

Chapter 9

Limits of Artificial Intelligence and Big Data Technology in Intelligence Analysis*

DOI: <https://doi.org/10.25062/9786287818408.09>

Jaime Andrés Naranjo Ardila

Jorge Luis Mejía Rosas

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: Artificial intelligence (AI) and big data create a teaching and learning environment for processing information in intelligence analysis. This technology introduces new scenarios in the geopolitical, security, and defense sectors, with features that help define boundaries that national security agencies will examine. In this context, it is important to trace the development of AI, as scientific and technological advances are rapidly progressing. This trend is vital for those involved in processing information, as easy access makes it crucial to follow legal guidelines for protecting personal data. Additionally, the challenges posed by AI foster innovation in the legal protection of personal data and application use.

Keywords: analysis; artificial; intelligence; limits; technology.

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

Jaime Andrés Naranjo Ardila

Lieutenant Colonel in the Colombian National Army. Master's in National Security and Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Specialization in Leadership and Management of Military Units and Specialization in Military Resources Administration for National Defense, National Army Arms and Services College, Colombia. Diploma in Leadership with an Emphasis on Administration and Diploma in Administrative and Disciplinary Expertise. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. Email: jaime.naranjoar@buzonejercito.mil.co

Jorge Luis Mejía Rosas

Retired Colonel of the Colombian National Army. Specialization in Military Intelligence, Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano," Colombia. Specialization in Military Resources Administration, Arms and Services College, and Specialization in University Teaching, Universidad Militar Nueva Granada, Colombia. Bachelor's in Military Sciences and Bachelor's in Business Administration, Escuela Militar de Cadetes "General José María Córdova," Colombia. <https://orcid.org/0000-0003-3233-4948>
Email: jorge.mejia@esdeg.edu.co

APA Citation: Naranjo Ardila, J. A., & Mejía Rosas, J. L. (2025). Limits of Artificial Intelligence and Big Data Technology in Intelligence Analysis. In L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Commandos: Challenges Facing Special Forces and Intelligence in Contemporary Warfare* (pp. 189-208). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818408.09>

COMMANDOS: CHALLENGES FACING SPECIAL FORCES AND INTELLIGENCE IN CONTEMPORARY WARFARE

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

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

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

Security and Defense Collection

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introduction

It is no secret that over the last decade, there has been a significant technological shift in habits, preferences, and how products and services are acquired. As part of these advances, there are currently technological innovations that can be applied in the field of military intelligence, such as artificial intelligence (AI), the Internet of Things (IoT), virtual reality, blockchain, apps, e-commerce, and big data, focused on customer needs, but which until now have not been fully utilized. Indeed, AI enhances information collection processes by creating a comprehensive data control system, which improves organizational performance and allows the Force to develop various skills, agreements, and commitments based on the science of military intelligence.

This chapter aims to analyze how AI and big data technology are used in military intelligence for planning in Special Operations (SO). First, it examines the technological advancements impacting Military Intelligence and Special Forces (SF), highlighting that innovation enables secure data collection through cryptographic codes that have not been breached so far. The chapter emphasizes the need to develop a plan that promotes the adoption of proactive measures to avoid improvisation when facing high-risk threats. Therefore, the use of big data and AI is seen as contributing to prevention, control, and mitigation efforts, while also ensuring the anonymization of personal data.

This process must include "data mining and big data" because if the variables and expectations of all stakeholders the organization interacts with are not considered, it will not be able to achieve its objectives and goals. Therefore, it is essential to perform control and monitoring at this stage to ensure the plan is practical and achievable.

Second, it connects AI and big data technology to human intelligence in SO. Based on the analysis, it is recommended that implementing processes and procedures is necessary to help the organization position itself effectively. To achieve this goal, AI is a practical option, as it allows the integration of all automated processes, creating a model that produces efficient results and, therefore, improves the information collection process. This enables the identification of the characteristics, customs, preferences, procedures, behaviors, and development of people and organizations.

Finally, the role of big data technology in ongoing improvement is analyzed as a global trend, suggesting that all kinds of good management practices should be examined.

Background

The first mobile apps date back to the late 1990s, when they were already embedded in computers. A clear example is the calendar in Windows 95, which initially started as an app that sent alert signals, or arcade games, a trend at the time, whose producers found a niche market (Bonami et al., 2020).

According to Ahedo and Danvila (2014), the evolution of apps continued with ringtone editors, which performed very basic functions and had a fairly simple design. From this point on, app development accelerated thanks to technological innovations, supported by significant advances in cell phones, as companies that produced them developed competitive advantage practices.

Actually, a revolution has started in the creation of apps, games, news, design, art, photography, and medicine, all in the hands of users, thanks to the rapid innovation processes of mobile applications (Fernández, 2020). At the same time, the internet has produced numerous high-quality tools aimed at fostering innovation through information and communication technologies (ICTs), providing personalized access to data and allowing citizens to identify the strengths and weaknesses of public administration.

This was evident during the handling of the coronavirus pandemic (Fernández, 2020), when it was publicly discussed that these innovations could violate rules regarding the right to *habeas data*, as they collect and centralize user information by locating personal data. Although used solely for health statistics, this data is centralized only for informational purposes (Navarro, 2014).

Therefore, while this information can be used to verify it with information centers, it can also be exploited to locate a person in real time for criminal purposes. Therefore, as Daza (2020) points out,

it is crucial not to oversimplify, polarize, or reduce the issue to just a renunciation of privacy to protect life or health, or to avoid lockdowns and other restrictions on our freedoms. Privacy violations, like those during the coronavirus pandemic, are often not recognized or felt until it is too late. Therefore, if the debate is framed in these extreme terms, no one would prioritize privacy. (p. 12)

Learning is another area where AI makes sense, as there are currently applications that, for example, convert maps into three-dimensional (3D) scenarios when viewed with a mobile device or webcam. Although these applications respond to the need to determine people's health status, identify risks, and include alarms or alerts, it is clear that these technological advances lead to a scenario that goes beyond the information level, as they deploy functionalities with invasive characteristics (Orozco, 2003).

Evolution in the Conception and Planning of Contemporary Hybrid War Scenarios or Confrontations

Currently, the evolution of conflicts in the international system has made adversaries invisible due to the widespread use of technology, creating many challenges for modern societies. This is especially clear when it comes to developing security and defense strategies, as well as public policies that can protect national interests, given the various risks to peace and harmonious coexistence. The importance of this issue is clear, especially with the emergence of new actors capable of destabilizing institutions in pursuit of their interests, which are often protected within the illegal economy and override the State's goals (Valencia et al., 2019).

In this context, the evolution of technology has enabled advancements in AI, which has achieved notable results across various fields of society. This has improved the ability to make informed decisions amid unexpected events by analyzing data processed by machines. However, this also creates high-risk scenarios for humanity's survival, as countries like the United States, Russia,

and China have revamped their national security strategies using AI resources to defend their interests during conflicts or peacekeeping missions.

Historically, globalization has gradually transformed the way a national security strategy is defined, leading to the creation of crisis, normalization, and stabilization zones, all aimed at fostering peace. State security has evolved over time and made a significant leap forward after the September 11, 2001, attacks on the Twin Towers in New York. This event revealed the rise of new threats to global security, which used different methods of action and attack. Consequently, state intelligence agencies adapted and prepared, leveraging technology to accomplish their goals.

Indeed, it is clear that the main advancements in AI are occurring in world power States, both in their security and defense strategies and in the implementation of their strategic plans. However, the fact that this technology is used in a wide variety of scenarios introduces the risk of serious threats emerging, some of which are technological and others human-related. Experts warn that two major threats linked to AI are that it could become self-sufficient or superintelligent, surpassing human abilities, and that it could be used for lethal or malicious purposes against other countries or non-state actors.

The self-sufficiency of AI, meaning when it surpasses humans in all understandable aspects, has already been considered by science and is called "the technological singularity." Stephen Hawking argued this point, openly saying that such technology could spell the end of humanity. Meanwhile, Nick Bostrom (2016), a professor at the University of Oxford, believes that AI can, to some extent, replace human intellectual work, such as by providing better analysis. He emphasizes that this kind of technology must include human values and work in harmony with all society's actors to produce positive outcomes; otherwise, Bostrom (2016) warns, the scenario could be catastrophic and irreversible for humanity.

From a more moderate perspective, Dr. Ramón López, director of AI in Spain, states that super AI is still far from reality, and therefore, the idea that this kind of technology could dominate the world lacks scientific foundation, since the necessary technological evolution is required to achieve the singularity (Pérez, 2023). Other experts point out that even if an AI with a higher intellectual level existed, it would never be superior to humans, as it does not interact with the environment in a human-like manner. However, these reflections make it clear that all types of ethical dilemmas must be thoroughly examined, especially regarding the use of autonomous weapons (Valls, 2018).

However, regarding AI used for criminal activities, Sonia Pacheco (as cited in Rubio, 2018), director of the Business World Congress, points out that it can have a significant impact due to the risks it poses to a State's security and defense. In this context, it is important to distinguish between the "unintentional" misuse of AI and its "intentional" misuse, such as using drones for terrorist purposes or manipulating electoral contests with accounts that use algorithms on social media to automate messages, known as bots, which perform repetitive tasks 24 hours a day. An example of this malicious use of AI is the attack on military bases in Syria by non-state actors or the development of autonomous weapons that are lethal (Rubio, 2018).

AI, a Strategic Component of a State's Defense

AI is a technology that can be viewed either as a destabilizing factor in military force deployment or as a disruptive tool across all sectors of society's economy, industry, and social activities. The geoeconomic and geopolitical capabilities produced by this technology directly influence the international strategic landscape, as they support informed decision-making and the development of national security strategies, allowing for the consideration of the most critical variables to choose the best course of action. While its use depends on the capabilities of individual States, it is currently a mechanism that major powers such as the United States and Russia have adopted.

Therefore, the development of AI is a crucial element of national security, helping shape domestic policies that align with international community considerations. This technology has gained widespread acceptance, with China in 2017 launching an ambitious state plan with a future-focused technological program (2030) aiming to become a global leader in AI applications. As a result, a worldwide race for dominance in this field started, according to a 2018 World Economic Forum report, which estimated that investment in AI will reach \$127 billion by 2025.

It is crucial to analyze the strategic idea of AI and the reasons for governments' substantial investments. Specifically, the current world is constantly changing, with major powers competing for technological and military dominance, vying for international influence, and aiming to protect their national interests.

Indeed, States that use AI should develop a multilateral foreign policy, considering the various threats in the global environment, such as climate change, the spread of weapons of mass destruction, financial crises, and pandemics. The

need to create and implement cooperation mechanisms that can unify efforts across multiple dimensions is clear.

Similarly, the use of AI is important for, for example, fighting pandemics and multidimensional poverty, or strengthening international commitments aimed at improving transportation infrastructure. Greater economic and social development boosts people's quality of life and raises the demand for better environmental protection, which in turn increases their participation in the global trade dynamics.

In this context, it is important to recognize that blockchain enhances AI processes in national security and defense, supporting better management of information aligned with national interests. Additionally, it aids in applying accounting methods in organizational performance, fostering the development of skills, agreements, and commitments in these technological areas, although it always faces limitations related to data protection, confidentiality, and privacy (Martínez, 2019).

In turn, this blockchain trend enables secure data storage using a cryptographic code that has not been compromised so far. Mechanisms for managing such information are evolving within a framework of globalization and technological progress surrounding the global village, showing that companies face specific risks that can affect their sustainability and profitability.

Means Used in Planning and Executing Contemporary Hybrid War Scenarios or Confrontations

Planning involves various methodologies that consist of systematic, step-by-step procedures leading to a series of decisions that can produce results in the military field. Specifically, the desired end states are defined through a study of the operational environment, with a focus on utilizing the capabilities of military units, including AI optimization, to attain a position of relative advantage over the adversary and other threats. These tasks are based on decisive action and promote offensive maneuvers (Bonami & Dala, 2020).

Considering the new security and defense challenges, the Joint Force is called upon to perform all types of activities using AI, in conjunction with the development of military operations, to create a strategic advantage and capability that will enable it to be more effective against current threats and trends in global security (Hueso, 2019).

Therefore, the use of AI technologies is not only important for movement and maneuver, as they improve the integration of the country's security and defense to achieve a unified effort in consolidating territories, but also in military operations, which aim to gain a relative advantage against any threat that endangers the lives and dignity of Colombians (Bravo, 2010).

The use of AI also makes it possible to neutralize the main structures of Organized Armed Groups (OAG) through aerial reconnaissance to identify the positions of mobile columns and through intelligence work (human and technical) on the enemy. This enabled the Government to effectively reduce activities such as kidnapping, homicides, and all types of illicit acts between 2018 and 2022. This state policy, as it has become, demonstrates the importance of institutions "occupying" all national regions and contributes to society's performance in eradicating the social inequalities the country faces (Galindo, 2005).

Indeed, planning involves the continuous and simultaneous coordination of military forces' activities, and in doctrine, it serves as one of the fundamental components of capabilities. This reflects the transformation of the institution's new organizational structures in pursuit of strategies for change and renewal, as well as the new vision, awakening, and potential transformation in training and capacity building. In this context, Unified Land Operations (ULO) enable initiative and provide an advantageous position against various sources of violence through a series of offensive and defensive operations, as well as collaboration from inter-institutional or international perspectives.

Military professionals utilize the art of movement and maneuver through training and tactics, guided by the commander's intent, by selecting among interconnected options.

- Types of offensive or defensive tasks that describe the maneuvers and tactical mission tasks
- Combat organization of available forces, including the distribution of limited resources
- Fundamental choice of control measures
- Time (before, during, and after) of the operation
- Challenges the commander is willing to take on (Vigevano, 2021)

This element is crucial for strengthening cooperation between Colombia and its allies, given that State Strategic Intelligence and Counterintelligence are key factors in decision-making. Additionally, it is important to consider that external factors directly influence Colombian foreign policy, and this element will help in achieving the State's main objectives.

- From a strategic point of view, the relationships between Colombian intelligence agencies and their allies can be strengthened by developing strategic intelligence and counterintelligence activities to protect national interests and gain greater control over transnational crimes.
- From an operational perspective, military intelligence can enhance its capabilities and resources with the main goal of conducting coordinated operations that directly target illegal armed groups operating in border regions.

In this context, the intelligence cycle within a hybrid warfare setting can be defined as the set of skills and abilities that, through the use of AI, enable the analysis of economic, political, and social factors. These components, working in an integrated manner, enhance combat effectiveness with the goal of gaining a military advantage and initiative to counter all types of threats to a State's sovereignty and policies. Currently, the implementation of all interventions relies on conflict-sensitive program management and a cross-cutting approach to equity issues. Special attention is also given to developing sustainable solutions and intervention methods, one of which is military intelligence, involving the broadest possible participation.

Hybrid Confrontation Scenarios Applied to Colombia in the Context of a Hegemonic and Regional Confrontation

Currently, there is an arms race to achieve global dominance, with the United States, China, and Russia as the main competitors. These countries understand the importance of enhancing their AI technologies to serve their national interests, a development the academic community calls the "AI Cold War." For example, China has invested about \$150 billion in technology as part of its development plans. This is why they are adopting proactive strategies to become world leaders in AI and establish themselves as the center of global innovation in the near future.

Undoubtedly, compared to previous economic and social revolutions, the development of AI is both dynamic and universal, as it ensures continuous and simultaneous connections that form the basis of so-called globalization. It influences economic, commercial, political, and social activities, capital accumulation, the creation and sharing of knowledge, and information management worldwide.

Similarly, following the Industrial Revolution and the advent of mass production, automation, and robotics, "Industry 4.0" is already considered the "Fourth Industrial Revolution" due to its potential and benefits related to integration, innovation, and process autonomy. The concepts of Industry 4.0 and smart manufacturing are relatively new and contemplate the introduction of digital technologies in the manufacturing industry; that is, the incorporation of technologies such as IoT, mobile computing, cloud computing, big data, wireless sensor networks, embedded systems, and mobile devices (Valencia et al., 2019).

However, some objectives help enhance information processes through open sources. A clear example is that these technologies encourage situations where individuals can share their collaborative skills, join groups, and build a sense of teamwork to gather useful information from large data flows. As shown, these technological features support long-term education.

In this context, for AI's information process to be thorough, specific specialties are needed—such as identity profiling, systemic situational analysis, and foresight—that help create a unique representation of humans. These specialties determine qualities of unification, consolidation, communication, and decisive actions, enabling controlled integration of AI and intelligence. Blockchain aids in distributing, but not copying, digital information. A simple example illustrates this: a spreadsheet duplicated thousands of times across a computer network. The network then updates this spreadsheet regularly, forming the basis of a blockchain (Palomo-Zurdo, 2018, pp. 11–23).

Currently, there is a wide range of information collection programs in the cyber environment, not only for academic purposes but also for obtaining precise data for a State's public services. As a result, there are programs that organize people's information based on their employer, home location, interests or preferences, and other relevant details to gather important data (Navarro, 2014). Some of the most commonly used open-source programs are:

- *Shodan*: This search engine locates computers, webcams, printers, and various electronic devices
- *Namechk*: It shows whether a username is available on more than 150 online services.
- *Tineye*: It is a search engine that, based on a picture, shows which websites it is on (Navarro, 2014).
- *Pipl*: This search engine connects people to different social networks and online links.

- *Domaintools*: This service identifies, monitors, searches, and analyzes a domain name.
- *Tagboard*: It analyzes different Twitter (now X) hashtags.
- *Twopcharts*: This tool analyzes everything posted on Twitter, allowing you to view likes, the timeline, and the history of posts, lists, and relevant content.
- *Foca*: This program extracts and analyzes metadata from different types of documents (Arcos, 2015). By understanding the metadata, you can determine who created or modified it, the type of software used to generate it, and other relevant information about the file (Rosales, 2005).
- *Metapicz*: It extracts metadata from photographs and thus reveals various types of information, such as the camera, software, dates, and phone used.

In this respect, the reality is that organizations cannot afford to wait that long in an era where cybersecurity breaches happen quickly, as an organization's security relies on rapid identification and response. This raises the question: How can a country like England, with strong information security processes, enhance its ability to detect "advanced adversaries" in systems and networks? The answer is that organizations have recently sought to proactively develop various processes, while simultaneously optimizing their cyber and AI infrastructures and institutions (Chipuxi & Paucar, 2020).

The Role of Special Forces in Using AI as a Strategic Tool

The process of automation and monitoring through sensors plays a vital and essential role for SF soldiers in today's operational environment. AI is increasingly advancing in gathering all types of meteorological data, as well as information on the physical and health status of personnel, and on a soldier's capabilities, in real-time to enable optimal decision-making. Additionally, regarding the enemy, it helps understand their weapons, identify their strategies, and analyze their courses of action to attack or defend based on patterns provided by large servers, among other highly relevant aspects.

Therefore, to fully develop AI's potential, interconnection is vital—i.e., the constant exchange of information between different systems, enabling each to

respond to potential threats. However, to accomplish this, access protocols for such data must be strong, ensuring no loss and preventing enemy interference.

In turn, AI enhances decision-making by allowing sensors to be placed on soldiers to monitor their physical and emotional states, as well as on vehicles and systems, and by utilizing aerial photography and audio and video recordings of the operational environment, providing a wealth of valuable information. Typically, 90 percent of SO involves planning and establishing strategies, control points, enemy locations, and other critical aspects. According to General Clarke, Commander of the U.S. Special Operations Command, most military leaders, especially those in the SF, spend the majority of their time on planning (Barceló, 2001).

Therefore, modern armies with SF must create new organizational structures that include AI technology to scan all types of computers and cell phones; gather and counter messages left by adversaries on social media and analyze their trends; examine in detail the situation and the enemy's interests or objectives; and establish an operations center to combat all forms of fanaticism and violent extremism that aim to destabilize government entities (Palomo-Zurdo, 2018).

In turn, AI must assist in detecting electromagnetic threats. For instance, drones equipped with this technology and autonomous learning capabilities can select targets and carry out direct fire actions. These operations must be overseen by an operational legal advisor to ensure the best legal decisions are made, always safeguarding the integrity of law enforcement officials. In this context, human control over these machines is essential to ensure humanitarian protection and proper legal oversight.

In this regard, it should be noted that the U.S. Department of Defense, in Directive No. 3000.09 of November 12, 2012, defines an autonomous weapon system as

A weapon system that, once activated, can select and engage targets without further intervention by an operator. This includes, but is not limited to, operator-supervised autonomous weapon systems that are designed to allow operators to override operation of the weapon system, but can select and engage targets without further operator input after activation. (U.S. Department of Defense, 2012, p. 21)

Autonomous weapons systems without human control are tools that select and attack targets based on criteria set by programming engineers and operational rules. However, they cannot be stopped by human intervention once the attack has

been initiated. It is also important to note that there are currently over 380 semi-autonomous weapons developed by Israel, China, the United States, and other countries (Sossa & Reyes, 2021).

Although they have not yet been used in armed conflicts, they are expected to be deployed soon as robotics and AI advance. To this end, developed countries, especially major powers, are investing substantial financial resources into the military sector, making the replacement of soldiers with technology appear not to be a distant possibility (Acosta, 2020).

Not every automatic weapons system is fully autonomous, as human intervention in programming must comply with all legal parameters, which means it requires an operator. Currently, many military weapons feature high levels of automation and can also operate semi-automatically. Drones, for example, can perform tasks like taking off and landing automatically, without human control, thanks to routes programmed with the Global Positioning System (GPS).

In the United States, a large part of its defense budget is allocated to developing AI, giving it a significant edge over China, its main rival. Specifically, these technologies are connected to the following areas:

- *Unmanned operations*: Includes aerial, land, and marine systems, both surface and submerged, with unmanned and increasingly autonomous systems.
- *Long-range naval and air operations*: Utilizing floating expeditionary bases or unmanned tanker aircraft, which greatly extend the reach of U.S. Forces aircraft without depending on unreliable allies (Vigevano, 2021).
- *Unobservable operations*: Includes stealth technologies that go far beyond radar "invisibility." Aspects such as material composition, paint, and infrared emissions complicate invisibility to unimaginable levels (Gutiérrez, 2014).
- *Submarine warfare*: This is another field dominated by the United States, but China is building unmanned submarines that would be capable of carrying out kamikaze-style attacks against enemy vessels.
- *Systems engineering and integration*: This is the key to the entire U.S. military architecture. It consists of a system of systems, focused on new levels of inter-arms cooperation within each army and across the armed forces as a whole, enabling greater control over the battlefield.

Therefore, it is important that many countries have established various legal frameworks to regulate the protection of personal data. With the rise of AI and the availability of big data, there is a risk of personal information being compromised,

such as through impersonation or the creation of detailed profiles used for extortion, illegal political activities, or what is called cognitive warfare. *Cognitive warfare* involves manipulating the masses into believing a series of catastrophic events caused by their leaders' decisions, often without any clear criteria or objectivity.

In short, the United States' strategy aims to outpace Chinese advances to protect human combatants. It is developing remotely operated and autonomous unmanned aerial, naval, and ground systems capable of surprise attacks and striking anywhere, anytime, based on a global observation and attack network (Acosta et al., 2020).

In this context, new technological developments have shown that privacy and personal data protection can be compromised in various ways. This issue affects not only one country but millions of people worldwide, crossing borders, as recently exemplified by the Cambridge Analytica scandal in the geopolitical electoral arena. This company specializes in conducting tests on large populations to send personalized messages aimed at influencing their purchasing decisions in both commercial and electoral areas, encouraging citizens to buy certain products or align their voting intentions with specific candidates. The most notable case was during the United States presidential election that resulted in Donald Trump's victory (Hill & Dance, 2020). These events highlight the importance of establishing limits that security agencies must consider.

AI technologies are another resource available to personnel responsible for analyzing and processing information, facilitating the collective creation of knowledge through their easy access. However, it is crucial to establish guidelines to legally protect personal data, ensuring that the results of these analyses do not fall into the wrong hands of criminals or corporations that blatantly misuse it for electoral or commercial purposes. In this way, AI and big data can offer a teaching and learning environment for analyzing the information used in intelligence processes.

Ultimately, new AI challenges drive innovation and shape trends. In the military sector, AI and big data connect user information databases to analyze data and determine solutions or corrective actions, including monitoring what was planned versus what was actually executed to ensure goals are reached. Therefore, establishing guidelines for the legal protection of personal data in apps becomes increasingly important.

Conclusions

AI and big data technology in information analysis are essential concepts in the intelligence process. This must be considered at various levels of strategic planning, as using these capabilities can influence the operational environment and decision-making, especially in developing grand strategies. Likewise, the use of AI and big data continually refines and enhances intelligence capabilities to conduct analyses that closely mirror reality, enabling the creation of more accurate future scenarios in response to this new challenge.

Likewise, it is important to identify the variables and expectations of all involved parties to verify their honesty and credibility. This allows for the clear definition of objectives and helps determine which goals are most likely to be achieved. Therefore, developing more effective control and monitoring systems is necessary to ensure that planning aligns more accurately with reality.

With the advancement of innovation and technology, AI and big data can serve either positive or negative purposes; they might be used to create advantages that leverage favorable situations based on truth or deception. In this context, the use of AI and big data technology in the planning and execution of modern war scenarios or hybrid conflicts is critically important for decision-making, as these are carried out as a series of interconnected tasks and strategies that involve deploying forces and various spheres of power to gain a relative advantage over the adversary, threats, and instability factors.

In this context, Military Intelligence becomes more effective when it enhances its capabilities and resources to gather more intelligence. By conducting a more comprehensive analysis with these tools, decision-makers can create more effective plans for coordinated operations that support mission success and achieve the desired end state in various theaters or areas of internal and external operations.

For this reason, we need to recognize the revolution that these technologies are creating. For instance, if they are used to develop AI that identifies the adversary's center of gravity, it can greatly increase the advantage, making operational decisions more efficient and reducing human resource interventions, thus making them more lethal. Similarly, weapons technologies, no matter how advanced, become vulnerable if a State's strengths are significantly impacted, turning them into a disadvantage in the area of influence or within their own territory.

Currently, the world is focused on technological developments of all kinds. Crises have transformed it, and therefore, it has had to innovate to survive. This

makes it necessary, for better or worse, to change the way of thinking because the real world is transitioning into the virtual world. From a strategic perspective, AI and big data technologies will enhance relationships between intelligence agencies, enabling them to develop strategic intelligence and counterintelligence tasks that neutralize common threats and protect national interests, thereby increasing control. Regarding operational issues, military intelligence must establish agreements to strengthen its capabilities and resources, aiming to carry out coordinated operations that directly target illegal armed organizations operating within the national territory.

However, it should be noted that without a legal regulation for the use and development of AI, a dangerous gateway could open to a range of criminal activities and serious human rights violations. In this context, it is important to distinguish between the “unintentional” misuse of AI and the “intentional” misuse, such as for terrorist purposes, which threatens national security and defense (Romero, 2019). Therefore, establishing a binding international legal framework to regulate this technology is crucial to mitigate these threats.

In the current landscape of hybrid warfare, using AI to analyze economic, political, and social factors that directly boost combat power will facilitate the comprehensive execution of tasks, help gain a military edge, and therefore neutralize all kinds of threats to sovereignty and national policies. Thus, having these tools enables a cross-cutting approach to operational development that emphasizes the participation of military intelligence.

Finally, AI and big data are instruments that must always depend on the analysis and control of a person, who must determine what is useful and what is not in planning. Therefore, it is also essential that a legal framework be in place to regulate them and provide appropriate advice to safeguard all decisions made when incorporating these technologies.

References

- Acosta, A., Aguilar-Esteva, V., Carreño, R., Patiño, M., Patiño, J., & Martínez, M. (2020). Nuevas tecnologías como factor de cambio ante los retos de la inteligencia artificial y la sociedad del conocimiento. *Revista Espacios*, 41(05), 25–32. <https://tinyurl.com/35dm93jd>
- Ahedo Ruiz, J., & Danvila del Valle, I. (2014). Las nuevas tecnologías como herramientas que facilitan la educación. In J. Días-Cuesta (Ed.), *Estrategias innovadoras para la docencia dialógica y virtual* (pp. 25–40). ACCI.
- Arcos, R. (2015). Reservas de inteligencia: una comunidad ampliada de inteligencia. *Inteligencia y Seguridad*, (8), 11–38. <https://tinyurl.com/yc77ra2d>
- Barceló, M. (2001). A.I. (inteligencia artificial). *Byte España*, (78), 98–99. <https://tinyurl.com/32x36khf>
- Bonami, P., Piazzentini, L., & Dala-Possa, A. (2020). Educación, big data e inteligencia artificial: metodologías mixtas en plataformas digitales. *Comunicar*, 65(25), 43–52. <https://doi.org/10.3916/C65-2020-04>
- Bostrom, N. (2016). *Superinteligencia: caminos, peligros, estrategias*. Teell.
- Bravo, G. (2010). El proceso de inteligencia, vigilancia, adquisición de blancos y reconocimiento. *Revismar*, (1), 58–64. <https://tinyurl.com/3w85djeu>
- Chipuxi, V., & Paucar, J. (2020). *Propuesta de un modelo de cadena de suministro basado en tecnología Blockchain* [Bachelor's thesis, Universidad Central del Ecuador]. Repositorio UCE. <https://tinyurl.com/yc6t2h4b>
- Daza, M. (2020). *Grado de conocimiento y nivel de implementación de la tecnología Blockchain en empresas colombianas* [Master's thesis, Pontificia Universidad Javeriana]. Repositorio PUJ. <https://tinyurl.com/bdv3w9ys>
- Fernández, M. (2020). *Tecnología Blockchain en la logística portuaria* [Bachelor's thesis, Universidad de Cantabria]. Repositorio UNICAN. <https://tinyurl.com/vhh4ztb3>
- Galindo, C. (2005). De la seguridad nacional a la seguridad democrática: nuevos problemas, viejos esquemas. *Estudios Socio-Jurídicos*, (7), 496–543. <https://tinyurl.com/2vh6a55c>
- Gutiérrez Abarzúa, H. (2014). El concepto ISTAR: ¿Una herramienta válida para la función de inteligencia de las Fuerzas Militares del siglo XXI? *Revista Fuerzas Armadas*, (230), 55–63. <https://doi.org/10.25062/0120-0631.859>
- Hill, K., & Dance, G. (2020, February 10). Una aplicación de reconocimiento facial ha identificado a víctimas de abuso infantil. *The New York Times*. <https://tinyurl.com/2m3tj3yd>
- Hueso, L. (2019). Riesgos e impactos del big data, la inteligencia artificial y la robótica: Enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo*, (50), 1–37.
- Martínez Devia, A. (2019). La inteligencia artificial, el big data y la era digital: ¿Una amenaza para los datos personales? *Revista La Propiedad Inmaterial*, (27), 5–23. <https://doi.org/10.18601/16571959.n27.01>

- Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Investigación, desarrollo e innovación. *Ciberseguridad*, 10–12. <https://tinyurl.com/5xkx5k6b>
- Navarro Bonilla, D. (2014). El ciclo de inteligencia y sus límites: producción de información. *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, (48), 51–65. <https://tinyurl.com/58yw8ncj>
- Orozco, L. E. (2003). *La calidad de la universidad: más allá de toda ambigüedad*. <https://tinyurl.com/9rsx47tj>
- Palomo-Zurdo, R. J. (2018). Blockchain: la descentralización del poder y su aplicación en la defensa. *Boletín IEEE*, (10), 885–904. <https://tinyurl.com/2s43yc2y>
- Pashchuk, Y. (2013). *Medios de implementación de Instar en el sistema de Inteligencia de las Fuerzas de Ucrania*. Universidad Nacional de la Fuerza Aérea (KNAFU). <https://tinyurl.com/y5d6ujv8>
- Pérez, J. (2023). Ramón López de Mántaras, experto en inteligencia artificial: "La IA sola no resolverá absolutamente nada. Serán los humanos". *Diario El País*, <https://tinyurl.com/52vwc9m2>
- Romero, S. (2019). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. *Revista de la Escuela Superior de Guerra Naval del Perú ESUP*, 16(1). <https://tinyurl.com/56a4vwah>
- Rosales Pardo, I. R. (2005). La inteligencia en los procesos de toma de decisiones en la seguridad y defensa. *Cuadernos de Estrategia*, (130), 39–64. <https://tinyurl.com/2u9yczne>
- Rubio, I. (2018, November 15). Necesitamos la inteligencia artificial para sobrevivir como especie. *El país*. <https://tinyurl.com/4yy47rz2>
- Sarda, J. M. (2016, September 22). *En la inteligencia de un Estado se pueden mostrar varios tipos de amenazas a las estructuras organizacionales del mismo que pueden afectar los procesos de información. Toma de decisiones y manejo de amenazas*. Universidad de Valencia.
- Sossa Azuela, H., & Reyes Cortés, F. (2021). *Inteligencia artificial aplicada a robótica y automatización*. Marcombo; Alfaomega.
- U.S. Department of Defense. (2012). *DOD Directive 3000.09, "Autonomy in Weapon System"*. <https://tinyurl.com/466nkb9b>
- Valencia Bermúdez, M. P., Puerta Bohada, J. S., Collazos Ballén, N., Urrea, D., & Cañas C. (2019). Influencia de la cuarta revolución industrial en Colombia. *Punto de Vista*, 10(16), 1-18 <https://doi.org/10.15765/pdv.v11i16.1419>
- Valls, M. (2018). La inteligencia artificial y su encaje en las estrategias de seguridad nacional. *Boletín IEEE*, (12), 472–485. <https://tinyurl.com/4y38fw4c>
- Vigevano, M. (2021). Inteligencia artificial aplicable a los conflictos armados: Límites jurídicos y éticos. *Arbor*, 197(800), Artículo e600. <https://tinyurl.com/s73rua84>