Chapter 5

Power in the Information Age: Perspectives on Cyber Power*

DOI: https://doi.org/10.25062/9786287818064.05

Milena Elizabeth Realpe Díaz

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This chapter analyzes the dynamics that take place in cyberspace. It explains how cyber power is beginning to be discussed in the general sphere of power while examining the meanings of the term according to different regional perspectives. It also describes the power from the U.S. military and the European Union perspectives. It expands the understanding of cyber power based on its location, all of which aim to establish adequate estimates of this subject matter.

Keywords: cyber conflict; cyberspace; cyber power; cybersecurity; power

* Book chapter resulting from the research project *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* conducted by the Cyberspace, Technology, and Innovation research group of Escuela Superior de Guerra "General Rafael Reyes Prieto," categorized C by the Ministry of Science, Technology and Innovation (MinCiencias) and registered under code COL0181179. The points of view and results of this chapter belong to the authors and do not necessarily reflect those of the participating institutions

Milena Elizabeth Realpe Díaz
Lieutenant Colonel of the Colombian National Army. PhD candidate in Strategic Studies, Security and Defense, and Master's in Cybersecurity and Cyber Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Master's in Information Security, Universidad de los Andes, Colombia. Specialization in Computer Network Security, Universidad Católica de Colombia. Specialization in Physical and Computer Security, Escuela de Comunicaciones del Ejército, Colombia. Specialization in Information Security, Universidad de los Andes. Bachelor's in Systems Engineering, Universidad Cooperativa de Colombia. Head of the Master's in Cybersecurity and Cyber Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. **https://orcid.org/0000-0003-4345-6182** - Contacto: **milena.realpe@esdeg.edu.co**

APA Citation: Realpe Díaz, M. E. (2025). Power in the Information Age: Perspectives on Cyber Power. In M. E. Realpe Díaz, & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 129-150). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818064.05

DISRUPTIVE TECHNOLOGIES, LOGISTICS, AND NATIONAL SECURITY AND DEFENSE IN CYBERSPACE
Print ISBN: 978-628-7818-05-7
Digital ISBN: 978-628-7818-06-4
DOI: https://doi.org/10.25062/9786287818064

Cybersecurity and Cyber Defense Collection
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Introduction

The technological revolution in the last years of the 20th century profoundly impacted how people relate to each other and perceive the world around them. The arrival of the internet and the digitization of information revolutionized the transmission and processing of information. For its part, the information technology revolution reshaped the material bases of a new society. Information technologies have become indispensable tools for generating wealth, exercising power, and creating cultural codes (López, 2002). According to Castells, this period of technological revolution corresponds to a historical interval during which the advances achieved by information technologies changed society's material culture, significantly influencing various activities performed by individuals, not as an exogenous source of impact but as a direct one (Castells, 2001, p. 112).

Additionally, the development and implementation of technologies have caused an accelerated transformation of the material base of society, profoundly affecting how people relate to one another and perceive the world around them, giving rise to the *information society.* This signifies that these technologies are present in people's daily lives and are used across various activities, from work and education to entertainment and interpersonal communication. As Estudillo states, it is a society in which new technologies and information affect the social structure in different areas of human life, such as the economy and social well-being (2002, pp. 83–84). Likewise, Castells (1996) maintains that information and communication technologies (ICT) are the driving force behind the transformation of society and have enabled the creation of a global economy and the real-time connection of people worldwide.

As Perlroth (2022) states, the internet, like many other things we now realize, has left us inextricably connected. Digital vulnerabilities that affect one affect all.

The barrier between the physical and the digital is increasingly insignificant. It is true that everything "can be intercepted," and most of what matters to us has already been intercepted: our personal data, intellectual property, chemical companies, nuclear power plants, and even the country's cyber weapons (p. 475). With this perception, technological progress and the internet are viewed as factors of social change. In this context, as noted by De Vergara and Trama (2017), the internet and technological developments have also significantly influenced the character of wars and conflicts. Several 21st-century authors agree, reiterating Clausewitz's postulates that conflicts are like a chameleon, changing their character depending on their nature, purpose, how they are led, the technology used, and the operational environment in which they occur (p. 58).

Thus, cyberspace arises as the common scenario where social, commercial, industrial, technological, and military interactions occur among people, organizations, institutions, banks, and armies. In this realm, threats, both criminal and those aimed at destabilizing states, often connect to rival or enemy countries. These actions result in cyber conflicts, "a type of conflict that takes place in cyberspace and that can involve military, intelligence, propaganda, and sabotage operations, in which actors use cyber tools and techniques to achieve their objectives" (Singer & Friedman, 2021, p. 2). An escalation of such hostilities in cyberspace leads to a cyber war, "...a serious form of disruptive cyber attack by a nation on another nation's cyberspace, crossing the line into being considered a use of force. Issues of the Law of War come into play" (Hunker, 2010, p. 4). In this context, a new concept emerges: *cyber power,* defined as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power" (Kuehl, 2009, p. 25).

As defined by Mitchell (1995), cyberspace is a new, digital dimension without borders, a space for communication and information exchange that has become an integral part of the daily lives of many people. It is a reality where new technologies bring opportunities and vulnerabilities for the most developed countries while contributing to an increasing technological gap with developing countries, especially concerning national security and defense (Ferreira, 2018, p. 36).

While technology has brought numerous benefits, it has also raised new ethical, political, and legal challenges that are still being addressed. If the multiple sources of information are analyzed, technology is becoming more accessible every day, allowing new threats to emerge from illegitimate regimes, terrorist groups, organizations outside the law, and organized crime that may have access to cyberterrorism, cybercrime, weapons of mass destruction, arms trafficking, and more. This implies a change in the concept of the traditional threat posed by identified enemies (CESEDEN, 2012, p. 126).

The above shows great concern, not only national but international, because although the relationship between the information society and cyberspace has brought significant benefits in terms of communication and globalization, it has also created a series of risks and challenges for society. It is important that steps are taken to address these issues and ensure that the benefits of technology are used responsibly and equitably.

From Power to Cyber Power

Historically, it was believed that a country's power depended on aspects such as its geographical location, national resources, the number of inhabitants, and its wealth, as these were considered essential elements for the development of military strength (Tellis et al., 2009). Traditionally, a country's ability to safeguard its borders from potential attacks, while being capable of threatening neighboring nations, was perceived as the ultimate symbol of its national strength. However, with the transition to the Fourth Industrial Revolution, conceptions of national power have evolved, incorporating the notion of a knowledge revolution. This transformation signals a significant change in the importance assigned to information technology and innovation within the structure and dynamics of society.

The evolution of the conception of power, from traditional notions based on geographical and economic factors to a new paradigm of cyber power, reflects the necessary adaptation to the Fourth Industrial Revolution. In this transition, the relevance of information technology and digital interconnection becomes a crucial element. The ability to leverage cyberspace to achieve strategic and tactical objectives redefines the landscape of influence and security in both national and international contexts. As digital technologies continue to evolve, it is imperative to address this emerging dimension of power in the contemporary era, where technology and information play a central role in shaping power dynamics and global relationships.

Migrating from power to cyber power implies adopting a series of measures and strategies that enable the utilization of the capabilities and resources of cyberspace to achieve strategic and tactical objectives. Additionally, it requires a significant transformation in how nations, organizations, and individual actors influence the global stage. This is due to the growing importance of information, communications, and operating technologies, as well as interconnection through the internet (Kuelh, 2009). The transition from a conventional power structure to a cyber power paradigm signifies the increasing preeminence of digital technologies and cyberspace in shaping influence and security in both national and international contexts. As these technologies continue to evolve, analysis and adaptation to this emerging dimension of power in the contemporary era become imperative.

In summary, traditional power and cyber power are two concepts that are intertwined today. On one hand, all power can be characterized as "the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate" and is only made evident by the effects it has on others (Barnett & Duvall, 2005). On the other hand, cyber power can be understood as the variety of powers that circulate in cyberspace and shape the experiences of those who act in and through cyberspace (Jordan, 1999, p. 3). Cyber power "is not created simply to exist, but rather to support the attainment of larger objectives... across the elements of national power—political, diplomatic, informational, military and economic" (Kuehl, 2009, pp. 41–42). Cyber power is one of the latest additions to the family tree of power, given how recent the digitalization of our societies and the emergence of cyberspace still is.

From Cyberspace to Cyber Power

To trace the evolution of cyberspace, from its origins to contemporary society, it is necessary to mention that this scenario is considered a strategic domain due to its capacity to transform society, influence the economy and politics, and affect the security and defense of countries. On this premise, it is essential to recognize that *cyberspace* is a term that has been used for approximately half a century; therefore, it is natural to present its evolution. This was first introduced in the book *Future Shock,* by Alvin Toffler (1970). Later, it was used and recreated by William Gibson in his works *Burning Chrome* (1982) and *Neuromancer* (1984), and consequently, it has multiple definitions, such as the one established by Bauman (2000): cyberspace is a space of uncertainty and ambiguity, where social identities and relationships can be easily constructed and deconstructed. For Castells (2010), cyberspace is a virtual space that extends beyond the physical world, in which users can interact, collaborate, create, and share information and knowledge, and in which information and communications technology play a central role (p. 69).

The history of humanity is also a record of the constant confrontations between civilizations and peoples. Modernity, for its part, brought with it two world wars, possibly the bloodiest known to date; however, it must be acknowledged that these gave rise to various formal institutionalized initiatives, such as the UN, along with a significant number of theoretical approaches that, for example, revitalized the romantic Kantian idea of perpetual peace (Kant, 1795), or defined or reinforced the notions and necessity of adhering to human rights (HR), International Humanitarian Law (IHL), and the traditional laws of war (LOW), which divide the *Jus ad Bellum* (the decision and causes of starting the war) from the *Jus in Bello* (which regulates the conduct of war).

Kant's idea was romantic and even anachronistic, yet materially correct, as the creation of a league of nations was a plausible initiative. Even though its operational ineffectiveness or the emergence of new forms of conflict and oppression at its expense would later be seen under the banner of humanitarian intervention or peace operations, Fisher (2011) points out that humanitarian interventions can take a wide variety of forms, from the provision of aid to the use of military force (p. 221). It is essential to quote Kant to contrast good ideas and intentions with pragmatic political achievements, along with their results and impacts.

> Preliminary articles of perpetual peace between states. 2) No state having an independent existence—whether it be great or small—shall be acquired by another through inheritance, exchange, purchase or donation. 3) Standing armies (*miles perpetuus*) shall be abolished in course of time. 5) No state shall violently interfere with the constitution and administration of another. (Kant, 1795, pp. 247-249)

We will leave this reflection at this point only to note that the regulations of war and human conflicts evidently fall short and are inappropriate to meet the demands of cyber conflicts, which are even more complex, diffuse, and conditioned.

The *postmodern global order,* as it is appropriate to call it, is usually studied from international relations, science, and political philosophy. For Gómez (2017), it is analyzed in terms of structure, actors, processes, their relationships, power, and phenomena such as violence. The structure is determined by the inclination toward the ordered or anarchic model of the international system; the position of the actors depends on the roles they play; and the processes operate based on interactions of conflict or cooperation (p. 59).

According to Hardt and Negri (2004):

> In the contemporary global order, a permanent global war is waged where the actors, even without pursuing common objectives and despite their inequalities, must cooperate [...] Empire rules over a global order that is not only fractured by internal divisions and hierarchies but also plagued by perpetual war. The state of war is inevitable in Empire [...] War is becoming a general phenomenon, global and interminable [...] a general global state of war that erodes the distinction between war and peace such that we cannot longer imagine or even hope for a real peace [...] the traditional distinction between war and politics becomes increasingly blurred [...] war, that is to say, is becoming the primary organizing principle of society, and politics merely one of its means or guises. (p. 8)

What stands out about Hardt and Negri's approach to the contemporary global order is that the very notion of *world power* has eroded. While it is true that there are key actors who fight tirelessly for economic hegemony, like China, or geostrategic hegemony, like Russia, complex interdependencies and the need for vital resources and dispersed interests make cooperation, deterrence, or even deception valid strategies for prospering and gaining advantage. This is especially relevant since many of these assets are intangible, products of knowledge, software, and cyber weapons available to the highest bidder, free from the control of states. This is reflected in Nicole Perlroth's research recorded in her book, *This Is How They Tell Me the World Ends:*

> For decades, under the protection of classification levels and confidentiality agreements, the U.S. government became the world's leading zero-day hoarder. U.S. government agents paid a high price (first thousands, then millions of dollars) to hackers willing to sell their lock-picking codes and their silence. But then, the USA lost control of its supply and the market. Now those zero-days are in the hands of hostile nations and mercenaries who do not care if your vote is lost, your water is polluted, or our nuclear power plants collapse. (Pelroth, 2022, p.1)

Studying cyberspace power helps us understand current threats. In an increasingly digitalized world, military operations and national security depend heavily on cyberspace systems. Grasping their importance will provide a clear path to protecting national interests, maintaining international stability, and promoting scientific and technological progress in the field of cybersecurity.

Foucault (1966) states that scientific knowledge is linked to power relations and that scientific discourse can be used to justify forms of social domination. Studying cyberspace power is essential because cyberspace has become a fundamental component of modern military activities. In this context, current military conflicts often involve cyber operations, which can significantly impact a country's ability to protect itself or conduct military operations.

In contexts of war, as well as in scenarios where it has not been explicitly declared, as Hardt and Negri would affirm, within the scope of permanent global war, various types of incidents are emerging in cyberspace—attacks or conflicts that illustrate the competition for power among different states, corporations, or national and international organizations. Valeriano and Maness assert that, in cyberspace, competition for power and influence is central to cybersecurity and cyber conflict. This approach carries significant implications for international politics and security, as cyberspace evolves into a new domain of strategic competition within the international system (Valeriano & Maness, 2015).

It is time to say that, based on the premise of permanent global war, ways of waging it have emerged that have led to definitions such as fifth generation wars, hybrid wars, cyber wars or cyberconflicts, and the special war doctrinally developed by the U.S. Army in the U.S. Army Special Operations Manual, ADP 3-05 (2012, p. 9), as well as MDOs (multi-domain operations). They all share the commonality of being carried out, using, or involving actions in cyberspace to a greater or lesser extent; consequently, understanding them is essential when assessing the cyberspace power related to each of them.

Many actions occur in cyberspace; moreover, it can be asserted without hesitation that these actions are executed by state actors, intelligence forces, and agencies. Media and cyberspace operations are conducted, often undisclosed, of which we can only observe the effects. For our topic, this is, *a priori,* unapproachable or even ineffective, but in reality, it is precisely the foundation of our inquiry. What types of cyber weapons are utilized? How do they function? How significant is the role of artificial intelligence in all this? And what is of utmost interest: How, being clandestine, can these capabilities be assessed as part of a State's arsenal or cyber power?

Hybrid wars, according to the LISA Institute, are those that combine military force with elements such as cyberattacks, manipulation of information via the internet and social media, or economic pressure. In such wars, cyberspace serves two functions: as a tool for conducting information operations and related actions, or as a battlefield where specific adversarial objectives are pursued. In this scenario, the use of cyber weapons is extensive, and their application is typically more evident and regulated, even doctrinally, as operations in cyberspace; case studies will be extremely useful in determining the extent of this regulation.

Before addressing cyber conflicts, the so-called special warfare is introduced. It is defined by the RAND corporation (2016) as a peculiar form of war and a strategy to protect and achieve U.S. national interests from a realist perspective that pays little attention to the ethical implications of the procedures. This approach is considered justified and permissible for intervening in other countries indirectly or surreptitiously, taking advantage to benefit unilateral interests while avoiding the compromise of troops and resources in decisive confrontations (p. III).

In many cases, special warfare can be viewed as a non-obvious war. According to Libicki (2012), technological and organizational innovations in recent decades have created the potential for a non-obvious war, where the identity of the fighting side and even the mere fact of war are completely ambiguous (p. 19). Libicki (2012) further points out that technological attacks—cyber warfare, space warfare, electronic warfare, drone warfare—and other strategies with long historical antecedents, such as sabotage, assassination, and the use of mines, are part of the spectrum of actions that can be executed in a non-obvious way. In all these cases, ambiguity underlies the lack of evidence: while the actor remains unknown, the act does not. Some non-obvious incidents of war would clearly be considered acts of war if they were more evident (p. 19).

It is indisputable, and we reaffirm it once again. In the study of cyber power, this form of warfare complicates the assessment and estimation of a state's actual assets and resources, as well as those it pays to enable these questionable ends.

In this type of warfare, political differences and global power dynamics are manifested through economic, military, and informational actions that impact the civilian population. This creates a breeding ground exploited by various global actors to enhance their power in cyberspace as an operational field. This includes not only strategic objectives targeting critical cyber and information infrastructures but also utilizing cyberspace as a repository of information where cyber and cognitive operations are consolidated as the fundamental source of hybrid conflict (Cano, 2021). The above highlights the importance of cyberspace today and how its evolution can affect the security, stability, and development of nations.

The President and founder of the World Economic Forum, Klaus Schwab, and author of the book *The Fourth Industrial Revolution* (Schwab, 2017), states that the Fourth Industrial Revolution promises great social changes. This technological revolution will completely alter the products we make, how we make them, how we interact, and, above all, who we are. As expected, this potential, characterized by the promise of automation and the interconnection of physical ecosystems with digital ones (Internet of Things, neural implants, smart prostheses, etc.), will not only offer benefits but will also pose dangers. War will also undergo changes (p. 2).

Schwab's aforementioned words present us with a form of conflict that is even more complex, where threats may not originate from actors in another country yet can endanger the strategic assets of states. This situation involves overwhelming threats in the face of which, without a doubt, traditional responses will be ineffective. Virtually, a redefined and possibly non-existent cyberspace military power will be required in the majority of the globe's defense forces.

From a strategic perspective, cyberspace has been recognized as an area of strategic importance for military power by many authors and organizations. In this context, Castells points out that cyberspace is a domain of global power with the potential to transform the functioning of society and the State. According to the author, digital networks enable the creation of new forms of political, economic, and social organization that can challenge the authority of traditional institutions (Castells, 2001). Furthermore, Kramer (2009) argues that cyberspace is a fundamental dimension of cyber power and national security, as conflicts in cyberspace can have devastating consequences for the critical infrastructure of countries and for the security of citizens. In modern society, cyberspace has become an essential arena for political, economic, and military activity, along with the role that artificial intelligence and cyber defense play in managing cyber conflicts (Arellano, 2019). In this regard, Psychogiou (2022) establishes that cyberspace has become the fifth battle space in an increasingly complex security landscape, and cyber threats have become part of the purview of international security (p. 1).

The above demonstrates that cyberspace has become a fundamental tool for the functioning of modern societies. Countries that can control and dominate cyberspace gain a significant advantage in military, economic, and political spheres. Cyberspace has transformed into a battlefield where nations can conduct covert operations without direct military intervention, enabling them to achieve strategic objectives without facing the consequences of armed conflict. Consequently, a relatively new form of conflict arises: *cyber conflict,* which becomes increasingly relevant as dependence on technology and the global interconnection of information systems grows.

Cyber conflicts should be regarded as a threat to national security and defense because cyberspace has become an essential dimension of the economic, political, and social life of nations—a virtual environment where communication activities and information exchanges occur through interconnected networks, technologies, and people. Incidentally, Thomas Rid (2012) has defined cyber conflict as the use of cyber means to trigger, escalate, or prolong a real-world armed conflict. Carr and Tikk (2021) argue that cyber conflict is a conflict involving the use of cyber tools and techniques to inflict damage or disrupt the computer systems of adversaries, which can have significant consequences for security, politics, and economics (p. 6). Additionally, Singer and Friedman state that cyber conflict is "a type of conflict that takes place in cyberspace and that can involve military, intelligence, propaganda, and sabotage operations, in which actors use cyber tools and techniques to achieve their objectives" (Singer & Friedman, 2021, p. 2). Although the definitions studied present a broad spectrum of perspectives on the subject, they all agree that cyber conflict entails the use of information and operational technologies to conduct hostile actions in cyberspace, either to damage or disrupt adversaries' technological systems or to achieve political, military, economic, or other objectives.

Meanwhile, Alberts and Hayes (2003) argue that cyber conflicts have become a significant threat to national security since computer and communications systems are essential for the functioning of the economy, government, and defense. The authors warn that cyberattacks can have serious consequences for critical infrastructure and society as a whole. Today, the nature of warfare and security has changed with the evolution of technology and the emergence of cyberspace as a new battlefield, presenting unique challenges and requiring a multidisciplinary approach. Various authors have addressed the importance of studying cyber conflicts. For example, Kramer argues that cybersecurity is fundamental to national security and that states must consider the technological, political, and social aspects of cyber conflicts. For his part, Libicki discusses the concept of cyber deterrence and the threats involved, highlighting how retaliation can help deter cybercriminals. Cyber conflicts are an expression of power in the information society, where the control of information and technology is essential (Libicki, 2018).

As noted, one of the challenges for studying cyber power, which also exhibits a notable strategic advantage of cyber conflicts, is that these can be carried out covertly, without the need for a large investment of material and financial resources and with the possibility of causing a great impact on the critical infrastructure of a country or an organization. Additionally, cyberattacks can be launched from anywhere in the world, making it difficult to attribute responsibility to a specific actor. Clarke (2010) argues that cyberspace offers a strategic advantage to adversaries because it allows them to operate undetected and affect critical systems such as infrastructure, communications networks, and military systems. This new form of conflict allows state and non-state actors to level the playing field against stronger adversaries, considering that cyberspace is a domain in which size and economic capacity are not necessarily determinants for the success of an attack. Kramer argues that cyber conflict can provide actors with a tactical advantage by allowing them to penetrate adversaries' information and communication systems to obtain classified information or disrupt command and control systems (Kramer, 2009).

Another strategic advantage of cyber conflicts is their ability to inflict damage and impact key objectives without the need for a conventional military force. Through cyberattacks, they can cause significant harm to critical infrastructure systems, such as energy, transportation, healthcare, and finance, which can have serious repercussions for the economy and society as a whole. According to Rid (2013), cyber conflicts allow powerful actors to extend their influence into cyberspace without the costs associated with conventional military operations (p. 4). This enables them to inflict considerable damage on critical infrastructure systems, financial and communications networks, among others, without putting their own military forces at risk. Cyberattacks can serve as a form of coercion and deterrence in international relations, conveying messages to other global actors and threatening greater repercussions if certain conditions are met (Libicki, 2009, pp. 11–12). Fernández (2022) states that from 2021 to the present, cyberattacks have been utilized as a non-conventional weapon among States; the primary parties involved have continued to be the nations that previously demonstrated significant activity in cyberspace, namely the USA, China, Russia, and the European Union, which are now joined by other countries that have previously not been very active in cyber conflicts, such as India, as well as other consistently active players like North Korea, Israel, or Iran (pp. 313–314).

From these statements, one can infer that the strategic advantage of cyber conflict lies in its capacity to inflict significant damage without risking one's own military forces. Additionally, it serves as a tool for coercion and deterrence in international relations. Cyberspace military power represents a latent priority on countries' agendas; however, we must not overlook the fact that this reality complicates how nation-states define, value, and acquire their cyberspace military power.

Cyber power is a form of power projection in the information age, and its development is essential for the security and defense of nations. Sánchez (2019) argues that cyberspace power is a critical tool for national security and defense, as it allows states to protect their critical computer systems and ensure their sovereignty in cyberspace. The author contends that cyber power is an integral component of national security and that its development should be a priority for governments. According to Segal (2017), cyberspace power refers to the ability to control and exploit cyberspace to achieve political, economic, or military objectives, whether by protecting one's own critical infrastructure or disrupting that of adversaries.

Cyber power allows us to achieve superiority or supremacy in cyberspace. This capability can provide a country with a strategic advantage regarding national security, politics, economy, and military. By establishing strong dominance in cyberspace, a country can protect its own information and communication systems while simultaneously spying on, sabotaging, or disrupting other nations' systems. Furthermore, cyberspace serves as a crucial platform for the digital economy and technological innovation, meaning that a country with an edge in cyberspace can secure a leading position in global trade and technology. Therefore, the contest for superiority or supremacy in cyberspace has become an important aspect of today's geopolitical competition. Countries strive for dominance in cyberspace because they believe that controlling information and communications in this domain is vital for their security, economy, and global influence. The competition for superiority in cyberspace significantly impacts national security and international relations (Sanger, 2018).

Countries compete for superiority in cyberspace to maintain national security, protect economic interests, and ensure political and social stability (Tikk & Kerttunen, 2020). They strive for this superiority because information and knowledge are the most valuable resources in the world today, and controlling these resources is key to power and influence (Stavridis & Farkas, 2012). This reflects the necessity for a nation or organization to develop cyber power and assert its superiority or supremacy.

Cyber power has become a fundamental element for national security and the defense of States because cyberattacks can cause serious damage to critical infrastructure and the economy of countries (Cujabante et al., 2020; Libicki, 2018; Valeriano & Maness, 2020).

Perspectives on Cyber Power

According to Nye (2011), not only have the types and sources of power in countries changed, but these changes also occur in the international context, specifically the scenario where States coexist. It is important to note that countries must coexist with other non-governmental actors. The perspectives on cyber power are broad and varied. First, cyber power is viewed as an essential tool for power projection in the modern world. Unlike traditional power, which is based on physical force and coercion, cyber power relies on the ability to influence and control individual behavior through cyberspace. Although cyberspace has not yet been used as a medium to exhibit the conventional hard power of coercion and threats supported by physical force, it does offer a suitable platform for projecting the soft power of attraction and imitation. Finally, the perspectives on cyber power are presented and analyzed from American military or strategic viewpoints (Kuehl, 2009; Nye, 2010) in contrast to Dunn's (2018) interpretations regarding cyber power in the European Union.

To continue this analysis, it is necessary to understand what I have termed the *localization of cyber power,* which follows two trends: the first is linked to the definitions of military cyber power and corresponds to a reductionist perspective that views cyberspace as a management tool that must be preserved to maintain the initiative; hence, operational efforts focus on generating protocols for the defense of strategic assets, sometimes pertaining not to the nation but to the forces, which is even more limiting. The other perspective, referred to as *comprehensive,* is expressed with the definition of cyber strategy or cyber power integrated into other domains or forms of national power; it incorporates and expands the core and capabilities associated with cyber power, based exclusively on the cyberspace domain, and adds or integrates with other components.

Cyber Power in the USA

To understand cyber power from the theory of military cyber power proposed by Gaines (2015), it is necessary to understand the terms and principles that form the basis of this theory and help to understand and apply operations in cyberspace in the context of joint operations and the expansion of combat power:

- Cyberspace: A global domain that encompasses physical, logical, and personal elements in the cyber realm.

- Cyber power: The application of operational concepts, strategies, and functions that employ operations in cyberspace to enhance combat power and achieve military objectives.
- Cyber military strategy: The development and employment of operational capabilities in cyberspace, integrated with other capabilities across different domains, to expand combat power and reach military objectives.
- Key terrain in cyberspace: Any physical, logical, or personal element of cyberspace that, if disrupted, degraded, or destroyed, limits combat power and provides a significant advantage to one of the combatants.
- Military cyberspaces: The various cyberspaces that exist, considering their diversity and heterogeneity.

Based on these precepts, the theory proposed by Gaines states that the integration of cyberspace operations with joint operations can expand joint combat power in several ways (Kern, 2015).

Operations in cyberspace present a series of strategic advantages. First, they offer greater attack capability, enabling joint forces to disrupt the enemy's command and communication infrastructure, significantly weakening their ability to respond. Additionally, these operations provide enhanced defense, allowing joint forces to safeguard their own networks and systems against cyberattacks, thereby ensuring the integrity of their combat power. Cyber operations offer greater situational awareness by gathering real-time information on enemy activities and capabilities, which facilitates informed decision-making and agile adaptation to changing situations (DoD, 2011).

Finally, these operations can support and enhance other military capabilities, such as land, sea, and air operations. This translates into increased effectiveness and coordination in joint missions, either by neutralizing enemy defenses before a conventional attack or by providing intelligence and communications support during combined operations. Overall, integrating cyberspace operations into joint operations expands combat power by introducing new forms of attack and defense, improving situational awareness, and leveraging additional military capabilities (Gaines, 2015).

Cyber Power in the European Union

Driven by ongoing concerns about threats from cyberspace, cybersecurity has emerged as a priority issue on the political agendas of States and international and supranational organizations, including the European Union (EU). The associated policy debate centers on measures to regulate behavior in cyberspace, aiming to transform it from a rebellious and insecure environment into a more stable, reliable, and orderly one. At the heart of this discussion are fundamental questions of power and control (Dunn, 2018).

The difficulty with the concept of cyber power is that there are still no systematic (empirical) analyses of the topic; in fact, the body of literature on cyber power is small and fragmented. Existing texts, including those specifically addressing European cyber power (Klimburg & Tirmaa-Klaar, 2011; Sliwinski, 2014a, 2014b), are primarily policy-oriented in nature and are accompanied by a contextually restricted understanding of power that is not necessarily easily applicable to other policies and contexts (Dunn, 2018). Addressing issues of power through empirical research, rather than conceptually, theoretically, or normatively, generally entails numerous challenges. These challenges are evident in the extensive literature written on various aspects of power in international relations and the efforts made to quantify it.

According to Dunn (2018), the EU assumes cyber power in various ways. Firstly, the EU recognizes the importance of cybersecurity and has developed policies and strategies to address cyber threats (Manners, 2002). The EU employs various instruments, institutions, and agencies to exercise different forms of cyber power, both internally and externally. Internally, the EU utilizes voluntary arrangements, incentives, dialogue, cooperation, and coordination to enhance its cyber power.

From an external perspective, the EU advocates a cooperation policy based on promoting cyberspace as an area of fundamental rights and freedoms. However, it is accepted that the EU lacks a unified strategic approach to intentionally wielding its cyber power. Although the EU has the capacity to utilize non-state cyber elements to support its policies, there is no clearly defined strategy to fully harness this power. As information technology becomes an increasingly central component in the convergence of security issues, it is recognized that any political actor with regional or global ambitions must engage in the cyber sphere. Therefore, it is suggested that the EU develop a kind of cyber power underpinned by resilience and the EU's core values, such as prevention, integrity, and multilateralism (Dunn, 2018). In short, the EU assumes cyber power through cybersecurity policies and strategies, using various instruments and agencies, both internally and externally. Nevertheless, the need to develop an integrated strategic approach to fully exercise its cyber power is acknowledged.

Conclusions

The transformation of cyberspace toward cyber power represents a fundamental change in the conception of power in the contemporary era. This change has been driven by technological advances that have turned cyberspace from a simple means of communication into a strategic field where battles are fought for influence, security, and supremacy. Cyber power not only implies the ability to control and manipulate cyberspace but also the ability to exert influence and achieve political, economic, and social objectives through digital means.

The diverse perspectives on cyber power reflect the complexity and multiple dimensions of this phenomenon. On one hand, some visions highlight the opportunities that cyberspace offers for innovation, collaboration, and citizen empowerment. From this perspective, cyber power is seen as a democratizing force that expands access to information, facilitates citizen participation, and stimulates economic and social development.

On the other hand, more critical approaches highlight the risks and challenges associated with cyber power. These visions caution against the growing vulnerability of critical infrastructure to cyberattacks, the erosion of privacy and security of personal data, and the potential for online manipulation and disinformation to undermine democracy and human rights.

In this context, understanding and addressing diverse perspectives on cyber power is crucial for designing effective policies and strategies that promote the responsible and ethical use of cyberspace. This involves strengthening cybersecurity, safeguarding individuals' digital rights, and fostering inclusive and transparent governance of cyberspace at both national and international levels. Ultimately, the challenge lies in harnessing the opportunities that cyber power provides to drive progress and human well-being while mitigating the risks and addressing the challenges posed by this new dimension of power in the 21st century.

References

Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: Command... Control... in the information age.* CCRP Publication Series. http://www.dodccrp.org/files/Alberts_Power.pdf

Arellano, A. (2019). *Ciberconflicto: La nueva amenaza global.* Instituto de Ingeniería UNAM.

Barnett, M., & Duvall, R. (2005). Power in international politics. *International Organization, 59*(1), 39-75. https://doi.org/10.1017/S0020818305050010

Bauman, Z. (2000). *Modernidad líquida.* Fondo de Cultura Económica.

Cano, J. J. (2021). Los conflictos híbridos y el poder de los algoritmos. *Revista Sistemas,* (161), 62-72. https://doi.org/10.29236/sistemas.n161a6

Carr, M., & Tikk, E. (2021). *International law and cyber conflict: Responding to new challenges.* Cambridge University Press.

Castells, M. (1996). *La era de la información: Economía, sociedad y cultura* (Vol. 1, La sociedad red). Alianza Editorial.

Castells, M. (2001). *La galaxia internet.* Plaza & Janes.

Castells, M. (2010). *The information age: Economy, society, and culture* (Vol 1., The rise of the network society). John Wiley & Sons.

Centro Superior de Estudios de la Defensa Nacional [CESEDEN]. (2012). *El ciberespacio: Nuevo escenario de confrontación.* Ministerio de Defensa Nacional. https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it.* Harper Collins.

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357-377. https://doi.org/10.21830/19006586.588

DoD. (2011). *Department of Defense Dictionary of Military and Associated Terms.* DoD. https://irp.fas.org/doddir/dod/jp1_02.pdf

Dunn, C. M. (2018). Europe's cyber-power. *European Politics and Society, 19*(3), 304-320. https://doi.org/10.1080/23745118.2018.1430718

Estudillo, J. G. (2002). *Visibilidad de la producción académica de feministas mexicanas a través de una base de datos* [Bachelor's thesis, Universidad Nacional Autónoma de México].

Ferreira da Silva, P. (2018). Oportunidades y desafíos de tecnologías emergentes: La importancia de la industria aeroespacial para Brasil. *Revista Fuerza Aérea-EUA,* (2), 36-48. https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%201%20Issue%202/Spanish/05-peterson_s.pdf

Foucault, M. (1970). *El orden del discurso.* Fabula Tusquets Editores.

Gibson, W. (1982). *Burning Chrome*. Ace Books.

Gibson, W. (1984). *Neuromante.* Minotauro.

Gómez Rodríguez, G. A. (2017). *Riesgos de transgresión moral del militar en la postmodernidad* [Thesis, Universitat de Barcelona]. Repositorio UB. https://diposit.ub.edu/dspace/bitstream/2445/119533/1/GAGR_TESIS.pdf

Hardt, M., & Negri, A. (2004). *Multitud: guerra y democracia en la era del imperio.* Debate.

Hunker, J. (2010). *Cyber war and cyber power: Issues for NATO doctrine* [Research Paper, N.º 62]. https://ciaotest.cc.columbia.edu/wps/nat/0031912/f_0031912_25908.pdf

Jordan, T. (1999). *Cyberpower: The culture and politics of cyberspace and the internet.* Routledge.

Kant, M. (1795/2010). *La paz perpetua.* Porrúa.

Kern, S. (2015). *Expanding combat power through military cyber power theory* [Master's thesis, Joint Advanced Warfighting School]. Repositorio institucional. https://apps.dtic.mil/sti/pdfs/ADA621664.pdf

Klimburg, A., & Tirmaa-Klaar, H. (2011). Cybersecurity and cyberpower: Concepts, conditions, and capabilities for cooperation for action within the EU. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf

Kramer, F. D., Starr, S. H., & Went, L. K. (2009). *Cyberpower and national security.* Potomac Books, Inc.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr & L. K. Wentz, *Cyberpower and National Security* (pp. 1-17). https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *Isjlp,* (8), 321. https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc8&div=17&id=&page=

Libicki, M. C. (2018). Expectations of cyber deterrence. *Journal of Strategic Studies, 41*(1-2), 44-57. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf

Lisa Institute. (n.d.) ¿Qué es la guerras híbridas y cómo nos afectan las amenazas híbridas. https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas#:~:text=En%20los%20%C3%BAltimos%20a%C3%B1os%20cobran,o%20vectores%20de%20presi%C3%B3n%20econ%C3%B3mica

MacDonald, D. B. (2009). *Thinking history, fighting evil: Neoconservatives and the perils of historical analogy in American politics.* Lexington Books.

Madden, D., Hoffmann, D., Johnson, M., Krawchuk, F., Nardulli, B. R., Peters, J. E., Robinson, L., & Doll, A. (2016, February 23). *Toward operational art in special warfare.* Rand Corporation. https://www.rand.org/pubs/research_reports/RR779.html

Manners, I. (2002). Normative power Europe: A contradiction in terms? J*ournal of Common Market Studies, 40*(2), 235-258. https://doi.org/10.1111/1468-5965.003

Mitchell, W. J. (1995). *City of bits: Space, place, and the Infobahn.* MIT Press.

Nye, J. S. (2010). *Cyber power.* Harvard Kennedy School.

Nye, J. S. (2011). *The future of power.* Public Affairs.

Pelroth, N. (2022). *Así es como me dicen que acabará el mundo.* Tendencias.

Psychogiou, V. (2022) Cyberspace: Is NATO doing enough? https://finabel.org/wp-content/uploads/2022/02/cyberspace-is-nato-doing-enough-1.pdf

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5-32. https://doi.org/10.1080/01402390.2011.608939

Sánchez, M. E. (2019). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. In G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 27-59). Escuela Superior de Guerra "General Rafael Reyes Prieto". https://doi.org/10.25062/9789585216549.01

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age.* Crown.

Schwab, K. (2017). *La cuarta revolución industrial.* Debate.

Segal, H. (2017). *Cyber-security at a frantic time: A rational plan.* Canadian Global Affairs Institute.

Singer, P. W., & Friedman, A. (2021). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

Sliwinski, K. F. (2014a). European union – Cyber power in the making. *Asia-Pacific Journal of EU Studies, 12*(1), 1-22. https://www.researchgate.net/publication/317717658_European_Union_-_cyber_power_in_the_making

Sliwinski, K. F. (2014b). Moving beyond the European union's weakness as a cyber-security agent. *Contemporary Security Policy, 35*(3), 468-486. https://10.1080/13523260.2014.959261

Stavridis, J., & Farkas, E. N. (2012). The 21st century force multiplier: Public–private collaboration. *The Washington Quarterly, 35*(2), 7-20. https://doi.org/10.1080/0163660X.2012.665336

Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity.* Routledge.

Toffler, A. (1970). *Future Shock.* Bantam House.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system.* Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. C. (2020). *Cyber strategy: The evolving character of power and coercion.* Oxford University Press.

Vergara, E., Trama, G., Uriona, M. N., Ortiz, J. U., & Destro, L. A. (2018). *Operaciones militares cibernéticas: Planeamiento y ejecución.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. https://cefadigital.edu.ar/bitstream/1847939/939/1/CAVIII%20-%20OMC%20DE%20VERGARA.pdf