Chapter 2

Challenges in finding sustainable leadership in cyberspace and the international system

DOI: https://doi.org/10.25062/9786287602502.02

Milena Elizabeth Realpe Díaz
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: In this chapter, a study is carried out in which the existing difficulties in establishing clear and forceful leadership in both cyberspace and the international system are evidenced, appealing to the *theory of realism of the discipline of international relations* and the study of threats and new forms of conflict. Certainly, the conjunction of economic, political and geostrategic interests has marked the dynamics in various dimensions at the national, regional and international levels, so it will be observed how this prevents some from eventually accumulating power resources in defined periods, but without genuinely establishing a leadership process. Finally, it addresses how cyberspace is analyzed as the preferred scenario of new forms of conflict, and how cyberspace power is not limited to the exclusive use of a nation's Military Forces but can be exercised by a large number of actors with the technical and human capacity for their own convenience in the cyber domain, which could force States to rethink the design of their national security and defense strategies.

Keywords: leadership, cyberspace, threats, international system.

Milena Elizabeth Realpe Díaz
Lieutenant Colonel, Ejército Nacional de Colombia. Ph.D. student in Strategic Studies, Security and Defense. Escuela Superior de Guerra. "General Rafael Reyes Prieto". Master's Degree in Cybersecurity and Cyberdefense, Escuela Superior de Guerra. Master's degree in Information Security, Universidad de Los Andes. Specialist in Computer Network Security, Catholic University of Colombia, Specialist in Physical and Computer Security, Army Communications School. Specialist in Information Security, Universidad de Los Andes. Systems Engineer, Universidad Cooperativa de Colombia.
https://orcid.org/0000-0003-4345-6182 - Contact: **milena.realpe@esdeg.edu.co**

APA citation: Realpe Díaz, M. E. (2023). Cyber threats in a hyper-connected world. In S. Uribe-Caceres & D. López Niño (Eds.), *Theoretical Approach to Notions of War and Strategic Leadership* (pp. 39-58). Sello Editorial ESDEG.
https://doi.org/10.25062/9786287602502.02

THEORETICAL APPROACH TO THE NOTIONS OF WAR AND STRATEGIC LEADERSHIP
ISBN (print): 978-628-7602-49-6
ISBN (online): 978-628-7602-50-2
DOI: https://doi.org/10.25062/9786287602502

Security and Defense Collection
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2023

Introduction

The technological changes that have accompanied human evolution have been, precisely, the basis for leaps that have led to the transformation of the human body, its environment, and the tools that the species uses to facilitate its life, maximize power resources and generate social, political and cultural changes that adapt to these technological transformations, and for which we enter what some have called *posthumanism.*

> It can be understood that the posthuman condition is configured under the tension between the definition of the ontological limits of the 'human', the 'animal' or the 'artificial' and a politics of emancipation that seeks to give a political meaning to these transformations. This means glimpsing the technological potential from the 'singular' historical moment in which the configuration, by way of 'enhancing', of our bio, psycho and physiological characteristics, will allow us, as a species, to shape a projected future, both for our longevity and our physical-cognitive aptitudes. (Cornejo, 2017, p. 222)

Although the central axis of this dissertation is not a bioethical reflection, it is necessary to contextualize that technology currently has interference even in biology, through biotechnology, which translates into an unparalleled power to transform life itself and create new worlds, designed in detail according to the convenience of the manager. Exactly this is close to what has gained popularity today: the *metaverse.*

What once seemed like a science fiction idea, in which the imagination of author William Gibson seemed to break every limit, is now a reality. In 1984, the publication of the novel *Neuromancer* gave the first glimpses of what is now known as cyberspace, recounting the life of a cyber cowboy, which at the time seemed

inconceivable, but now makes sense and focuses the attention of large technology companies, opening the possibility of living in a different context.

> The experience of maximum customization will most likely come in the metaverse, which we can translate as a space in creation 'beyond the universe'. This is the next technological stop, resulting from the mixture of virtual reality, social networks, video games and maximum speed internet. That parallel world let's say that, in another dimension, will offer us the possibility of being who we really want to be, without limits even for Physics. We are talking about a hypothesis, of course, of something futuristic, of one of those technological projects that we see on the horizon... But so far Mark Zuckerberg has already announced the hiring of 10,000 people to bring that metaverse to life. (Bueno, 2021, p. 6)

In this sense, it is necessary to examine what happens to the social forms that have taken the form of the nation states in which humanity is currently organized, as well as in intergovernmental organizations, non-governmental organizations (NGOs), transnational corporations and armed groups, which are the main actors of the traditional international system.

Thus, at the beginning of the study of these actors, classical authors, such as Thomas Hobbes or John Locke, made a comparison between the natural condition of man and the behavior of States. In this sense, the first, from a pessimistic viewpoint in anthropological terms, indicated that States, as well as humans in a state of nature, would only favor their benefit, since they are selfish and individualistic (Aparicio, 2018). Therein lies the genesis of one of the classical theories of the discipline of international relations, which will compose the theoretical framework of the present paper, accurately relating that, both in the traditional international system -which was forged since 1648, with the Peace of Westphalia- and in the fifth domain and in the possibility of living an alternative reality in the metaverse, there are clear limitations to consolidate the leadership of a single actor or that of a group of these.

The dynamics inherent in the human condition have led to strategies to concentrate power and wealth, and which are susceptible to the emergence of technological innovations. That is, although industrial revolutions have been conceived with the purpose of evolving -especially in the field of production processes-, in the end they have become excellent tools for the accumulation of power resources. Its ambiguity lies precisely in the interpretation and use that people and organizations

give to technology, which, on the one hand, can be an opportunity to substantially improve the quality of life, but, on the other, can mark the mutation of a series of threats that are present in the now so popular cyberspace.

Thus, from the approach to the qualities and characteristics of a leader and the comparative study of the international system and cyberspace, it will be sought to show that these contexts, although they have visible leaders within the units, do not facilitate the consolidation of a leader who persuades others to follow a certain path, imposes order and guarantees, as could happen in a traditional physical plane, the protection of rights or specific regulations.

The outstanding author and leader in cyber and conflict in cyberspace is Colonel Crowther, who, through the construction of knowledge, evidences his beliefs about the understanding of cyberspace as a domain of warfare that notably impacts the revolution of military affairs in digital realities. These beliefs are based on studying and explaining cyberspace, its conformation, the cybernetic domain, military operations in cyberspace and the art of war in a modern world, among others, all of which demonstrate that this fifth domain, unlike the traditional domains of land, sea, air and space, is a virtual environment created by man, who, therefore, has the possibility of leading, transforming and expanding it.

Consequently, cyberspace, by its nature, is not a safe or protected space: in fact, the attack surface has increased exponentially and, therefore, it is vulnerable to latent or emerging cyber threats or attacks, which can result in significant losses for the economic, political, and social sectors or constitute a serious threat to defense or national interests. For this reason, cyberspace is analyzed as the preferred scenario of new forms of conflict, as is the case of hybrid conflicts (Luque, 2019) and as a domain in, from and through which military operations create intended effects and where the fundamental military objectives related to this domain are essentially the same as in the other domains, and the main objective is freedom of action in, through and from cyberspace, as necessary to support the objectives of the mission.

Finally, the complexity of cyberspace power is addressed considering that it is not limited to the use of the Armed Forces. of a nation but can be accessed by a large number of actors with the technical capacity. In the context described the development of capabilities in cyberspace is a state priority, which presumes a redesign of national security and defense strategies. This new scenario serves as a means and an end, to achieve the modification, maintenance, or expansion of the *status quo* of the States and actors that, par excellence, have dominated the international agenda.

Methodology

From a qualitative analysis with the design of the grounded theory, in the first part a conceptual framework will be made to contextualize the transversal axes of this work: cyberspace, international system and metaverse, among others. Subsequently, from a theoretical approach, the guideline will be set for the analysis of the plausibility of a leadership dynamic in these spaces, so that, finally, it can be examined where the main actors are heading in order to guarantee their leadership in their immediate environments.

The design of the *grounded theory* is specifically chosen, since "the researcher produces a general explanation" (Hernández, 2014, p. 93) of a phenomenon, which is applied to a particular context in which various aspects are related.

Thus, by using various variables in this paper, we seek to find a relationship between them that allows us to explain the phenomenon that is being presented, for which a *theory of the discipline of international relations is used as a basis*, in the absence of an explicit one that deals with the proposed phenomenon, given its novelty.

General context of cyberspace and the international system

As already noted, it was in a 1984 novel that the first approximation was given to that space that opened in virtuality, and that was consolidated as the precedent par excellence when talking about cyberspace.

> It was the science fiction (cyberfiction) writer William Gibson (1948) who created the concept of cyberspace in his novel Neuromancer (1984) to designate the spatial scenario that existed within computers and their interconnections. And which now defines the anthropological space of the computer network where all users of the computer network when entering cyberspace become netizens, and which in turn make up the cybersociety, characterized by its alternative forms of socialization for the social appropriation of ICT, so that Cyberspace is a defining element of the virtual space of relationship between users of the Internet and other telematic or computer networks. (Martínez et al., 2014, p. 45)

Certainly, it is complex to find a single and complete definition; however, the one already provided brings together two fundamental aspects: the technical and

the anthropological. Although at the beginning it could be perceived that it is only a purely technological dimension, the fact that it is finally operated by humans' merits review from anthropology, sociology, etc. Precisely, when these aspects are integrated, it is when it is necessary to review how effective leadership is generated in the field, understanding that the spheres of life intermingle. Moreover, when the new generations do not know any way of interacting other than through the tools available there, and when more and more scenarios, which were usually *physical,* converge on this *virtual* plane, in which relations between States, world leaders and international organizations find opportunities and threats.

> Our private space and our public space interact with cyberspace and its services, with or without our authorization or knowledge. Therefore, although it is not perceptible by our senses, it is real because it is a product of the development of telecommunications, computing, interactivity and multimedia message: 'The only way to "see" cyberspace is through a "virtual reality", an 'artificial reality' built by man'. (Pérez, 2013, p. 2)

In that construction, intentionally or not, spaces have been left that can be co-opted by those who indiscriminately seek profit, power or the instability and consequent fall of their opposite. This is possible given the migration of processes to this digital environment, which generates benefits, but also vulnerabilities, especially with regard to critical cyber infrastructure.

In accordance with CONPES 3854 of 2016, the *critical cyber infrastructure* is that supported by information and telecommunications technologies (ICTs), and its operation depends on the State being able to guarantee its essential purposes and the provision of services to all citizens. If a failure were to occur in any of the digital platforms provided for this purpose, economic stability would be seriously affected, as well as the functioning of institutions and public administration; even, depending on the extent of the impact, an environment of uncertainty and chaos could arise.

These scenarios are planned on a national and international scale, as internal or external actors can cause such effects, depending on the interests they seek to collect. That is why it is plausible that, in the context of powerful actors, such as States, a simile is made with the international system, understanding that interdependence and globalization are two precepts that make everything have some connection and correlation; especially if it concerns the public.

Thus, Frederic Pearson and Martin Rochester (2003) refer to the international system as that general pattern that defines the political, social, economic, technological and geographical relations that shape the world agenda or, as they also simplify it, "the general scenario in which international relations occur at a given time" (p. 37).

In this sense, today those interactions across borders are taking place at a time when it is not necessary to take a plane to attend a presidential summit, but technological platforms allow real-time connections; especially, after the pandemic. Likewise, it is not necessary to fire a missile or mobilize troops for a conflict to explode or escalate, but, from an attack on critical cyber infrastructure, even more dire consequences can be caused than those of a trench confrontation.

Now, it is worth asking who is in control of those two spaces: cyberspace and the international system. You may wonder who leads and why. This, following Hoojberg et al. (1997), who establish that there are three axes of complexity in leadership: *cognitive, social* and *behavioral.* Therefore, to answer the questions raised, we will address, among other issues, how, from knowledge, the regulation of interactions and the control of the behaviors of those who interact in cyberspace, we can think about the consolidation of a leader.

Realism: the explanation and prescription of a particular world

Although the interactions between the units and various forms of human organization have been studied since ancient times, it was with the world wars when formal studies emerged that sought not only to understand what had caused such a disaster, but to prevent and foresee the possible outbreak of a new conflagration of such a level. Thus, in 1919, in Wales, the first Faculty of International Relations was created and the rigorous study of interactions between States began (Frasson-Quenoz, 2014).

With the end of the First World War, it was thought that the chances of a second war of the same type were, moreover, nil, having witnessed the extraordinary loss of human lives, infrastructure and economic resources. Therefore, liberalism emerged as the other classical theory that insisted on man's capacity for peace and cooperation as the best tools, not only to rebuild Europe after the war, but as a basis for the interaction of actors and, essentially, States.

However, incidents related to the expansionist interests of the Germans, Italians and Japanese were triggered (Venatici, 1978), which showed how the language of joint work was not being interpreted by all from the same perspective. It was then that Realism, as a classic paradigm, took control of the explanation and prescription of what was happening in the international system, not only towards the end of the 1930s, but throughout a history that evidences the individualist and belligerent action of some countries.

In this context, in the study of international relations as a scientific discipline, the principles proposed by Hans Joachim Morgenthau take force. In the first place, this classic author prescribes a theory of international politics with explanatory and prescriptive capacity, since, for him, realism cannot only be about explaining the world, but must also generate lines of behavior suitable for rulers (Frasson-Quenoz, 2014).

Likewise, it identifies that the motivation of the actors, of the politicians, is the interest in terms of power, which is the essential element of politics in general. Likewise, it reflects on morality and politics understanding that moral values can be incompatible with needs, so that, ultimately, these will be given priority.

One of the most important premises in this author was that the international system is anarchic and competitive, and he based his analysis on an essentially pessimistic human nature. Selfishness and the instinct for domination are what can describe the international system for what it is, and not as it should be, which is this author's main critique of classical liberalism (Frasson-Quenoz, 2014).

In this order of ideas, that anarchic nature of the system, as a central idea of Realism, is the key to understanding the limitations that exist when establishing clear leaderships. In addition, unlike a State that has a monopoly on the use of force because all citizens agree to cede part of their rights and freedoms to obtain the greater good of the protection and safeguarding of their primary interests, this is not the case in the international arena.

While the other theoretical approaches have highlighted, through historical examples, the functionality of cooperation and international institutions, among others, it is not possible to omit that potentially violent relationships have also profoundly transformed the international system. World wars and conflicts such as those that occurred with the dissolution of Yugoslavia and the Soviet Union, etc., show how the particular interests of each State prevail over the possibility of establishing relations of leader and followers, because in this way there would be no control of resources or possibilities of conquering a certain goal.

Thus, before, among all, building a path that leads to the general well-being of humans, each, from his own perspective, culture, religion, history and objectives, takes steps towards what he has prescribed for himself, even if it implies the weakening or elimination of the other. In the same way, it is necessary to take into account that, progressively, States are no longer the only actors with the capacity to act, but that intergovernmental organizations, NGOs, transnational corporations and armed groups have been the protagonists of several of the recent phenomena.

Especially since illegality, there are armed groups that have acquired extraordinary capabilities to destabilize entire nations. That is why in the following section an approach will be made to all the threats that emerge from cyberspace and are strengthened by issues inherent in the inability to fully identify the actors, the possibility of developing varied and innovative tactics and strategies and the failures of a system created by humans.

Cyber threats in a hyper-connected world.

The Secretary-General of the United Nations warned that "cyberwarfare had become a major threat to international peace and security and that massive cyberattacks could well become the first step in the next great war" (UN, 2018). However, there is widespread agreement among the signatory countries of the Charter of the United Nations, whose precepts apply in full to ICTs, together with the obligation on the part of States to resolve disputes by peaceful means. Hence, the behavior of States in cyberspace, in relation to the maintenance of international peace and security, is coming to the forefront of the international agenda (OEWG, 2021).

The consolidation of cyberspace as an issue that has become a general trend for most countries in the world has been triggering the expansion of the new attack surface for the national security spectrum. This, as a consequence of the fact that the greater the intensity of human action in cyberspace, the greater the potential for an eventual provocation of conflicts in cyberspace. This threat is not limited to national cybersecurity, but will also have an impact on the security and defense of States. In this context, it is necessary to mention that the domination of cyberspace was a career initiated by the great powers, such as Russia, the United States and China, and that is why they are a reference point for the creation of instruments that safeguard national security and defense in cyberspace (Gaitán, 2018).

At present, cyberspace is configured as an artificial domain created and modified by man, in which there is no absolute perfection and, consequently, it serves

as a parallel world in which humans can operate. In this way, all human activities carried out in the real world can also be carried out in cyberspace, with their successes and mistakes, their agreements and disagreements and, even, the multiple frictions and controversies that arise from daily coexistence in society. Which causes relations of enmity that could converge in the consolidation of threats or attacks in or through cyberspace or, in the worst case, in conflicts or wars of a cybernetic nature. Threats in cyberspace are classified as real threats, so facing them requires an effective defense strategy with high deterrence capacity (Nur, 2022).

Undoubtedly, if looked beyond the lack of physical consequences, cyberattacks can cause enormous damage by undermining social cohesion and trust in government institutions, given the steady growth of technological convergence, transmission speed, and individual empowerment within the cyber domain. According to the report presented by UNESCO regarding the Forum of the World Summit on the Information Society 2021, it is established that

> Societies have been transformed thanks to information and communication technologies in a way that could not even be imagined a decade and a half ago. In many cases, these technologies have fulfilled their promise of development and spectacular expansion of inclusion and participation in society. However, awareness of new risks has increased, such as misinformation and hate speech, digital surveillance, data privacy, and now the rise of artificial intelligence, all of which have important implications for human rights and fundamental freedoms. (UNESCO, 2021)[1]

The future of digital conflicts in geopolitics will have broad implications for public and private actors and for civil society. For this reason, in Colombia, since 2011, there has been talk of the importance of close cooperation not only at the national level, with the participation of multiple stakeholders[2], but also at the international level, which will be essential, but not sufficient, in order to prevent and resolve future digital geopolitical conflicts. The construction of political, social, economic and even military relations in this hyper-connected world not only requires the use of traditional media, but will also require resorting to the tools and means offered by cyberspace, in order to adapt to the new digital reality.

---

1 In the first instance, the effects of conflicts or attacks in cyberspace do not have a perception in the physical dimension, however, in the escalation of the conflict, effects can be seen when the critical cybernetic infrastructure is impacted, having effects on the physical survival of people.

2 Multiple Stakeholders: five actors: Government, Public and Private Company, Public Force, Academy and Civil Society. (CONPES 3854, 2016).

New forms of conflict

The existence of a parallel world in the form of a metaverse will trigger an expansion of the security spectrum, given the conditions of anonymity and clandestinity that allow one to act freely and, at times, evade laws and regulations. To face these threats, in addition to cooperation, it is necessary to build a defense strategy for the country for society in general, in addition to continuing to strengthen the country's cybersecurity and cyber-resilience capabilities.

With regard to Colombia, through the public policy document CONPES 3701 of 2011, it was established that the national defense would be in charge of the Armed Foces and, in particular, the Joint Cyber Command (CCOCI), based on the postulates according to which multiple stakeholders must be involved for national defense: territorial government entities, public and private companies, the Public Force, owners and operators of critical infrastructure, academia and civil society, making use of modern technologies and appropriate processes; However, above all, under the leadership of people capable of transforming everyday life by innovating under the new conditions of a digital current to make proposals that revolutionize the future in cyberspace.

This is the case of Colonel Crowther, who, through the construction of knowledge, evidences his beliefs about the cybernetic component, which increasingly acquires more strength and becomes a reference when it comes to influencing people through knowledge, and academia, and even in the transformation of military affairs, through issues related to cybersecurity and cyberdefense. These beliefs are based on studying and explaining cyberspace, its conformation, the cybernetic domain, military operations in cyberspace and the art of war in a modern world, among others. All of which demonstrate that this fifth domain, unlike the traditional domains of land, sea, air and space, is a virtual environment created by man, who, therefore, has the possibility of leading, transforming and expanding it.

Consequently, a fundamental variable in this new scenario is the human being, who interacts through their real identity or multiple digital identities. Crowther (2017) establishes that cyberspace has three layers: a *physical network,* which is framed in the *hardware.* A *logical network,* consisting of the *software* that makes the network operable, anda cyberperson, which are the humans who are leading and operating in cyberspace with their real identity and their multiple digital identities. Under this concept, both the physical and the personal layer exist within the States and, therefore, are subject to their laws and policies. This allows us to lay a

foundation for understanding the new reality. The human element is a fundamental part of the cyber domain that cannot and should not be ignored. Because humans built the cybernetic architecture, it is presumed inherently imperfect. Under its precepts, the fundamental imperative to mature the understanding of cyberspace is to treat it as a place, and not just as a mission. That is, cyberspace is a domain in, from, and through which military operations create intended effects. Similarly, the fundamental military objectives relating to that domain are essentially the same as in the other domains, and the primary objective is freedom of action in, through, and from cyberspace, as necessary to support mission objectives.

The result is to deny adversaries freedom of action at times and places of our choosing. The ability to do both provides cyber military superiority (USAFT, 2011). Thus, Colonel Crowther, the leader studied in this analysis, has been able to address different types of audiences, with different ages and races, strongly impacting the changes in issues associated with the cybernetic domain. This type of leadership is very well defined by Yulh (2010) when he states that leadership is the "process of influencing others to understand and agree on what needs to be done and how to do it, and the process of facilitating individual and collective efforts to achieve common goals" (p. 8).

Today's world, marked by the Fourth Industrial Revolution, requires VUCAH leaders (for the initials in English of *Volatile, Uncertain, Complex, Ambiguous and Hyperconnected*) to face a scenario characterized by instability. Cyberspace requires leaders to face unexpected, unpredictable, and sometimes turbulent changes, where each one is an integral part of the context of change itself, in which the theoretical perspective of Realism can be included, in order to explain and foresee the possible actions of those who, rationally, will pursue their particular interests in terms of power, even if this implies diminishing the capacities of a couple.

In this environment, a contemporary leader requires acting differently from a traditional leader. The role of a modern leader requires becoming successful change agents, with a broad capacity to adapt to continuous transformations and disruptive changes, with the right knowledge to face uncertainty, with the ability to respond to changes and recover to their normal state, despite any situation. That is, with the capacity for resilience not to give way to ambiguity; with the ability to communicate clearly and simply to combat complexity and, without a doubt, with enough emotional capacity to handle the new generations of alphas, *millennials* and *centennials* (IBERDROLA, 2022). Who are highly influenced by everything they

experience, see, hear and what they believe to be true; that is, their own beliefs, with the bias fostered by the explosion of information, not necessarily true.

Although in traditional leadership the use of symbols is not always so obvious and striking, when talking about complex leadership this type of identity is even more blurred, due to the diversity of the environment in which it is developed. A maxim of Crowther (2018), and which symbolizes his thinking, is to define that leaders with more experience and experience must understand how younger followers perceive and use technology. Although military leaders understand the importance of cybernetics and information, not everyone understands the scope of opportunities and challenges offered by cyberspace.

That is why this leader, through his approaches, has allowed us to understand and analyze that the military services will have to spend more resources on training and equipping. Not only the cyber forces, but all the forces that depend on technology and in that environment, they will be serving under a continuous cyber approach.

Nations and their defense capabilities in cyberspace

In the new national and international strategic scenarios, cyberspace is analyzed as the preferred scenario of new forms of conflict, as is the case of hybrid conflicts (Luque, 2019). The cyber domain, unlike traditional domains, presents great differences that deserve to be studied and investigated from different and advanced perspectives; especially, when we are faced with situations never seen before. During the International Security and Defense Symposium, in Peru, in 2005, PhD Kevin Newmeyer stated that, unlike the other domains, in which a potential possibility of conflict prevails, cyberspace has been completely shaped by man with uncertain borders and some rules for governance policy.

In this area, nations increasingly seek to control the cyberspace domain by generating *cyberspace power*, understood as the potential to use the cyber domain to achieve the desired results (Nye, 2011, p. 123). The complexity of cyberspace power is configured because it is not limited to the use of FFs. AA. of a nation, but can be exercised, according to a will, by a large number of actors with the technical and human capacity for their own convenience in the cyber domain, which could be evidence of the correct projection of the realistic paradigm of international relations.

For their part, Major General Evergisto de Vergara and Rear Admiral Gustavo Adolfo Trama, of Argentina's active reserve, point out that

> All actions carried out in this field will affect the armed component of national power from various perspectives. The first of these is the use of conventional military force in response to a massive cyberattack. The second involves the use of countries' conventional military power in the face of cyberattacks on civilian infrastructure (p. 11).

Similarly, operations in cyberspace are changing the characteristics of warfare. Although the nature of warfare is constant, the characteristics of warfare can change each time a new weapon or tactical approach is introduced. Cyberspace operations now make it possible to acquire and share more information and exercise better command and control on the battlefield, theoretically reducing the *fog of war* by adding fidelity to the commander's understanding of the battle space.

Thus, cyberspace enables more precise and effective use of the people and logistical capabilities involved by putting the right person or device in the right place, at the right time. These capabilities require governments and their FF AA to modify their practices. It also highlights the need for leaders and organizations to do a better job of selecting and using new technologies. Laws and policies must be updated to take advantage of new technology, also considering an international environment that works from complex geopolitical and geostrategic trends.

All this has led humanity - and especially the military component - to reflect on the intensive use of digital technologies as a trend that will remain in daily life, so that concepts such as cybersecurity and cyberdefense, applied by individuals, organizations and States, are extremely important to guarantee and capitalize on the benefit of connectivity and availability of information in a secure way, in order to provide an environment of greater possibilities for development. As well as social welfare and strengthening democracy in a nation.

Traditional and hierarchical views of leadership are becoming less useful, given the complexities of the modern world. Leadership theory must transition to new perspectives that account for the complex adaptation needs of organizations and states capable of meeting the challenges posed by cyber dominance. And in this context, Colonel Glenn (Alex) Crowther, a distinguished veteran and specialist in cyber policy, defines cyberspace, by nature, as neither a safe nor protected space and, therefore, vulnerable to latent or emerging cyber threats or attacks, which can result in significant losses to the economic, political and social sectors or constitute a serious threat to defense or national interests.

Consequently, states, increasingly dependent on technology, face the challenge of a wide variety of state and non-state actors in cyberspace, which is already enormous and constantly growing, without being clear which interests in terms of power they will manage. The integration of national capacities through their defense, security and justice departments have to operate in this environment as the three main actors of the government, which, in addition, must seek partnerships with the private sector, which operates almost all the internet. Therefore, the development of capabilities in cyberspace is a priority for the defense and security of Colombia, increasingly dependent on technology, while the deployment of military operations in cyberspace is a necessity for the advancement of current defense models (Sánchez, 2006).

Aligning these strategies on a national and international scale in a hyperconnected world is a bit complicated with traditional theories, as it is a dynamic that transcends the capacities of individuals alone. That is why it is necessary to generate new leaders capable of articulating the complexity of systems and establishing guidelines and postulates that allow theorizing and conceptualizing on issues related to cyberspace, which until today shows ambiguity.

In this context, Crowther (2017) has allowed the academic community to address the understanding of cyberspace as a domain of warfare that notably impacts the revolution of military affairs in digital realities. The leadership exercised is disseminated and materialized in societies of different nations through the construction of documents of great interest and international relevance that base their foundation on organizations such as the NATO Center of Excellence in Cyberdefense and other multiple organizations and nations that have taken advantage in the development of the race for the development of capabilities in the cyber field.

In this context, Crowther, whose resume totals more than 30 years of service in the United States Army, and includes eight tours abroad, with an extraordinary academic background and admirable experience, has found that, in this new scenario of confrontation, once societies understand the nature of the threats they face, it will be necessary to mobilize non-governmental assets adopting a *whole-of-society* approach to reduce the nation's risk. Here it is quite clear how, despite the widespread belief that the role of the leader is to "manage conflict", which means "reduce it". On the contrary, the conflict experienced in the dynamic tension between two systems is actually the key to innovation and adaptability in organizations, a clear characteristic of complex leadership.

Conclusions

The cybernetic domain was created by man, and in that context, as has happened with traditional forms of organization and interaction, human relationships have been expanding to unconventional digital environments. Likewise, with the use of the internet and technologies, the attack surface has increased exponentially, and with this, the risks associated with this domain generate the need to change techniques, tactics and procedures applied in the field of defense.

Current conflicts are governed by asymmetric warfare methods, with multiple vectors and activities that are enabled with greater intensity in cyberspace. In this context, it is necessary to have people capable of innovating, proposing and, above all, leading revolutionary changes in state and non-state organizational structures, in the generation of policies, programs, strategies and doctrine, in technological development and production, changes in strategies in the Public Force that allow the agile development of measures and countermeasures that make use of the cyber domain, or others that can be identified in the future.

The uncertainty of the anarchic international panorama, as conceived by the theory of realism of the discipline of international relations, and the rapid changes that are taking place in all areas are having a great impact on security and defense policies, both national and international (Gil, 2017). Which forces preventive actions and capacity building that can respond to an eventual conflict in this domain. To this end, the development of capabilities in cyberspace must be a priority for the security of any technology-dependent country.

As in the international system, the intentions, and interests, in terms of power, of the actors in the domain are not clear; even less so when the anonymity of the digital environment prevents identifying where the cyberattacks or the various emerging threats in the environment come from. This new scenario serves as a means and an end, to achieve the modification, maintenance, or expansion of the *status quo* of the States and actors that, par excellence, have dominated the international agenda.

Faced with this certainly complex scenario, it is imperative that each institution, organization, and State provide for the training of leaders in the new generations who develop the skills and competencies conducive to guaranteeing national interests, always ensuring that ethics and morality are included in such decision-making, whether in a physical or cybernetic dimension.

References

Aparicio, Z. (2018). El pesimismo antropológico en Hobbes desde una visión poliana. *Mercurio Peruano. Revista de Humanidades,* (531), 51-62. https://doi.org/10.26441/MP531-2018-A2

Bueno, C. (2021). Estoy en el Metaverso, ahora vuelvo. *Digital 4.0. Factoría & Tecnología,* (93), 6-26.

CONPES 3701. (2011, 14 de julio). *Lineamientos de Política para la Ciberseguridad y Ciberdefensa.* Departamento Nacional de Planeación. https://bit.ly/2UhnzYC

CONPES 3854. (2016, 11 de abril). *Política Nacional de Seguridad Digital.* Departamento Nacional de Planeación. https://bit.ly/3brazVR

Cornejo, S. (2017). La relación naturaleza y ser humano, tecnología y biología bajo la luz del posthumanismo. *Revista Antropologías del Sur, 4*(8), 215-232.

Crowther, G. (2017). *The Cyber Domain. The Cyber Defense Review, 2*(3), 63-78. https://www.jstor.org/stable/26267386

Crowther, G. (2018). *National Defense and the Cyber Domain.* The Heritage Foundation. https://www.heritage.org/sites/default/files/2019-10/2018_IndexOfUSMilitaryStrength_National%20Defense%20and%20the%20Cyber%20Domain.pdf

Frasson-Quenoz, F. (2014). *Autores y teorías de relaciones internacionales: Una cartografía.* Universidad Externado de Colombia.

Gaitán, A. (2018). *Ciberguerra. La consolidación de un nuevo poder en las relaciones internacionales contemporáneas.* Universidad Santo Tomás.

Iberdrola. (2022). *Tipos de liderazgo empresarial.* https://www.iberdrola.com/talento/tipos-de- liderazgo

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

Luque, J. (2019). *Los nuevos conflictos bélicos del siglo XXI: las amenazas híbridas.* [Programa de Doctorado en Ciencias Sociales]. Universidad de Murcia. https://repositorio.ucam.edu/bitstream/handle/10952/4239/Tesis.pdf?sequence=1&isAllowed=y

Martínez, L., Leyva, M., & Félix, L. (2014). Qué es el Ciberespacio. En L. Martínez, P. Ceceñas, & V. Ontiveros (Eds.). *Virtualidad, ciberespacio y comunidades virtuales,* (pp. 44-93). Red Durango de Investigadores Educativos, A. C.

Newmeyer, K., Cubeiro, E., & Sánchez, M. (2015). Ciberespacio, Ciberseguridad y Ciberguerra. En *II Simposio Internacional de Seguridad y Defensa de Perú* [Simposio]. Escuela Superior de Guerra Naval de Perú.

Nur, A., Ferdion, M., Ari, D., Abdillah, I. (2022) Indonesian StateDefense as an Effort to Counter the Cyber space Security Threat of Metaverse. *International Journal of Arts and Social Science.* https://www.ijassjournal.com/2022/V5I8/414665868.pdf

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. I*nternational Security. 1*(1), 44-71.

OEWG. (2021). *Open-Ended Working Group OEWG. Reporte Final 2021*. https://dig.watch/resource/oewg-2021-report

ONU, (2018). Documento S/2018/404 (2018, Annex, 3).

Pearson, F., & Rochester, M. (2003). *Relaciones internacionales. Situación global en el siglo XXI.* Mc Graw Hill.

Pérez, V. (2013). El ciberespacio: ¿una realidad en construcción? En P. Irala, & V. Pérez (Eds.). *Cibermedios. Palabra, imagen y tecnología,* (pp. 2-5). Ediciones Universidad San Jorge.

UNESCO. (2021). Informe de la Directora General sobre la aplicación de los resultados de la Cumbre Mundial Sobre la Sociedad de la Información (CMSI). En *Conferencia Anual 41ª reunión* [Conferencia]. UNESCO. Paris, Francia. https://unesdoc.unesco.org/ark:/48223/pf0000379370_spa

USAFT. (2011). *Cyberspace – The Fifth Operational Domain.* https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx

Venatici, C. (1978). *Los orígenes de la Segunda Guerra Mundial.* https://revistamarina.cl/revistas/1978/6/venatici.pdf