovation involved constantly checking the date and time of its simulated web requests, which helped defeat the web caching security mechanisms of the time (Geers, 2004).

Thus, the Middle East cyberwar demonstrated that the internet age and political conflicts can quickly escalate into international conflicts. For example, according to BBC News (2000), the Pakistani "Hackers Club" hacked into the U.S.-based pro-Israel lobby, AIPAC (the American Israel Public Affairs Committee), and published confidential emails, credit card numbers, and contact information of some of its members. Similarly, Page (2000) claimed that "the telecommunications firm AT&T was targeted for providing technical support to the Israeli government during the crisis."

Furthermore, Rebecca Anna Stoil and James Goldstein (2006) asserted that the Middle East cyberwar has generally continued in cyberspace and remains ongoing today. In 2006, as tensions between Israel and Gaza increased, pro-Palestinian hackers shut down about 700 Israeli internet domains, including those of Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel, and McDonald's Israel.

United States and China (2001)

On April 26, 2001, the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC) released Advisory 01-009:

Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems [...] Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC. (Information Warfare Site [IWS], 2001, p. 86)

Tensions increased sharply between the two nations after the United States bombed the Chinese embassy in Belgrade in 1999, and following the mid-air collision of a U.S. Navy plane and a Chinese fighter jet over the South China Sea in 2001, along with the prolonged detention of the U.S. crew in the People's Republic of China.

According to Jeremy Wagstaff (2001), a reporter for *The Wall Street Journal*, hackers on both sides of the Pacific, such as the China Eagle Alliance and PoizonB0x, started large-scale website defacements and created hacker portals with titles like "USA Kill" and "China Killer." After the cyber skirmishes ended, both sides repeatedly accused each other of defamation and DoS.

In this context, the FBI investigated a 17-day hack of a California power grid test network that started on April 25 (Weisman, 2001). The case was widely dismissed as media hype at the time, but in 2007, the CIA informed industry leaders that not only is a tangible threat from hackers to such critical infrastructure possible, but that it had already occurred (Nakashima & Mufson, 2008).

Estonia (2007)

On April 26, 2007, the Estonian government moved a Soviet World War II memorial from the center of Tallinn, its capital. This action sparked outrage among the public in Russia and among Estonia's Russian minority population.

Starting on April 27, the Estonian government, law enforcement, banking, media, and internet infrastructure faced a series of cyberattacks that lasted three weeks, whose effects continue to attract considerable interest from governments around the world.

Since Estonians perform over 98 % of their banking online, the impact of multiple distributed DoS attacks, which shut down communication with the country's two largest banks for as long as two hours and caused international services to be partially unavailable for days, is understandable.

Less discussed, but likely of greater importance to both national security planners and computer network defense personnel, were the attacks on the internet infrastructure (router) of the Estonian government's ISPs, which reportedly disrupted government communications for at least a "short" period.

On the propaganda front, a hacker defaced the website of the Estonian Prime Minister's political party on April 27, changing the page's text to a purportedly fabricated apology from the government for relocating the statue, along with a promise to return it to its original location.

There was significant diplomatic interest in this cyberattack due in part to the potential reinterpretation of NATO's Article 5, according to which "an armed attack against one [Alliance member] [...] shall be considered an attack against them all" (NATO, 1949, Article 5). It should be noted that Article 5 has only been invoked once, following the terrorist attacks of September 11, 2001. Potentially, it could one day be interpreted to cover cyberattacks as well.

Iran (2010)

One of the most notable cases in the era of cyberwarfare is Iran. Clearly, the development of the Stuxnet worm became a tool capable of seriously impacting

the country's critical infrastructure. Specifically, this attack aimed to disrupt the nuclear activities at the Bushehr reactor. It is worth noting that the goal was successfully accomplished, causing a significant delay in Iran's nuclear program.

The unique characteristics of this case show that its entire execution meets the ideal conditions for cyberwarfare. Therefore, it can be concluded that the creation of this cyberweapon ultimately served as an effective tool that impacted Iran's national interests. Additionally, establishing an infiltration and deception operation to activate it and compromise a country's computer networks—leaving them vulnerable to various types of attacks (Porteus, 2010)—can only be described as clever and innovative.

Ukraine (2014)

Ukraine served as a testing ground for new types of information operations (Patrikarakos, 2021). On November 21, 2013, Mustafa Nayyem, a Ukrainian journalist of Afghan descent, posted on Facebook, urging people to gather at Maidan Nezalezhnosti (Independence Square) in Kyiv. He aimed to protest President Viktor Yanukovich's decision to reverse his commitment to sign an association agreement with the European Union, which would have strengthened their political and economic ties.

On the anniversary of this cyberwar, as companies prepared for another round of hacking, the Chinese government reportedly succeeded in a last-minute withdrawal, implying that Chinese hackers may have a higher level of coordination than their American counterparts (Hess, 2002).

Operational and Strategic Scope of Military Intelligence

The internet is transforming many aspects of life, including how warfare is conducted. Sometimes, cyber tools and tactics favor nations with strong information technology infrastructure. However, the internet is a powerful resource that smaller or weaker groups can use to attack a more powerful traditional enemy. Like terrorism and weapons of mass destruction, the ever-changing, asymmetric nature of cyberattacks prompts questions about all elements of cyber defense—such as detection, analysis, investigation, prosecution, retaliation, and more—for national security and defense planning.

As seen in the case studies, it is clear that the operational and strategic scope of military intelligence can greatly benefit from the use of cyber tools to achieve its goals. There is no question that their potential must be examined from a national security and defense perspective, in accordance with both national and international laws.

Therefore, analyzing, designing, developing, testing, and using cyber weapons in the near future are actions that will shape the next step in the evolution of cyberwarfare. It should be noted that the strategic and operational levels of military intelligence must work together to provide the necessary resources, methods, techniques, tactics, and procedures to accomplish future intelligence missions.

Nevertheless, it is essential not to forget that contemporary war scenarios have limits and gray areas that must be considered.

Contemporary War Scenarios

Patrikarakos (2021) argues that conflict is guided by two principles: first, that force is not always the best way to reach strategic goals, and second, that 20th-century geopolitical and security models are insufficient for today's threats. Therefore, using cyberspace as a new battlefield plays a crucial role in creating the impact needed to meet objectives.

At this point, it is essential to note that several factors suggest that modern war scenarios are increasingly focused on traditional domains of warfare. The areas of knowledge, influence, or activity, and the territory where dominance is exercised, become useful tools that help describe broad areas of understanding and visualize the environment where operations occur (Ejército Nacional de Colombia, 2017b).

Considering that "cyberspace is a global domain within the information environment composed of interdependent networks of information technology infrastructure and data, which include: the Internet, telecommunications, networks, computer systems, and integrated processors and controllers" (Ejército Nacional de Colombia, 2017b, p. 491), its significance in modern conflicts should be emphasized. Consequently, it must be utilized to its fullest potential to gain a strategic advantage against the adversary.

Gray-Zone Conflicts

National and international laws prohibit security and defense agencies from acting irrationally or illegally; therefore, these gray areas are heavily exploited by threats. In other words, the locations, areas, and illegal activities carried out have several

key supports, including secrecy, encryption, geographic sanctuaries, and legal loopholes.

In this regard, it is worth noting that secrecy allows actors considered threats to carry out actions without being identified, and in some cases, it is also impossible to determine why they carry out their plans. Furthermore, encryption enhances this by hindering forensic identification of the criminal network. For its part, geographic sanctuary benefits cybercriminals, as they enjoy protection from other States. Ultimately, loopholes in the law form the foundation of cybersecurity and cyber defense, indicating that without adequate tools, a meaningful response to threats cannot be achieved.

Conclusions

Strategists must recognize that part of every political and military conflict occurs online, and because of its widespread and unpredictable nature, battles fought there can be just as crucial, if not more so, than those on the actual battlefield.

The case studies indicate that it is no longer just hackers who caught national security and defense planners off guard, but rather more complex structures, organizations, and States that need to be examined from a wider perspective.

The landscape of modern warfare has shifted with the rise of cyberspace; therefore, any nation that does not dedicate itself to strengthening its cybersecurity and cyber defense measures today is walking a high wire, partly supported by land, sea, air, and space domains. In essence, they would not be strong enough to compete with cyber threats.

Additionally, the widespread presence of risks in cyberspace necessitates the activation of cyber intelligence at the strategic, operational, and tactical levels, which is essential for identifying, categorizing, and comprehending adversaries in cyber warfare.

Nothing can stop nations or States from building functional cyber capabilities, but ingenuity, expertise, and knowledge are crucial for success in cyberspace operations. Similarly, understanding the overall situation, the structure of the OE, and identifying problems enables the development of operational art options that support better decision-making on the battlefield.

References

- BBC. (2000, November 3). *Israel Lobby Group Hakend*. <https://tinyurl.com/muukxy4p>
- Bullough, O. (2002, November 14). Russians wage cyber war on Chechen websites. *InfoSec News*. <https://tinyurl.com/44h6c2vt>
- Colom, P., Coz, J., Fojón, E., & Hernández, A. (2013). Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales. *ARI*, (26), 1–10. <https://tinyurl.com/2p8puuvv>
- Ejército Nacional de Colombia. (2017a). *Manual Fundamental de Referencia del Ejército MFRE 1-01 Doctrina [Public]*. Imprenta Ejército. <https://tinyurl.com/2vpdpwpm>
- Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones [Public]*. Imprenta Ejército. <https://tinyurl.com/ducum7tje>
- Ejército Nacional de Colombia. (2019). *Manual de Técnicas del Ejército MTE 5-01 Metodología de Diseño del Ejército [Public]*. Imprenta Ejército. <https://tinyurl.com/3zjfspr2>
- Geers, K. (2004, April 4). *Cyber Jihad and the globalization of warfare: Computer networks as a battle ground in the Middle East and beyond* [Slide presentation]. <https://tinyurl.com/yjabbbax>
- Geers, K. (2009). *Cyberspace and the changing nature of warfare* [Keynote Speech IST-076/RSY-017]. OTAN. <https://tinyurl.com/bddy3pa>
- Geers, K. (2020). #Cyberwar: International Conflict in Cyberspace. In *Alliance Power for Cybersecurity* (pp. 3–5). Atlantic Council. <https://tinyurl.com/y5p2pajx>
- Goble, P. (1999, October 9). *Russia: Analysis from Washington – A real battle on the virtual front*. <https://tinyurl.com/5f798nju>
- Hess, P. (2002, October 29). *China prevented repeat cyber-attack on US*. <https://tinyurl.com/435u3bwz>
- Information Warfare Site [IWS]. (2001). *The Information Warfare Site*. <https://tinyurl.com/ycyzbxu2>
- Ministerio de Defensa Nacional. (2018). *Plan Estratégico del Sector Defensa y Seguridad. Guía de Planeamiento Estratégico 2018-2022*. <https://tinyurl.com/2sh6v5mt>
- Nakashima, E., & Mufson, S. (2008, January 19). Hackers have attacked foreign utilities, CIA analyst says. *Washington Post*. <https://tinyurl.com/43nc2fbm>
- North Atlantic Treaty Organization [NATO]. (1949, April 4). *The North Atlantic Treaty*. <https://tinyurl.com/yc2ujn2t>
- Page, B. (2000, November 11). Pro-Palestinian Hackers Threaten AT&T. *TechWeb News*. <https://tinyurl.com/5n7wnenj>
- Patrikarakos, D. (2021). *Un muy moderno "niebla de guerra", Ucrania: siete años después*. CHARCR.
- Porteus, H. (2010, June 10). *The Stuxnet Worm: ¿Just another computer attack or a game changer?* [In Brief, No. 2010-81-E]. Parliament Information and Research Service of Canada. <https://tinyurl.com/2hu9uasw>

- Preatoni, R. (2014, August 10). *Calling All Hackers*. <https://tinyurl.com/29w58ryh>
- Timothy, T. (2003). Information warfare in the seconds (1999-) Chechen War: Motivator for military reform? In A. C. Aldis & R. N. McDermott (Eds.), *Russian military reform 1992-2002*. Routledge.
- Wagstaff, J. (2001, April 30). The internet could be the site of the next China-US Standoff. *The Wall Street Journal*. <https://tinyurl.com/yuk6r3j2>
- Weisman, R. (2001). *California power grid hack underscores threat to U. S. news factor*. <https://tinyurl.com/f7nyz54y>