Document Analysis

[Visit the WEB](#) [Receive E-BULLETIN](#)

09/2025 04/02/2025

Juan Luis Sánchez Sánchez Sánchez

Artificial intelligence in support of military intelligence. Fundamental axis of success or failure in the strategic competition between great powers

Artificial intelligence in support of military intelligence. Fundamental to success or failure in strategic competition between great powers.

Originally published in:
[Artificial intelligence in geopolitics and conflicts](#)
Issued in June 2024

Abstract:

The power of artificial intelligence, AI, in future technological developments will impact deeply in the global pre-eminence and in the strategic great power competition, the way of facing the crisis and hybrid conflicts and the multi domain military capabilities and their integration with the civil ones. The advanced use of AI applied to intelligence will allow a better and faster understanding of the strategic and operational environment in order to anticipate, in relation to competitors, the most appropriate management solutions that will allow the survival of the social, economic and political model of our liberal democratic societies.

Keywords:

Intelligence, Information, Artificial intelligence, OSINT, Cognitive warfare, Special operations, Intelligence Disciplines, Intelligence cycle, IMINT, SIGINT, Strategic competition.

How to cite this document:

SÁNCHEZ SÁNCHEZ, Juan Luis. *Artificial intelligence in support of military intelligence. Fundamental axis of success or failure in the strategic competition between great powers*. IEEE Analysis Paper 09/2025. [IEEE web link](#) and/or [bie link](#)[3] (consulted day/month/year).

A very real film

A crisis in country X has led to the escalation of inter-racial tension and the explosion of violence. The Spanish embassy in the capital advises the resident population to evacuate, going to the embassy premises to manage it. In the interregnum, an unidentified ethnic terrorist organisation attacks the embassy, killing its security service and taking an unknown number of hostages. The terrorist group's demands are unacceptable, nihilistic intent is foreseen, and they kill the hostages by self-immolation. Special Operations Units of the Spanish MOE[1] and Intelligence are requested to carry out a possible release of hostages, of national legal competence as they are consular territory and Spanish citizens; country X can only support.

The operational team alerted to the rescue operation immediately begins intelligence gathering by intelligence specialists. They search and manage access to all Armed Forces databases using AI from their LLM with *prompts* tested in other incidents similar to the real situation. The collection is autonomous and systematic, with mapping and aerial photography being downloaded first for individual and team digital planning and navigation systems. Simultaneously, in open sources, with the appropriate safeguards against alerting of intentions, OSINT search capabilities are put in place: the operational team, the intelligence units of the MOE (tactical level) and the MCOE at the operational level, supporting the other levels that have a need to know such as RINT n.No. 1[2] , J2[3] of the MOPS[4] at the operational level coordinating with X and allies and, of course, the CIFAS at the strategic level; the strategic guidance and planning unit in the Joint Chief of Defence Staff's Joint Staff also coordinates at STRATCOM . [5]

The AI presents in hours what used to take days, all the information available in the multiple databases of basic intelligence and by means of the appropriate *prompts* launches automated requests for information, RFI[6] , to the centralised management system of the Armed Forces Intelligence System, SIFAS, and collects with IA the requirements of all units involved in current intelligence acquisition and distributes tasks

---

[1] MOE. Army Special Operations Command (ET).
[2] RINT No. 1. ET Ground Force Intelligence Regiment No. 1.
[3] J2. Joint Level Intelligence Headquarters. NATO nomenclature.
[4] MOPS. Joint Defence Operations Command. In charge of command and control of external operations and, in the event of a conflict or crisis, would become the Operational Level Command.
[5] STRATCOM. Strategic Communications. In charge of coordinating information campaigns and executive measures for the cognitive domain, including psychological, "influence" and public information operations.
[6] RFI. *Request for Information*. Request for Information.

in an automated way to sensors, UAV flight plans, own and, where appropriate, allied control satellites, ships, submarines or electronic warfare aircraft and imagery intelligence.

The SIFAS AI alerts and provides all the nodes involved with reports and products available up to the moment on the crisis, adapted to their needs, with two points of contact: at the operational team that will have to carry out the operation, the main one; and at the political-military decision-making level.

Information is collected and summarised on ethnicities, leaders, their indirect psychological profiling, intentions, capabilities, type of weaponry available, support network of insurgent or terrorist groups; social networks of the country, locality and embassy environment are mapped, videos and multimedia material of insurgent groups are collected and biometric data such as facial features, voice, iris or tattoos and other distinctive identity attributes are separated from them to investigate who the perpetrators may be. AI separates and sequences hostile actors with their physical traits and CIFAS OSINT[7] teams collect *Identity Intelligence*[8] information from them: bank accounts, phone numbers, IP addresses and details of computers, servers, vehicles, family, friends, addresses, habits such as routes frequented, bars, shops... all with automated AI prioritisation of the relative importance of these actors. In addition, physical information is collected on Spaniards and workers who may or may not already be in the embassy. We do not forget the plans of the embassy and surrounding buildings that could be used to gain access by surprise in the assault that is being prepared.

The electronic map of the target, and of all approach routes, is acquired: which hostile or friendly radars to warn of the passage of helicopters or air support in a timely manner; which communications and repeaters manage the information from the embassy; the host country is asked to intercept radio and mobile communications in the embassy and its vicinity, as there could be informants complicit with the assailants outside. Using AI, the communications are translated and transcribed in real time, analysed and, if of interest, passed on to the intelligence agencies at various levels so that they can use the information.

[7] OSINT. Open source intelligence.
[8] *Identity Intelligence*. Department and activity that brings together all the biometric identification characteristics of individuals, together with the rest of the features that define that "person", such as their bank accounts, vehicles, network of friends and family, habits, personality or any other related feature.

Thanks to an image acquired by a HUMINT team[9] , from a local undercover collaborating agent who has approached the embassy, photos and videos of several terrorists have been taken and a nose and some ears have been extracted from the masks, ways of walking and picking up weapons which, analysed with AI, have demonstrated the identity of some assailants, belonging to one of the insurgent factions and whose leader is known from a propaganda video; At higher levels, the leader is psychologically profiled and his behavioural possibilities are analysed with AI. The HUMINT team has managed to place unattended micro-robot video cameras with microphones, wifi transmitters-receivers; all sensors are controlled from Spain, and collect the number and position within the embassy of the activists, their communications and routes... and, most importantly: where the hostages are, grouped in various rooms.

The operational team, with the help of architectural software managed by AI, has virtually recreated the facilities, furniture, positions of terrorists and hostages, accesses... information that is updated in real time as it is acquired. The team begins to rehearse the rescue plans with augmented reality equipment and simulated weapons, where the rest of the components and support are incorporated as in a video game. As the test field is replicated in real life, the team has already memorised the facilities and trained all possible incidents on the attack plan, which, once physical, is optimised with AI to reduce times, optimise access locations, weapons used, and, above all, risks for the hostages. The security and speed of the hostages' release is prioritised over that of the intervention team.

CIFAS gathers more information and analyses with its experts and external experts from academia, diplomacy and business and, with the help of its AI tools, makes predictive models of the various scenarios at all levels: political-military, strategic to tactical, and the impact of the various possibilities of action on adversaries, allies and neutrals. AI weights variables, influence of actors, instruments of power of intervening systems, relates them to the whole body of evidence, related intelligence products, predictions, and updates its algorithms to reduce uncertainty and cognitive biases, and presents possibilities for the human component to finally make the final decisions of assessments and recommendations for decision-makers.

[9] HUMINT. Intelligence from human sources.

The government and the crisis cabinet where the Minister of Defence, the JEMAD[10] and other important actors such as the Department of National Security, CNI[11] , the CIFAS, the Army/Navy, MCCD[12] and MOE receive the intelligence update from the CIFAS as to the military option to be taken; finally the MOE sets out the action to be taken and the executive decision is taken.

The operational team has moved and is about to intervene in the vicinity of the embassy in country X, and continues to receive, in real time, thanks to its combat cloud, all the intelligence update, live video from UAVs[13] and satellites, communication jammers update and the updated situation within the target, the AI recognises the patterns of importance and presents to the team only the information of interest; by swarming micro UAVs, robots able to anticipate and recognise uncontrolled areas, identify and relay information to each other and to the cloud and to Spain. Each component of the team receives real-time alerts on their holographic visors fitted to their helmets, while vitals and combat circumstances such as fire directions, images, hostage or terrorist recognition and identification or fire support on specific locations are transmitted from the local combat cloud to the helicopters and fighters on standby to provide support, and will receive hostile fire origins and landing parameters in real time thanks to the various AI algorithms that suggest alternative courses of action in relation to the information received by all sensors.

The hostages are rescued and the kidnappers neutralised and arrested. Part of the team escorts the hostages to their evacuation helicopters, while another part stays at the embassy to collect forensic evidence, photos, DNA, weapons, phones and computers for further analysis; this evidence will be shared with allies and country X, with whom data will be cross-referenced to resolve the involvement of some of the terrorists in other IED attacks[14] . The use of AI has been key to data science to search through thousands of clues and cross-reference them into relational clues to dismantle criminal and terrorist networks in which the deceased were involved.

[10] JEMAD. Chief of Defence Staff.
[11] CNI. National Intelligence Centre.
[12] MCCD. Joint Cyber Defence Command.
[13] UAV, Unmanned Aerial Vehicle. Flying drones.
[14] IED, improvised explosive device.

But the intelligence work does not end there, because it is necessary to assess the impact on social media[15] , media and perception in the society of country X and other countries of interest, along with Spain. Disinformation and hybrid warfare campaigns are detected, aimed at destabilising and benefiting from criticising the successes, maximising the possible errors produced in the operation, victimising and aggrandising the terrorist group as freedom fighters. We work on the detection of the disinformation campaign, its narratives, dissemination networks, detection of bots, procedures and real perpetrators, AI is key to carry out the work in minimum time and contributes to linking hidden links. *Hacking* operations and physical arrests of those responsible for these cyber entities are carried out to find out who is behind them and what intentions they have had or could have in the future.

For all of the above, the MCCD and specialists DOMEX[16] of the MOE, RINT and CIFAS carry out the extraction of information from these computer terminals, for which the encryption codes are broken and their files are analysed remotely to find instigators and clandestine networks in the dark web dedicated to financing with cryptocurrencies, recruitment, propaganda and training of terrorists and organised crime groups related to each other. And with J9/10 Influence[17] and EMACON in its STRATCOM Strategic Communication unit to provide the relevant information to develop the counter campaign of infoxication and disinformation with dynamic measures. Finally, thanks to intelligence work after an operation, future hostile actions against the interests of Spain and its allies are detected and prevented.

An introduction

With this story, similar to a movie script that could well be real, we have reviewed in a general way the current major multiplier effects of AI in a military hostage rescue operation, perhaps one of the most difficult; and the intersections with intelligence as a discipline, responsible for the success of the operations.

[15] RRSS, Social networks.
[16] DOMEX. Extraction of data and information from documentation and captured computer/electronic media.
[17] Staff Sections J9 Information and J10 Influence.

Indeed, the growing importance of intelligence in crises of all kinds is unquestionable since the *Intelligence leads operations* paradigm became popular[18] , an overwhelming trend with the counterinsurgency doctrine (Kilcullen, 2010) after the second Gulf War and a reflection of the importance of intelligence in 'surgical' operations such as special operations and police security forces, with its *Intelligence Lead Policy* (ILP), in which the detail and verifiability of intelligence conditions and authorises all operations[19] (Burcher and Whelan, 2018), all with final legal oversight after the intelligence gathering process.

If there is one thing that characterises these surgical operations, it is the enormous need for information and intelligence, its processing and analysis. With the advent of AI, we are able to take in more, with less effort, in a better way, fewer people and faster.

The use of AI to solve intelligence problems is related to technological developments and the revolution in technology, especially in the first quarter of the 21st century. In other chapters of this work, the recent history of AI is presented, but let us remember that the development of computers and the first complex algorithms were born from the needs of war during the Second World War, in particular, from military intelligence in deciphering the messages coded by the analogue and mechanical tool Enigma; thanks to which and to the interception of communications, what we call SIGINT[20] , the allies gained a strategic advantage, which favoured their victory. Today, the foresight of AI in support of military operations as a whole, and Intelligence in particular, is on Ukraine, which is specifically analysed in another section of this paper.

AI at the heart of today's strategic competition

Since the Second World War, the US has been at the forefront of military innovation and, in particular, AI could not remain aloof from it, although the global security environment places the strategic competition between the US and China. We can consider that Russia would become more of an ally of the new pretender to "hegemony" in the global

[18] "Intelligence leads operations". The translation can be misleading, as the verb lead means according to the Cambridge dictionary: to direct, lead, lead, lead, lead, lead, lead, ... Its meaning inverts the paradigm of the bureaucratised armed forces of peace, accustomed to all-paper exercises, who have not participated in war situations of maximum effort and casualties; in the latter, Operations lead and justify all the other facets of the organisational functions of the General Staff, including Intelligence.
[19] *Intelligence-led policing* (ILP). A model for police state security forces that seeks to place crime intelligence at the forefront of decisions or operations. Concept used in Anglo-Saxon countries.
[20] SIGINT. Signals intelligence, divided into those relating to COMINT communications and ELINT electronic signatures.

geopolitical balance, even if it maintains the strategic weight that nuclear power gives it and not so much conventional military and technological development power, as is being seen in its aggression against Ukraine.

China, at the economic level, is already at a level of equilibrium, which allows it to move on to the last phase in its strategy enunciated by Pillsbury of the "100-year marathon": military supremacy; and this will be based on finding its *Assessin's Mace*, the ultimate weapon of its ancestral imaginary, which will give it success against its most powerful enemies (Pillsbury, 2016). These weapons, strategies (Aranda, 2023) or disruptive technologies with which China intends to outmanoeuvre the US, the current hegemon, and its allies are intended to prevent the US and its allies from surrounding it, as in the wo[21] , and strangling China's economy and strategic output with their naval and space superiority.

To this end, in the quest for the ultimate weapon, they are creating a number of weapon systems that are heavily AI-loaded in their development, design and C4I[22] . Examples include submarines, hypersonic weapons, anti-satellite missiles, cyber weapons and interception assets, *hacking* and everything related to cognitive warfare . All of these were introduced by Chinese conceptual work (Liang and Xiangsui, 1999), which probably inspired Al Qaida and the rest of the asymmetric strategies we now call grey zone or hybrid warfare[23] (Pillsbury, 2016).

But, for China's technological dominance, one of the fundamental axes has been the development of its copying and technology theft capabilities using its significant espionage capabilities, that is intelligence (Pérez, 2023), with both human and technological infiltration, with the widespread use of cyber capabilities to even access personal information of a large part of the US population (Clarín, 2020).

The common nexus interlinking all these needs and capabilities is the development of AI, which is presumed to be the true cement of its intended future global supremacy, helping

[21] Wo, an ancestral Chinese game, preferred to chess, in which the opponent's surrounded stones are eliminated; one has to surround without being surrounded. In Chinese education "The 36 stratagems" (Aranda, A. 2023) and the ancestral stories of the struggles of the warring Chinese kingdoms before unification are the basis of the mental and cultural structure.
[22] C4I. Command, Control, Communications, Computers and Intelligence.
[23] The strategy of unrestricted war was first embraced by al-Qaida, according to multiple analysts, as examples of actions described in this essay were carried out very soon after its publication, such as the attack on the Twin Towers on 9/11, or attacks in Africa, as well as records of Chinese advisors in the Taliban's Afghanistan, and predate Gerasimov's famous formulation of hybrid warfare.

it to develop its *Assessin's Mace*, along with deep knowledge and influence in global governance systems, with superior strategic foresight and knowledge through intelligence and its management by AI, which it intends to lead by 2030 (Knight, 2017).

But before we continue, let us clarify a few terms.

Basic concepts: types of AI and intelligence

We understand AI as the process carried out by a machine that can analyse, organise and convert information into knowledge (Jiménez, 2021). These AIs use programs, which are a representation of an algorithm in a programming language that can be interpreted and executed by a computer. And algorithms are the description of the method by which a task is performed; a sequence of instructions that, when executed correctly, lead to the desired result. Algorithm designs are based on mathematical processes that can be transferred to a computer, so they are computable and included in the theory of computability (Abellanas and Lodares, 1990).

Types of AI

The types of AI fields, without going in depth, are recalled in the following AI branches, referring to the development of the application of the subject or the field of AI research.

These fields of AI research are diverse (Russell and Norvig, 2004) in reference to the Turing *test* in:

- *Machine Learning* (ML). They make future decisions using past experience.
- Natural Language Processing (NLP).
- Expert systems. They would provide a solution to a given problem.
- Artificial vision.
- Fuzzy logic. Creating mathematical approximations for problem solving produces exact results using imprecise information.
- Intelligent agents. Using their own knowledge, adjusting to changes in the environment, they are able to perform operations that satisfy a user's request.

- *Deep Learning*. Artificial Neural Networks.
- Robotics.
- Genetic algorithms. These are those inspired by the processes of genetic evolution and the survival of the solutions best adapted to the environment.

All these fields of AI are of diverse application to intelligence activities, as will be developed below.

Types of intelligence

The advances that have been made in recent years in the fields of AI are extraordinary and are increasingly being applied to intelligence. In an immediate way in what we call current intelligence[24] , thanks to the speed and automatism of its processes, which make it possible to approximate to real time the time that elapses from the capture of information by the sensor to the use of this information thanks to the also autonomous mechanisms in the processing and preparation of data to transform them into intelligence.

But for this final transformation of intelligence, a compilation of current information with pre-existing information in the form of basic intelligence is required. Until very recently, the use of some AI was implemented in database management and storage processes. With the advent of AI and specific techniques such as *Machine, Deep Learning*, and natural language processing (NLP), it is possible to make intensive use of advanced statistical processes in any database, which allow us to take advantage of the stored data.

Before the advent of AI, the massive use of data and the computational mechanisation of arduous and highly demanding tasks in terms of precision was limited; optimal work for robots. To the above, we can add, in the last year or so, the emergence of LLMs[25] or large natural language models such as ChatGPT and their global conceptual and technical revolution, which many have compared to the invention of the wheel or the internet (Leonhard, 2023), and, of course, also in the field of intelligence as a generic activity.

[24] Current intelligence. That of the moment, closely linked to timeframes of less than 24 hours, and of course, that of time close to real time, thanks to sensorisation and AI intervention in JISR processes.
[25] LLM. *Large Language Models*. Inspired by the revolutionary developments of Open AI (ChatGPT) and the other technological giants in their respective developments, which are not yet so advanced.

We will analyse the current situation and future developments, from the perspective of intelligence, its phases and disciplines, and how AI intervenes or may affect them.

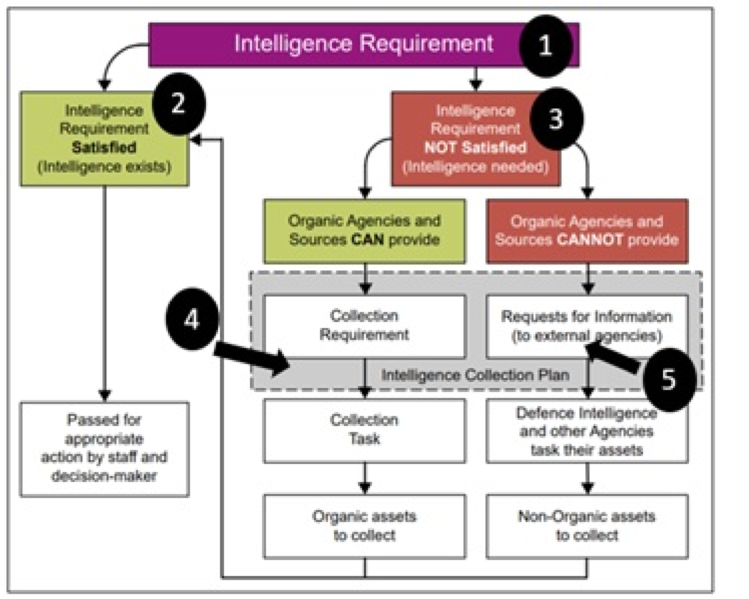
AI in the intelligence cycle

Let us now review the general processes of intelligence, in which the omnipresent intelligence cycle stands out, but of the various types that exist, we will take the NATO and Spanish doctrine as a reference: direction, collection, analysis and dissemination.

Address

This phase of intelligence processes has traditionally been the most reluctant to the robotic intervention of AI in the volitional decision-making aspects of bosses. But the situation is changing with the emergence of AI fields such as "Approximate Reasoning", the automation of processes that were already mechanical in their human execution, such as many of those under the conceptual umbrella of JISR[26] (Scott and Michell, 2022) and its sub-processes of IRM[27] , intelligence needs management and CM, management of the means of procurement. An interesting new AI-heavy contribution is the focus on intelligence, information, cyber, electronic warfare and space capabilities, I2CEWS[28] (Borne, 2019).

[26] JISR. *Joint Intelligence, Surveillance and Reconnaissance*. Joint Intelligence, Surveillance and Reconnaissance (any domain).
[27] IRM. *Intelligence Requirement Management.*
CM, *Collection Managements.*
[28] I2CEWS. New concept being implemented in the USA. *Intelligence, Information, Cyberspace, Electronic Warfare, and Space*



In these IRM processes, the requirements and information necessary for the production of an intelligence product are compared and the AI can autonomously collate which ones are already in the basic intelligence databases and, for those that are not, pass them on to the next doctrinal structure, the CM procurement management, where the information needs are divided and prepared for the elaboration of orders of procurement to the sensors and units themselves or, failing that, to request this information through information requests to the units or entities of equal or higher level, with the RFIs[29] , according to the table attached and order of processes from one to five.

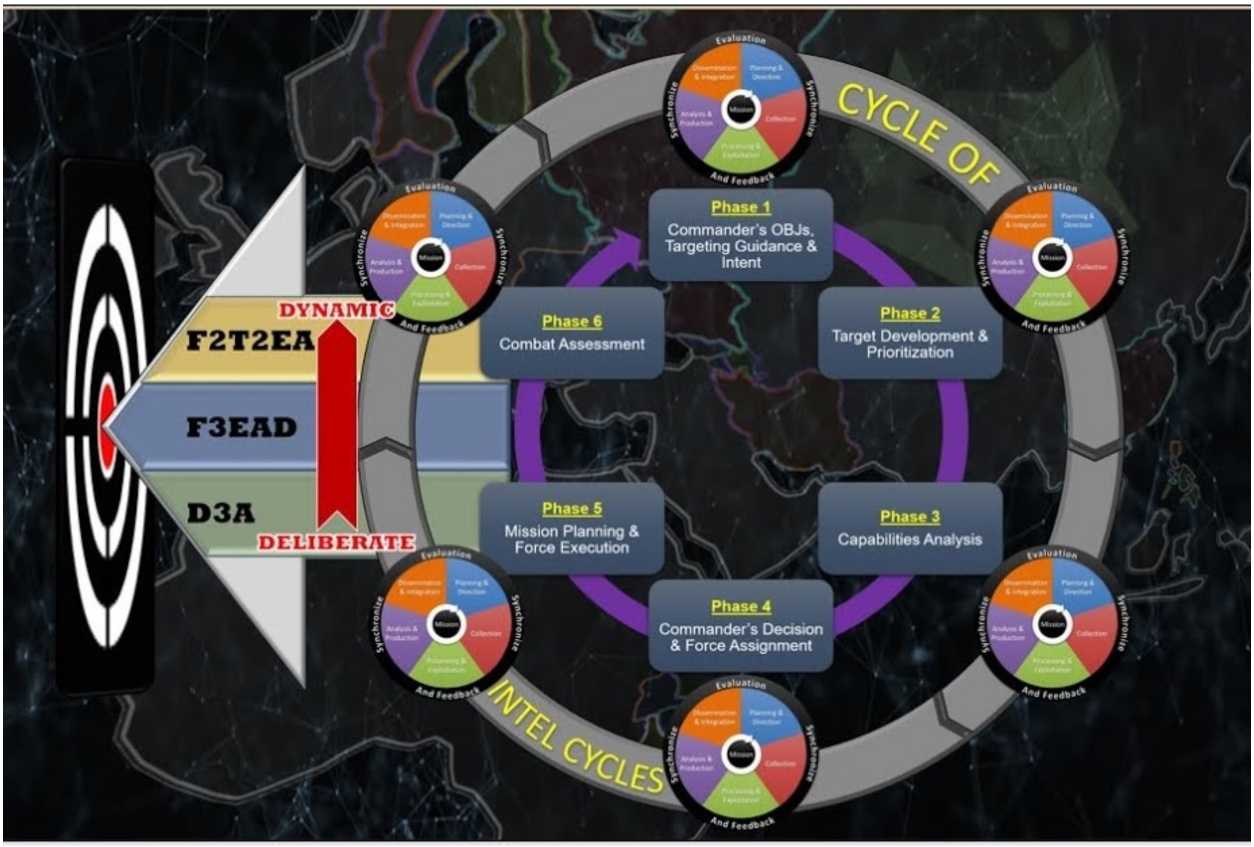
Automated AI assignment of missions to sensors can increasingly be done in near-real time and *dynamic re-tasking* (Saling, 1999) of the means of procurement, that is, the reassignment of missions once they are launched into execution, is becoming simpler and is rethinking mission request and planning timelines. Concurrently, the extensive occupation and sensorisation of the non-continuous battlefield means that dynamic mission re-tasking is no longer exceptional, thanks to the intervention of AI in the administrative and operational management necessary to vary orders, air routes, standardised announced overflights and management of air-ground and maritime battlespaces.

AI increases security in these dynamic reallocations to avoid conflicts or collisions. Algorithms that bypass human failures and increase the necessary speed of information

[29] RFI. *Request for Information.* Request for information, with a specific, standardised format for circulation and common use in all Western armies and services. See bibliography for UN presentation.

transfer and calculations of complementary shared interest between different platforms/sensors or organisations; all these decisions and management require automation to reduce the time of all processes to times that are unmanageable.

Lead times are minimised by the AI to request and plan missions to enter the ATO[30] on a given day. These planning cycles are dynamised and accelerated, and must be imposed on those of the adversary, as they are important for the coordination of the rest of the cycles such as *targeting* (ATP 3-60) and JISR, and for the prioritisation of missions, the allocation of sensors and means for each procurement. These processes can also be automated with AI.



Indeed, the model of asset and mission allocation in the fields of intelligence and operations framed by modern *targeting* (Kyle, 1999) involves AI automation for TSTs[31] , those targets of opportunity typically developed in counter-terrorist or counter-insurgent operations, as exceptions in long lists of targets, and which stopped all plans in their

[30] ATO, *Air Tasking Order.* The publication of air missions with their routes, schedules and airspace occupancy.
[31] TST, *Time Sensitive Targets*. Targets of opportunity of paramount importance.

tracks to redirect them to that all-important target to be hit as soon as possible whenever it was located.

Other fields of AI use can be applied to this phase, making it easier for there to be no such distinction of phases, it is all fluid with the merit of the speed and reliability of AI allowing us to blur when we are in one phase or the other.

In this way, a combination of the various Information Needs, NI, can be interconnected simultaneously or sequentially, complementing and feeding back in near-real time as conditions develop and developing new NI, and adaptations of the commander's Critical Commander Information Needs, CCIR, can be made more dynamic as intelligence, *targeting* (US Joint *Targeting School Guide,* 2017) and operations cycles are synchronised: intelligence, *targeting, control and communications (*C4ISR) cycles are also accelerated by AI to collapse adversary cycles, and the C4ISR, decision, intelligence, control and communications (C4ISR) cycles are also accelerated by AI to collapse adversary cycles. US Joint Targeting School Guide, 2017) and operations: decision, intelligence, control and communications cycles, C4ISR, are also accelerated by AI to collapse adversary cycles.

What specific fields of AI are applicable to this diverse set of activities? Among others, algorithms adapted to solve complex, sequential decision problems[32] , whether partially observable or not[33] ; also dynamic decision networks to adapt their knowledge states as new information is received to complete the perception of reality, to ultimately infer possible future actions; and finally also concepts adapted from game theory[34] , among others.

The specific intelligence needs[35] (SIR), the essential elements of information (EEI) and even the commander's critical information needs (CCIR) are broken down into variables and search algorithms from which the priority intelligence needs (PIR) are specified in

---

[32] Richard Bellman, working at the RAND Corporation, developed the concept in 1949. *Dynamic Programming* (1957) for solving infinite horizon problems. Sequential decision problems in uncertain environments, called, in English, by the acronym MDP, *Markov Decision Processes*, a process that specifies the probabilistic outcomes of actions and the reward function that scores it for each case.
[33] POMDP. Acronym for *Partial Observable* MDP, Partially *Observable* Sequential Decision Problems.
[34] Game theory seeks a Nash equilibrium in which there is no incentive for decisions that deviate from a human-defined strategy, and thus transformable into a human-controlled algorithm.
[35] SIR, *Special Intelligence Requirements;* EEI, *Essential Elements of Information*; CCIR, *Commander Critical Information Requirements*; PIR, *Priority Intelligence Requirements*; KPI, *Key Performance Indicator*.

scenario indicators; all are indicators (KPIs) of various levels of detail that can be related as qualitative variables transformable into quantitative and actionable with AI.

Ultimately, intelligence warning systems need mechanisation to monitor changes in conditions in real time and, with decision support systems (DSS), reduce the reaction times of human decision-makers. These processes apply to any civil or emergency response activity, with NATO nomenclature depending on the functions involved (Delgado, 2020).

In this sense, the Spanish Armed Forces are implementing an integral system, the National Command and Control System, SC2N, (Ruiz, 2023) within which there is a subsystem dedicated to intelligence work, where the activities of the intelligence cycle are integrated and interrelated with the rest of the systems such as *targeting* or operations, among others.

Procurement

In this phase, the sources, human or technical sensors, are exploited and, therefore, intervened to a greater or lesser extent with AI, all means of collection. We also have in this phase the mechanisms for the delivery of the information obtained to the analysis bodies of the next phase of the intelligence cycle, but including a first eminently technical analysis of the collecting body itself.

These sensors we are talking about are the JISR means, for the most part, which in NATO doctrine has become so important as to underpin specific processes and integration with command and control, communications, known as JC4ISR, which is the backbone of this massive sensorisation of the battlefield, and which requires management in which AI goes from simple assistance to being an essential protagonist in this autonomous *big data.*

Conceptual creations of the future 5G and 6G communications combat cloud are causing major companies such as Telefónica and GMV to explore solutions to export the technological world of always-on connectivity to remote areas or areas denied by hostile action and take advantage of technological superiority in future conflicts.

Here we will divide this capture of unprocessed information into the main (but not all) disciplines, fields and techniques of intelligence exploitation that allow us to divide the facets into which reality can be dissected for better assimilation.

OSINT. Open source intelligence

We start with the discipline that has grown the most in its relationship with AI thanks to digitalisation with the internet in almost all human activities.

As Alvin Toffler advanced in some of his prescient books of the nineties of the last century, including *The Shift of Power* and *The Wars of the Future*, digitalisation would allow the transition from a second wave society[36] to a third wave society in which knowledge, and by extension intelligence, are the keys to success and categorisation as advanced societies. In these, the added value is given by the quality of the population, fundamentally with access to advanced education in order to transform society itself through technology. Let us say that this last reflection fits in very well with the transformative effect of AI in our current society, which some theorists already classify as the 4th Industrial Revolution (Pérez and Sánchez, 2019)

The current importance of OSINT comes from the global use of open sources, *Open Source*, and the democratisation of technology that many early AI theorists advocated. We can say that in the toolbox of an OSINT analyst, those with an open access character are preponderant.

Virtually no intelligence service is able to compete with *Open Source* worldwide, where individuals not affiliated to any organisation and united by a tribal sense of belonging to this world of sharing move forward without restrictions. In it, the challenges, the transfer of innovation and solutions between the community of interest and even the sharing of code between the OSINT community means that in a matter of months the tools that were a feasible solution become obsolete or are blocked by their developers in order to monetise them, but are immediately replaced by others with the same initial character, let's call them *Open Source*.

The technological union of the capabilities and needs of the cyber world and the OSINT world is a fact, and OSINT analysts or teams integrate the skills of computer engineers and developers, as well as diverse profiles of data scientists and statisticians. The need

[36] Toffler's wave theory of the development of societies. Wave 1 with the agrarian revolution, wave 2 with the industrial revolution and the current wave 3 in which globalisation and the change to knowledge societies with the irruption of information technologies.

for specific code and ethical *hacking* brings together worlds that until recently were distant. Intelligence analysts, already specialised in security, political science and international relations, but with the addition of in-depth computer and cyber security expertise, are increasingly in demand. With such professionals, the leap to the use of AI, whether proprietary or customised, boosts OSINT capabilities to levels of technical self-sufficiency and of paramount importance to intelligence services.

This fact is confirmed by the increased importance of a discipline that claims its key role for the rest, not only to provide the knowledge base for other disciplines such as HUMINT, IMINT or SIGINT, but also as the source of the unique knowledge on most intelligence needs, either because it is able to collect the available set of information on them, or because no other disciplines have access to the niche where the available information is located.

Single discipline reports, OSINTREPs, are no longer considered a minor report, without distinction or added value compared to the other, non-OSINT disciplines, which are usually exclusive to military and state service capabilities, who can afford the expensive means and sensors that support them, such as satellites, drones or SIGINT pods, or the possibility of recruiting and training HUMINT agents, the James Bonds of our collective cinematic imagination.

Journalistic researchers, or the OSINT world, make extensive use of occasional informants who post their videos and photos, their evaluations or comments on the various social networks. These social networks are located in the deep web, the *deep web*, where information is not indexed, searched or catalogued by search engines such as Google or Yahoo: the *surface web*, which exploits only 4-8% of all the information circulating on the internet. The immediacy that makes it possible to have improvised witnesses wherever the news or important event takes place, transcends worldwide thanks to the possibility of sharing that experience globally. The fact that there are commercial platforms such as those of companies like Dataminr that have come to exploit these capabilities with the intensive use of AI to extract information, verify its veracity, contrast it with other available sources, and all in close to real time, is enabling the emergence of private companies in the use of these knowledge technologies at the service, previously exclusive, of large corporations and states.

The fact that these tools developed by companies specialising in OSINT intelligence can be adapted to the needs and preferences of each user makes them very attractive for other companies in which the use of information is vital for their business in fields as diverse as risk analysis, strategic planning of activity, marketing, or the impact of the social, cognitive or political situation on their business activities in certain geographical areas or globally.

The current technological revolution means that capabilities that were previously only within the reach of official entities and powerful companies are extending with economic intelligence and the irruption of intelligence needs in companies for early warning, risk assessment of their investments in compromised locations and the security of their personnel. OSINT is the discipline that has spread and is within the reach of any company, either organically and permanently, or as an external service with security and intelligence consultancy. We are dealing with dual-use technologies: civilian and military (Toffler, 2001).

Portals such as *Github, Google Colab* or other sharing or collaboration portals mean that this transfer of code in different languages minimises the efforts to develop singular and unique solutions adapted to the needs not only of the organisations, but also of the analyst teams. Their capabilities in OSINT are multiplied by the implementation of *ad hoc* AI solutions to solve very specific problems.

Effective uses of OSINT are becoming increasingly conclusive and interesting, and the war in Ukraine is becoming a global view of the rise of the discipline. The added value of its democratisation and the possibilities afforded by the widespread access of the population with its applications on *smartphones* and phones to social networks through which photos, videos and direct comments are disseminated, turns simple citizen spectators into improvised agents or first-rate witnesses, bordering on "cyber HUMINT".

HUMINT. Human intelligence

It is the intelligence of information collected by human operators from the physical and human environment, from human sources.

We might think that these are activities outside the scope of AI, but these human operators have limitations, prejudices and cognitive biases (Heuer, 1999), they do not control all the theatre languages in which they can be deployed, and when it comes to interviews or interrogations, AI assistance will allow the interpretation of dialects, non-verbal language, lie detection, among other needs, all in real time.

One of its tasks is reconnaissance missions, which can be done in the old-fashioned way with binoculars or a camera and noting incidents, vehicles, people, etc., or by expanding the uses of AI with cloud-linked cameras with recognition and detection algorithms, as in a closed-circuit television (CCTV) system. or by expanding the uses of AI with cloud-linked cameras with recognition and detection algorithms as if it were a closed-circuit television (CCTV), but being able to expand the capabilities of visible images to infrared or thermal images, automated recognition of actors or vehicles, or by implementing new technologies to interpret wifi signals at the target, near the target or by the equipment itself using RGB cameras, LiDAR, and portable or non-portable radars to detect movements and people behind walls (Newcomb, 2023) and in which DensePose algorithms are used .[37]

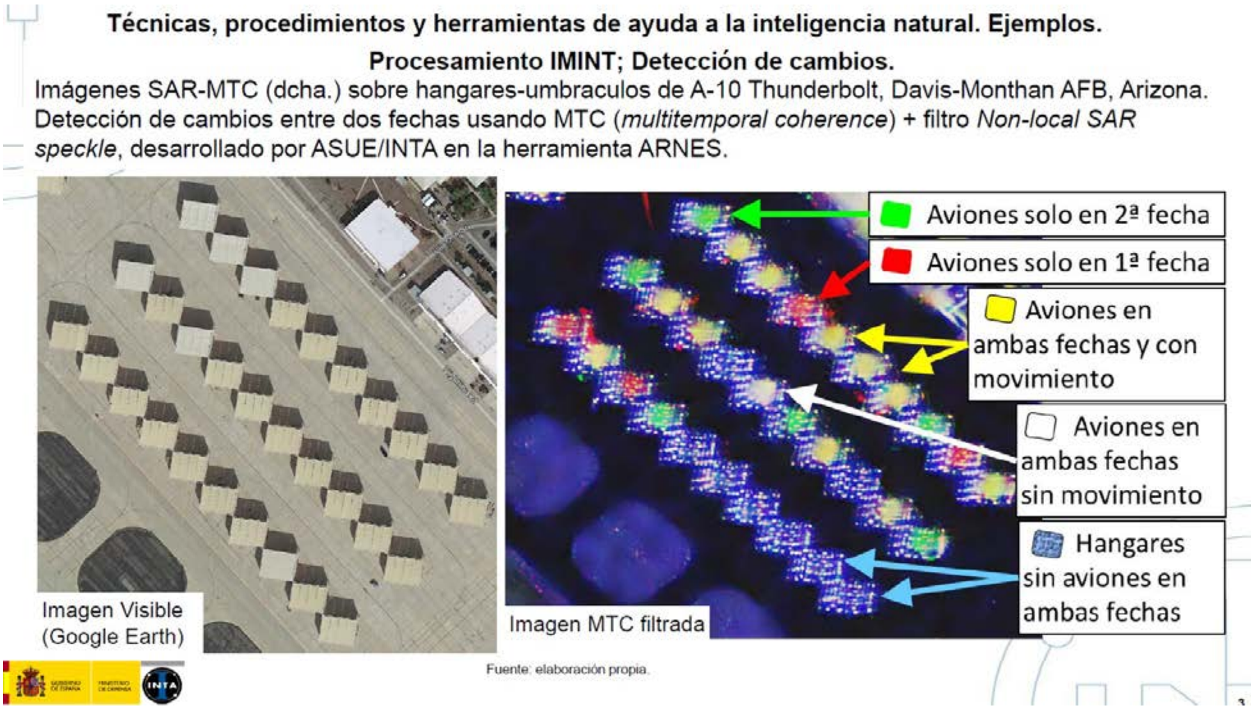
IMINT. Image Intelligence (De la Fuente *et al.,* 2022)

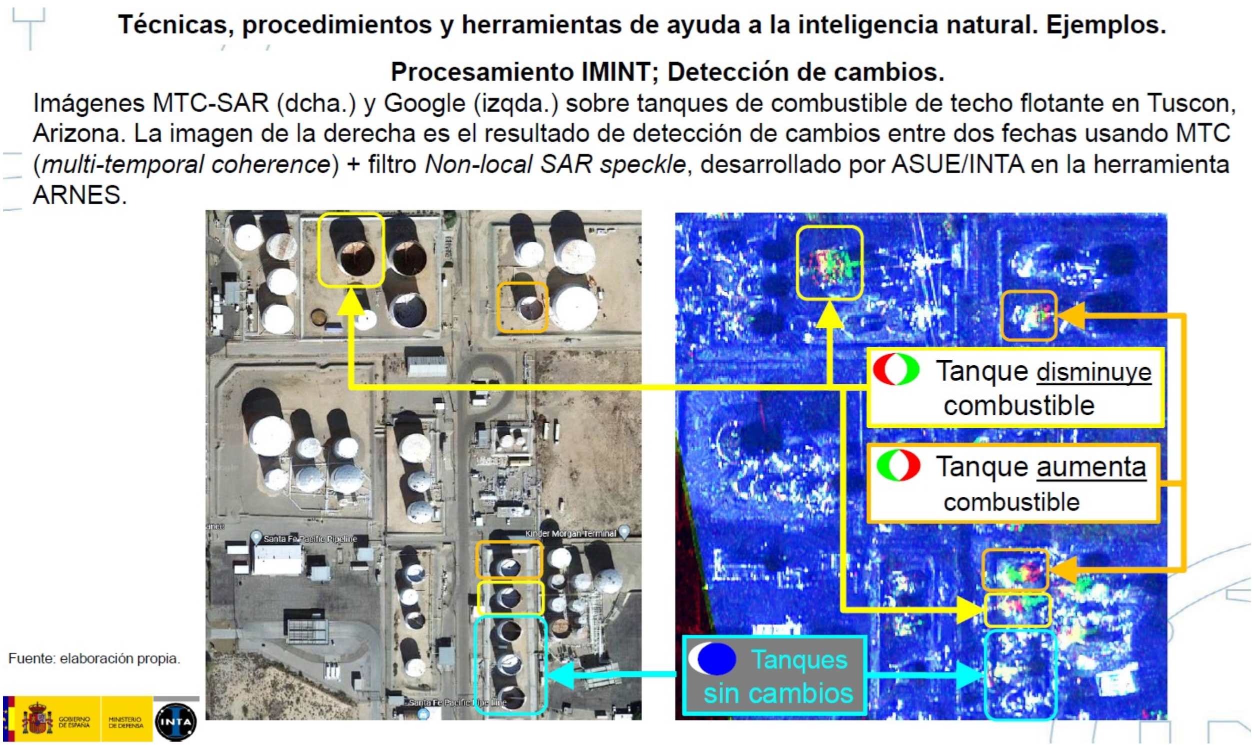
It is the intelligence derived from the acquisition of imagery from different sensors and platforms, whether ground-based, air-based or space-based. The acquisition of such imagery can be in the visible spectrum, infrared, multispectral, electromagnetic radiation detection or radar imagery.

The specific field of AI (Lauroba, 2021) dealing with imagery is developing extensively with image datasets from various platforms and shooting angles to detect for example those exposed by INTA :[38]

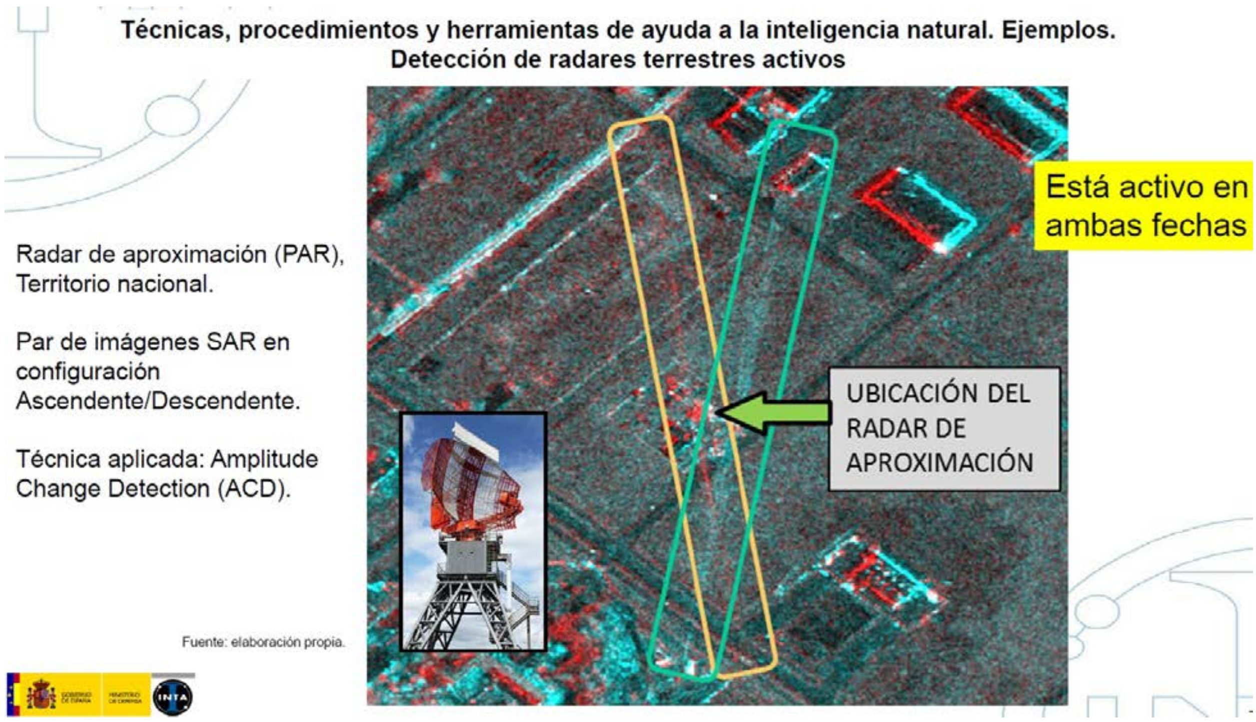
– Change detection

[37] Available at: densepose.org
It is part of the COCO and Mapillary Joint Recognition Challenge Workshop at ICCV 2019.
[38] INTA. National Institute for Aerospace Technology.

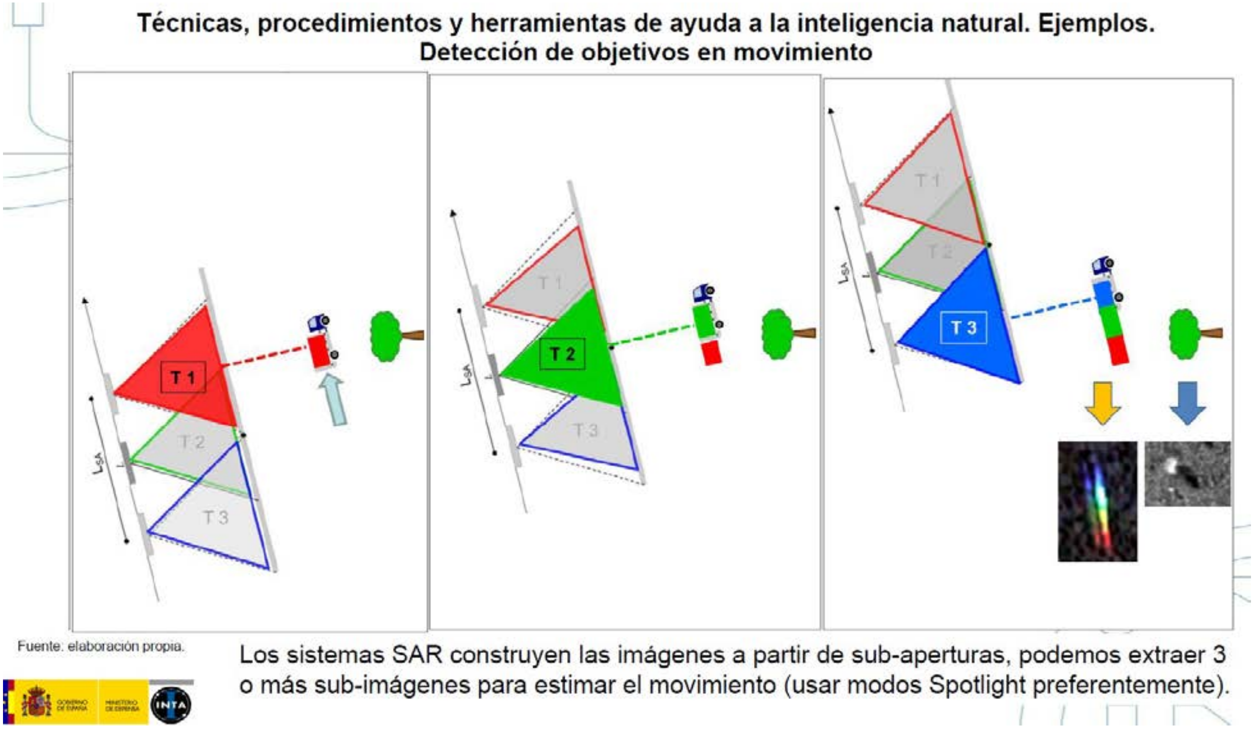




– Active radar detection



– Motion detection



And, of course, all the object recognition using datasets and fundamentally various *Deep Learning* techniques with combolutional neural networks, with all kinds of constructions, aircraft, etc.

Computer vision or artificial vision is in full development, being able to understand its environment, contributing to the autonomy of the systems and applicable to all types of drones and is the link between the classic IMINT discipline, which was limited to aerial images, to being able to integrate those of any terrestrial and maritime sensor as well, with which the battlefield wrapped in the cloud[39] of combat, thanks to the computing at the edge[40] and in the fog . [41]

Image processing incorporates powerful graphics cards that provide computing power for electro-optical and infrared imagery, with *software* defined radio (SDR) and PNT modules for position, navigation and timing, enabling sensors and systems to communicate and interact with each other to ensure unique references with the NATO vetronics standard.

[39] Computer services on the network, internet or other proprietary network.
[40] A distributed computing strategy that brings computation and data storage closer to the location where data is collected and computation is needed, to reduce latency and the required communications bandwidth.
[41] Decentralised computing infrastructure where computers, data and applications are located between the data source and the cloud.

This will enable the interaction of intelligence systems with FCAS, the Future Combat Air System, and drone swarms as fundamental to future battlefields.

The development of space systems is leading to an increase in ISR functions and their importance for all domains and autonomous systems, using new constellations of microsatellites.

Intermediate Earth Orbit (MEO) satellites and space platforms and Low Earth Orbit (LEO) space sensors with higher signal strength and security that will improve positioning systems such as GPS, Galileo or GNSS[42] and also through inertial sensors, odometers, cameras, gyroscopes. All these improvements involve on-board computing and AI to fuse data with data pre-processing, reducing base communication data, and autonomy in navigation processes and overcoming failures; but with major limitations of space and energy requirements, until quantum computers arrive.

Possible robot or drone monitoring, through virtual, augmented or extended reality, will enable the human-machine interaction that will be the key to the presentation of immediately actionable information and intelligence at all levels to all warfighters, whatever their role: command, advisory, executive.

SIGINT. Signal intelligence

It is the intelligence obtained from electromagnetic emissions. Its field of action is divided into two:

- Communications Intelligence (COMINT), when voice transmitted by any electromagnetic means is involved.
- Electronic Intelligence (ELINT), specific to electromagnetic emissions that do not belong to the above.

The possibilities provided by AI to analyse, remove distortions, and compare such signals, whatever the type, coupled with network analysis of actors and relationships augments the successes already achieved in counter-insurgency and counter-terrorist missions, such as in Iraq against Al Qaida. Currently, in Ukraine, there has been a combined use of such location, cyber jacking, ISR extraction of mobile content, contacts, multimedia and

[42] GNSS: *Global Navigation Satellite System.*

the management of information to psychological operations units, intelligence and SIGINT, artillery and planners. This information has allowed the development of a TTP by Russia with the preparation of offensive operations on previously demoralised and preoccupied units by mass deception of their fighters, their families/friends, news and photos manipulated to achieve effect and disquiet just prior to the traditional conventional attack.

This example above denotes the fact of the trend in the convergence of cyber defence and electronic warfare in what they call cyber-electromagnetics (Porche *et al.,* 2013).

In Spain, cyber defence depends on the MCCD[43] in all its aspects, offensive, defensive and electronic systems reconnaissance, however, the intentions of actors and their prospective in conjunction with the rest of the intelligence disciplines resides in the bodies of the intelligence system, if they are threats from entities designated as such at the highest level: the JEMAD.

On the other hand, electronic warfare (EW) in terms of SIGINT intelligence activity in its two subdivisions has a maximum responsibility in the national intelligence bodies at the various levels with the apex in CIFAS, but the offensive and defensive action part of countermeasures, etc. depends on the operational commands themselves and the EW units with their specialised vehicles, drones and antennae which will need further AI processes for their automatic protection either from cyber attacks, measures or electronic countermeasures like chafs etc. against missile or anti-radiation weapon attacks. Also changing disruptive signals adapted to threats in an automated way with AI.

The successive presence of AI together with network and graph analysis systems, entities, actions, etc. implies the discovery and effective interconnection of massive amounts of data, characteristic electromagnetic traces, telephone numbers, repeaters, etc.

ACINT. Acoustic intelligence

This describes the intelligence obtained from emitted acoustic signals, which is always associated with movement. The use of this acquisition discipline requires: great

[43] MCCD. Joint Cyber Defence Command.

technological advances, such as the latest generation of sonar; sophisticated AI algorithms for processing and analysing the acquired signals, updating the corresponding databases with the relevant classification of what is found; and, finally, a high level of qualification and training of the acoustic operators.

MASINT. Measurement and signature intelligence

It is derived from technical analysis of the information obtained by detection instruments and finally associated with various emitting sources. All the intelligence obtained refers to comparisons with those available in a DB with known technical information.

Elaboration

In general, supervised ML learning, with its regression algorithms, producing numerical measurable values, and classification algorithms, in which labels are obtained from a finite set of possible outcomes, alternatives can be chosen when they are defined; thus, uncertainties can be assessed and quantified. In addition, predictions can be made when the probabilities of the effects, given the causes, are known, or conversely, the probability of the causes given the effects (algorithms based on Bayes' theory), simulating conditions of uncertainty and counterfactuals when it is not known whether the stated hypothesis is true or false.

On the other hand, it is in the elaboration phase, and in all its sub-processes, where the clustering and dimensionality reduction algorithms of unsupervised ML learning have their place, dealing with chaos and finding patterns in large databases with all kinds of information.

In this phase, the information obtained is transformed into intelligence with the following sub-processes which, with new technologies, do not necessarily have to be sequential:

Compilation

From the information obtained. If when we talked about OSINT we already considered AI as a solution for "infosication", the intoxication caused by producing and acquiring more data than we were able to assimilate, at this stage we replicate the solutions we talked about and with the use of AI, we add all the necessary information regarding an event, person, place, investigation or object, in the computer sense of the term, which can give a global and integrating sense of what is perceived in reality by our various sensors.

Evaluation

Information and its sources. This stage is increasingly carried out by each procurement discipline if it has the entity and capacity to do so, and is part of the first single discipline analysis by specialists and technicians who are in direct contact with reality. Here, taking into account previous assessments of sources can be the subject of dedicated research for the other disciplines, such as, for example, the categorisation of a HUMINT source, gathering information by SIGINT and OSINT to verify its veracity, the value of the information to which it has access, its personal nature or its security vulnerabilities as an infiltrated or double agent. For all of this, having extensive, well-categorised data from the various sources, thanks to AI with deep reinforcement techniques, can verify the veracity over time of the information received. So again we are talking about *big data* and data management for this purpose. The information extracted from our databases gives us the competitive advantage and the importance of nurturing the basic intelligence of the organisation.

Analysis of the information

In all phases of the intelligence cycle we have analysts in their various functions and degrees of specialisation, but it is in this part of the cycle that more refined analytical skills are required. The analyst's job is to find cause and effect relationships between different facts, circumstances, actors and situations, in order to gain situational awareness and to be able to make predictions for the future (Heuer, 1999). And in all processes involving humans, with their previous experience, errors occur due to simplified strategies used by people's minds to process information, which are referred to as cognitive biases (Heuer, 1999).

We could talk a few years ago, when the buzzword in these types of technology was *big data*, that intelligence processes rarely incorporated AI into the reasoning and structured analysis processes that have become so pervasive in intelligence services since the Iraq war.

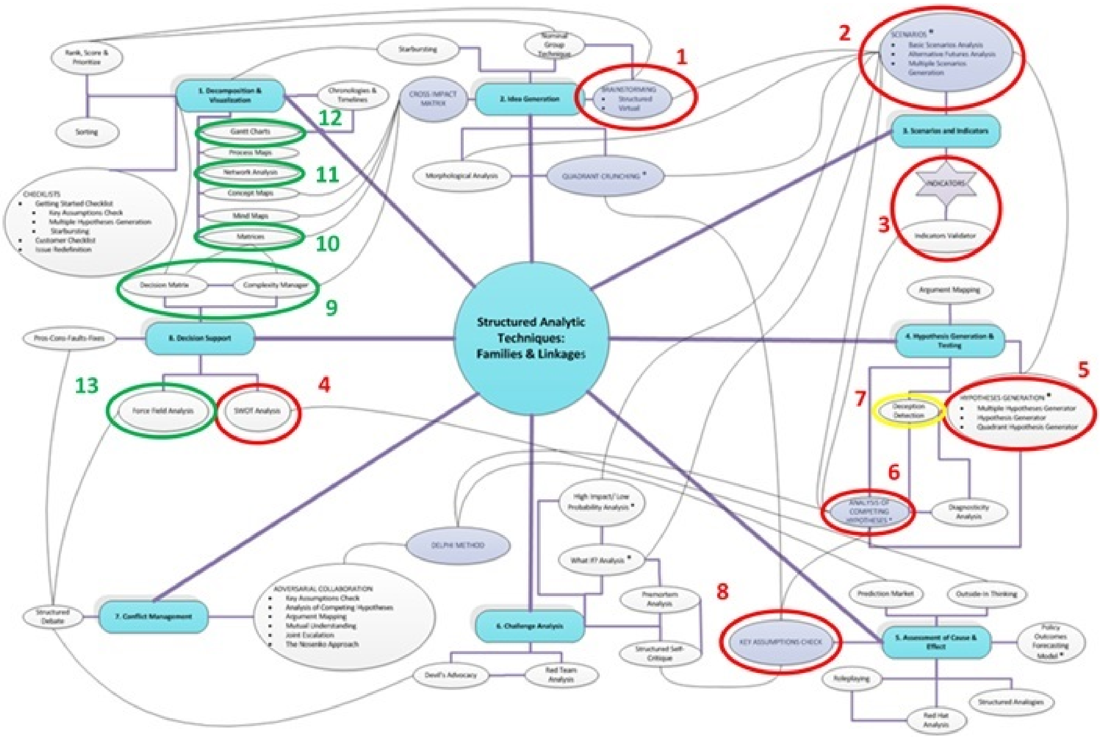
These structured techniques allow the reduction of biases and the implementation of modular and perfectible scientific thought processes and analyses by teams of analysts, using their rational and logical capacities and their knowledge of reality as experts in an area, activity or actor. All of this structured analysis provides added value in terms of foresight as a final product.

The emergence of statistics as a field in the social and political sciences has been key to bringing scientific and mathematical reasoning to spheres previously colonised by intuition: that sense of smell that came from the experience of those specialised intelligence advisors.

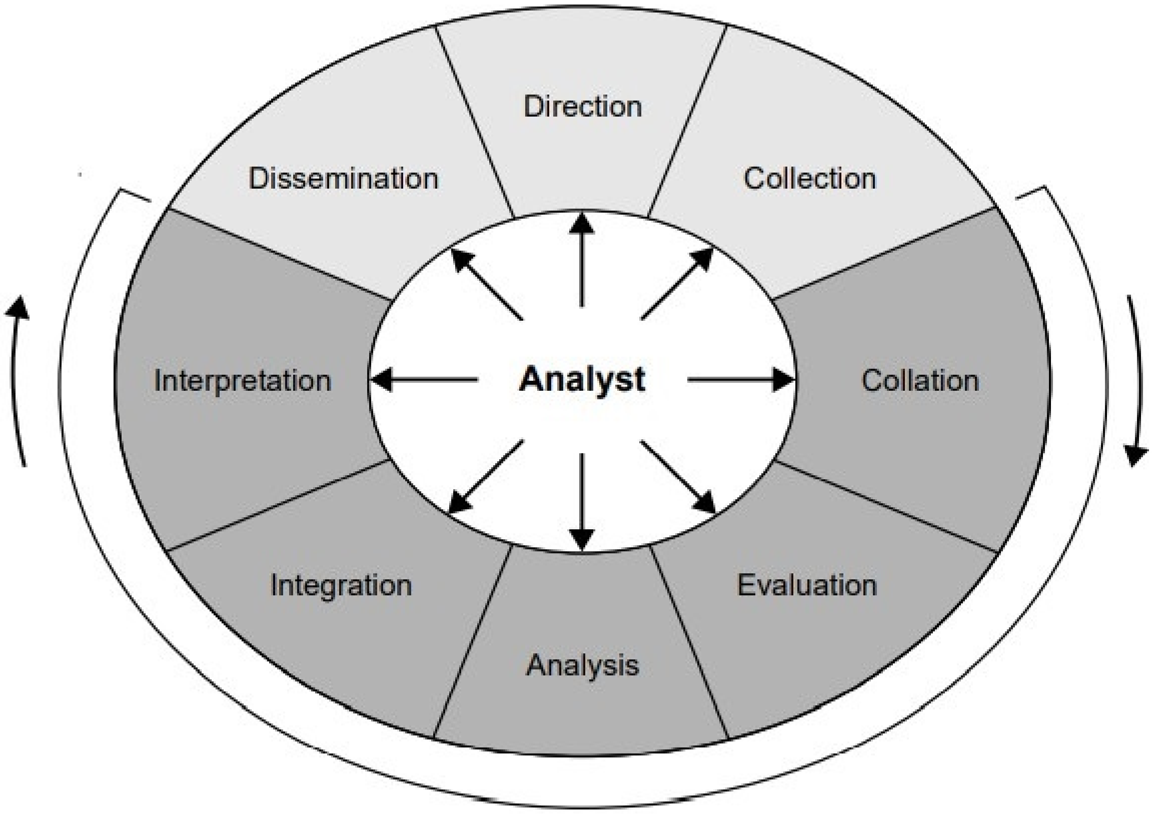
The use of AI is making it possible to go beyond purely statistical techniques and thanks to M/DL to take advantage of large amounts of existing data or data that can be acquired by sensing the world and the battlefield to use the datasets to train predictive, inference algorithms that help analysts and then advisors to discern the possibilities of the future and thus to be able to advance corrective actions to the future through executive tasks in the organisation. AI is not replacing human analysts, it is already empowering them.

If we consider structured analysis techniques, we could divide those that are more of direct human reasoning, which we could simply classify as "analogue", from those that allow digitisation and automation through AI that enhances the results by limiting analysis time and improving the capacity to assimilate data and variables in the processes. Let us remember that one of the disadvantages of structured analysis techniques is the time required, their predominantly qualitative nature as opposed to the quantitative, which is ideal for accurately measuring parameters.

In the following table we point out which of the techniques from the collection of structured analysis techniques (Heuer and Pearson, 2015) are more likely to be adaptable to AI processes as opposed to the more 'analogue' human techniques, although all techniques, in one way or another, could be aided by AI.



The incorporation of AI into analysis processes, and their sub-phases in appropriate places, can help reduce such cognitive biases, as mathematical and statistical processes informed in real time by DSS and AI processes have the objectivity and promptness to reduce uncertainty and present reality in a uniform and similar manner on all occasions, or modified to avoid earlier errors of judgement, assessment or bias. In this field, modern LLM and systems with algorithms trained autonomously or supervised by human experts in such assessments are the most advanced, developed and applied.



There is a turning point in the history of intelligence as an activity which was the Gulf War and the failures attributed to intelligence in justifying the war on the existence of weapons of mass destruction, without going into whether they were real failures per se or manipulations to follow a procedure[44] in American democracy of misrepresentation or manipulation of democratic societies to adhere to measures necessary for a political elite, but unpopular until then, such as starting a war.

Although the approach to social sciences and the application of science to the resolution of intelligence foresight problems was not new in intelligence services as large as the American one, , it was the trigger for the worldwide embrace of structured analysis techniques as a toolbox available to analysts to justify and modularise their analyses in a logical and sequential way so that decision-makers could no longer simply attribute successes to themselves, exonerating themselves from failure in a lack or failure of intelligence, a classic.

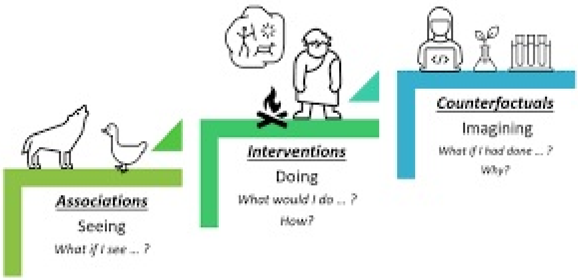
[44] Contrasting facts of this kind were the fortuitous or self-interested explosion of the Maine that started the anti-Spanish press campaign and justified the Cuban War of 1898, or the allegedly erroneous analysis and concealment of indications and reports warning of a Japanese attack on Pearl Harbour that justified and changed American popular sentiment for entry into World War II.

Thus, this modularity allowed decisions to be presented as a process in which, if the decision-maker, normally from the operations speciality or General Staff, without understanding the reason for the final analysis, the intermediate steps and the scientific methodology used were explained to him. If he did not agree, he could modify and go down to the detail of what part of the process he saw as erroneous, to redo it, insert it again into the general process and give a final analytical result, often the same as the initial one, but which already gave confidence to the decision-maker because of his direct intervention.

Evidently, in these modular processes and differentiated techniques, the application of AI is more than feasible and with the passing of the years and the development of more ambitious fields of AI, including generative AI and LLM models[45] that make obsolete the table of identification of feasible techniques to mechanise (in green) of the indispensable compilation book by Heuer and McPherson, in terms of eminently qualitative and analogue techniques of expert intervention, multidisciplinary work teams, white minds, etc. of those that are feasible to transform into quantitative and, therefore, modellable with algorithms and dynamic AI intervention, with cycles of analysis and re-evaluation of the most necessary parameters in near-real time.

Therefore, the incorporation of AI into analysis techniques, among which intelligence professionals largely prefer the structured ones, with the irruption of analysis techniques from sociological, political and advanced statistical science with data science, will revolutionise the discipline in many facets, as it will reduce planning times, effort and time dedicated to punctual analysis of subjects, effects, decisions and prospective scenarios. The wide-ranging analyses of strategic ambition can be used, not operationally, but tactically, insofar as the updating of these analyses goes hand in hand with the pace and tempo of operations at the more immediate tactical level.

[45] LLM, *Large Lenguage Models.*



A point that would need a separate article is the incorporation into the world of intelligence of the so-called "causal revolution" (Pearl, 1981). The conceptual incorporation of the causal ladder to the levels of internalisation and deep knowledge of the matter, place, character or circumstance that is the object of an analysis is for some intelligence professionals of very correct and necessary implementation. Briefly, we would say that this ladder establishes the limits within which the human mind establishes knowledge of any matter, always based on processes of cause and effect, experimentation and feedback.

First we would have the first basic step, which Pearl calls association (Pearl, 2009), in which, by observing reality with our sensors, we try to get as correct an idea of reality as possible. These are facts, events and evidence that we would gather in our situation maps, SITMAP, perfecting the situational alert of the term *Situational Awareness*[46] and that AI is revolutionising with the possibility of visualising on a single screen the various sensors, how and where the enemy and our own troops are, what they are doing... and we are able to see what happens if one of our sensors locates a flash in one position by a type of weapon that impacts a few seconds later in another location and with an effect, for example an enemy artillery battery.

In short, we are able to set variables and see how they are related. On this rung, predictions are needed that are based on passive observations (Pearl and Mackenzie, 2018), and whose mathematical and statistical basis is conditional probability, correlation and regression to associate effects, variables and actors. Here we need data, the more the better, and therefore data management requires AI intervention, in short.

In the second causal step, of intervention, we carry out an experimentation that demonstrates how reality behaves, we solve and we are able to know the processes that

[46] *Situational Awareness.* Situational awareness, a term used in NATO to denote the knowledge of reality that we would include in our current concept of intelligence.

give rise to certain results and, therefore, we would be able to dissect the set of possible solutions and with Bayesian methodology we can infer what effect it would produce on another target if the shot fired by that piece of artillery, which we have previously visualised in the first step, were to hit it. At this level we are not satisfied with just seeing, but we modify what exists, we alter the environment. This is where modern statistical operators come in, such as the *do* for probabilities (P(destruction of my unit | do (enemy battery fires)) that adapt to this type of conditioning factors.

Finally, we have the third causal step, the application of counterfactuals, where we use the unique human capacity to imagine, to deeply understand the processes and we are able to link them together to realise that the key to minimising the impact of that artillery battery in our example, as we ask ourselves what if the battery had not received information about the fire calculation or the location of our position? What if the information is wrong because we give a decoy to the enemy's sensors, what if the truck or the logistics chain does not give the battery the shells it needs, what if the access road to the artillery position is blocked by mines dropped, what would happen? As we can see, we integrate many types of knowledge, in addition to ballistics, to deeply understand the capabilities and even intentions of the problem, in this case the enemy. This is where mathematics comes in, and once mathematics comes in, the step to computational algorithms is immediate.

The three causal steps are intelligence, but truly prospective, anticipatory and effective intelligence implies knowledge of the counterfactuals that allow us to establish futuristic scenarios based on indications and KPIs[47] common in the world of business intelligence, BI, *big data*, automated or algorithmically aided decision making, informed interactive dashboards, the use of *data warehouses* dedicated to a given topic, and, in short, the massive use of AI.

Integration of information

The use of the possibilities offered by network analysis, *link analysis*, and the use of matrix mathematics and graph theory have allowed us to expand AI to fields in which the integration of information is available in various databases, whether structured or not. The

[47] KPI. *Key Performance Indicators*

use of tools or robots to autonomously search for connections by diving into our *data lake*[48] has also pushed the limits of our information integration and exploitation processes.

This *data lake*, in its most accepted English terminology, refers to the general database in which all the data and metadata are available for those robots, those AI algorithms that search for what we tell them in a more efficient, faster and less error-prone way, as they can autonomously recatalogue, rename, reorganise the information into formats understandable by the meta-searcher, being able to drastically reduce that 70% of the time that the *data scientist used to spend in organising, repairing and preparing* the data, reorganise the information into formats understandable by the meta-search engine, being able to drastically reduce the 70 % of time that the data scientist spent until now in the organisation, repair and preparation of the data, manually before applying data science, *Machine or Deep learning*, depending on the purpose sought, let's take for example. The management of various databases and OLAP/ROLAP cubes are among the most solvent for the application of new technologies (Jiménez, 2023; JFD, 2017; Gómez, 2021).

Let us return to the importance of social network analysis and the expansion of the initial tools in the service of intelligence analysts who sought to understand, structure and visualise them in a coherent way in order to use the principles of graph mathematics to search for topography, cohesion and *clustering*, the links between nodes, their power, centrality and many other concepts that began to be analysed with programs such as UCINET, Netdraw, Pajek and ORA (Everton, 2012)[49] , and, of course, the *software* that is so widespread among police, intelligence and NATO services, almost standard we could say: Analyst Notebook, ANB, from i2 that have now diversified to AI libraries in javascript, R or Python, democratised codes in the *Open Source* world, as we exposed in the OSINT section.

With the emergence of AI, the capabilities to extract entities, links, weights of entities, actions, sentiments... makes possible the massive automated transformation of reports into CSV and ANB format, which in Afghanistan needed entire ships of junior analysts 24/7, extracting and preparing these graphs and tables, which once linked by the software enabled senior analysts to get a spatial picture of the networks and their interconnections.

---

[48] *Data Lake*. Data Lake.
[49] ORA. *Organizational Risk Analyzer*

It is nuclear to have computer systems that are capable of extracting data from various types of databases, a subject pioneered by the American company Palantir of Palo Alto, which has long sought to mechanise access to those databases that did not speak to each other even though they physically had liaison officers each with their own system in the intelligence fusion centres, the *Intelligence Fusion Centers*, which General McCrystal planted in Baghdad at the time of the 2007 Surge, and which for many of us was a new revolution in intelligence and the way in which intelligence was integrated to increase the tempo and pace of special operations to be able to win by collapsing a guerrilla insurgency with the intensive use of new joint and integrated approaches and uses of intelligence.

Interpretation

This is perhaps the most human sub-phase and involves the experience, and why not say it, the art, the analyst's nose, to see and intuit what is sometimes not so apparent, aided by the techniques and scientific knowledge behind so many of the processes described.

Broadcasting

Timely delivery of intelligence products by appropriate means to customers who required or may be interested in them. Time is of the essence and security classification is appropriate. Often the products are repetitive and standardised, allowing for mechanisation and form-filling, with the presentation of previous products to give context and a suggestion by IA of events or points to include in descriptive reports, for example.

The integration of intelligence products with DSS systems will be in the Intelligence Fusion Cells, IFCs, which prepare, conduct and collate all briefing and processing missions shaped in the intelligence cycle and then integrate them with the operations cycle and their Joint Operations Centres, JOCs, where they can be tracked and coordinated in the Common Operational Picture (COP), Common Operational Picture (COP), providing rapid access to imagery and intelligence (JFD, 2017), through IT systems, these enriched SITMAPs can be tracked and coordinated in the COPs, *Common Operational Picture,* providing rapid access to imagery and intelligence (JFD, 2017), where early warning systems, intelligence situational awareness (SA), with situational maps are also merged to make sense of the whole.

All of this, which is an EIS, can be enhanced with AI to relate variables and indicators, whether critical or not, to processes that are only visible under parameters set by users, but behind which a multitude of processes are carried out in an automated manner and in real time (Jiménez, 2021; DCDC, 2011).

Counter-intelligence and security

In NATO, the J2X nomenclature is widespread to unify these intelligence tasks, which have the same procedures and tools already described, but which focus on the inside of our countries and organisations, on avoiding information leaks to external services, whether potentially hostile or friendly, because in the search for information we are all looking for everything and everyone (Herraiz, 2023).

The interrelation of certain security departments to protect the physical security of facilities, people, documentation, etc. is complemented by the actual cyber security of computer systems, checking and certifying security systems and anti-intrusion. There is no doubt that the application of AI systems for routine checking of passwords, security breaches and automation of already logged responses will provide survival and keep our secrets and data safe from external spies.

A field that touches on all forensic relations and of great application of AI advances is all that is involved in the sub-discipline of intelligence of personalities and identities, *Identity Intelligence*, which we have already explained above and which has great applications for counter-intelligence and security. Just to underline one fact, it is in J2X where there is a greater link with other civil and police intelligence services with international organisations such as Interpol and Europol for the sharing of information and where biometric information, for example, is not classified and allows the agile exchange of these technical data, "zeros and ones", in which people are represented; without judicial intervention or slowing down or infringement of fundamental rights.

Conclusions

We begin this chapter with an account of a special operation, exposing the exorbitant amount of intelligence that is handled for the development and execution of this example of a mission and its derivatives. To end with conclusions, let us look at these special operations units and the disturbing future of high-intensity conflicts in the "strategic competition between great powers for world domination" in which we are already immersed.

– FIRST. Paradigm shift to broaden the focus of threats to be addressed from insurgent/terrorist non-state organisations to conventional adversaries with the structure, means and order of battle, doctrine and rules of engagement of a state, i.e. a recognisable military force.

  All this implies changing the type and methodology of *targeting*, intelligence gathering, reporting and advice to decision-makers. The intensity and pace of all processes will be the key to success in all domains. AI will enable the automation of processes to shorten decision, intelligence and planning cycles relative to the competitor (Brown, 2022).

  We maintain the idea of broadening the focus insofar as those Islamist insurgent organisations have not disappeared, or new ones may continue or be exploited as *proxies* for state powers. In our case we will have to operate in this Grey Zone (Nieto, 2021), promoting allied armed resistance or as counterinsurgencies on our terrain, and all of them will need intelligence and special operations forces, among others, that are capable of operating in the grey zone.

  There, information superiority and understanding of what strategic competition entails will be facilitated by AI in all aspects: political, military, economic, social, information and infrastructural (PMESII), alongside the diplomatic, cultural and legal that requires access to the maximum depth of knowledge of reality by the lowest tactical levels: That strategic corporal (Krulak, 1999) or the autonomous warriors of the future (Toffler, 1991) as a syllogism of special operations and intelligence soldiers with training equivalent to diplomats with degrees in economics, politics, *marketing/propaganda*, psychology, sociology, medicine... and lethal soldiers; capable of solving situations at the highest level without instructions.

- SECOND: Struggle for all domains: cognitive, moral, physical (land, sea, air/space). The struggle for narrative and legitimacy, as well as competition in the grey zone, will be facilitated by the massive irruption of AI in the coordination of multi-domain actions. Of particular importance for its development with new technologies is the cognitive domain, with the impact of social networks and the links and information residing in *the Deep* and *Dark web* and the use of offensive and defensive social engineering techniques to influence the perceptions, feelings and attitudes of the population and political entities, through psychological and information operations to modify morale, which is fundamental for victory. The increasing use of AI to analyse the information environment through OSINT will be fundamental to prevail and advance intelligence scenarios for subsequent defensive/offensive employment to secure the cognitive and morale domains through the use of campaigns, news creation and manipulation, disinformation with *fake news, deep fakes*, if necessary to finally control the cyber and physical domains (land, sea, air).

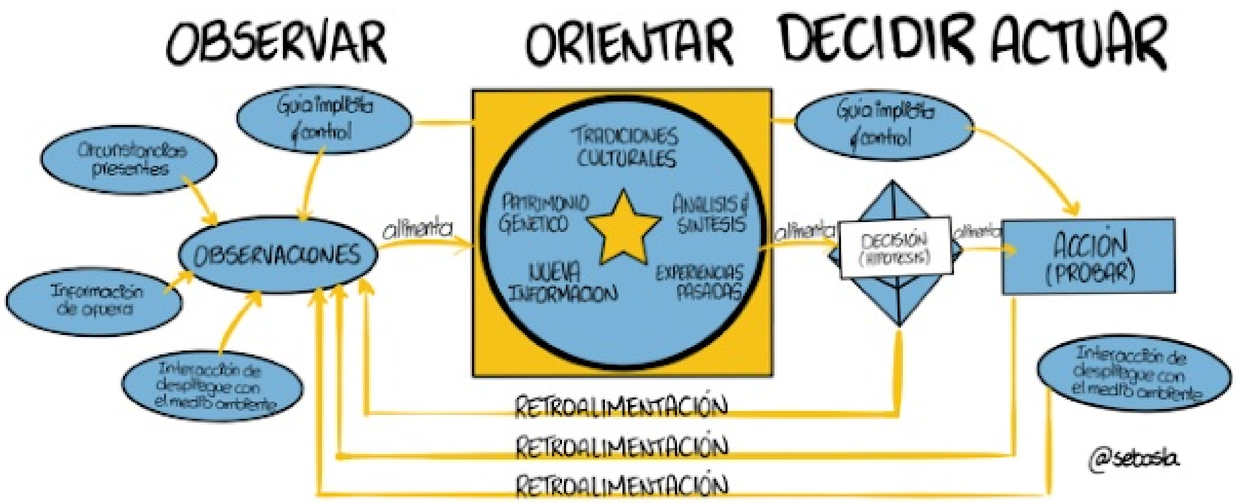
- THIRD: Interconnection of systems and digitisation in an automated way with AI. Technology that can acquire and fuse information from these systems in any domain[50] (Kyle, 2019) and level of conduct (strategic, operational or tactical) with access to sensors[51] to ensure the application of the most appropriate lethal or non-lethal measure, once the potential target has been tracked, identified and acquired. As a corollary, the hyper-sensorisation, computerisation and AI analysis of all environments, mainly urban, makes agent infiltration more complicated, and requires additional cyber capabilities to be able to spoof or mask profiles and physical signatures to those sensors or systems, using alternative systems such as OSINT and IMINT.

- FOURTH: Increased lethality through the use of intelligent and autonomous weapons, increasingly robotised and without final human decision when choosing missions or targets with the help of AI, with lethal or non-lethal effects. War without direct contact[52] (Brown, 2022) at various levels from drones to hypersonic missiles,

[50] *Joint All Domain Operations,* JADO.
[51] *Internet of things* concept applied to tactical communication clouds in areas of operations where military intelligence actions are planned.
[52] Concept of *Contactless war.*

integrated weapons systems, which include autonomous acquisition and analysis with sensors of useful information for their operation in real time, with less and less need for human intervention from their base due to the intervention of AI in the various phases.

– FIFTH. Increased speed and tempo in operations and crises with the intervention of AI in the whole process of orientation and decision making "OODA loop" (Boyd, 1987) in which we basically perform chained causal analyses in which we observe, orient, decide and act/execute and in which the first two are eminently the responsibility of the intelligence cycle.



AI will involve taking command and control warfare to the extreme in order to collapse the corresponding capability of the adversary. Coupled with the hyperbolic capabilities that computers and quantum technologies will give to what we now know, we can infer that the future projection of automated AI application will not have technical limits, but ethical ones.

Fuel	Analytic Type	Observe	Orient	Decide	Act
	Descriptive - What happened?	X			
	Diagnostic - Why did it happen?	X	X		
Data Assets/Sensor Data ->	Predictive - What will happen?	X	X		
	Prescriptive - What should I do?	X	X	X	
	AI - Automation	X	X	X	X

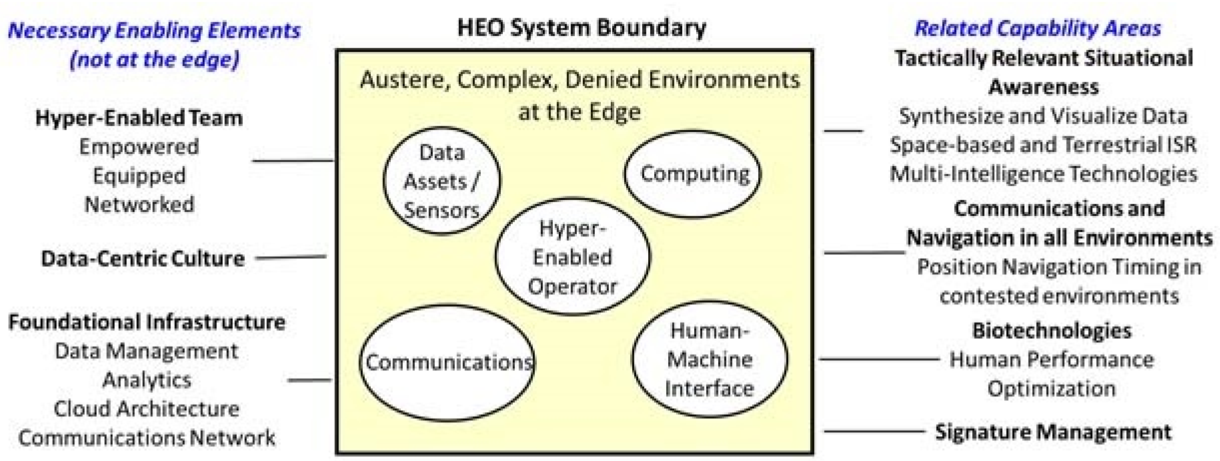
– SIXTH: We believe that we should not be afraid of the transformation that AI will bring about in all areas of society, including the military, as it will enable a leap in technology and capabilities that is difficult to assess. Some analysts argue that the leap will be comparable to the invention of the wheel in ancient times, and we know what happened to the civilisations that did not take advantage of it.

The EU's hyper-regulation in many areas, including AI, may constrain European and Western capacity in the global competition for AI development and application, however laudable this world's first regulatory initiative may be; some practices and uses of AI will be banned altogether, such as cognitive behavioural manipulation and the use of indiscriminate facial recognition systems (Foreign Policy 1358, 2024).

The regulation will not apply to areas outside the scope of EU law and will not affect Member States' competences in the area of national security. Nor does it apply to systems used exclusively for military or defence purposes, including intelligence activities, or to those used for research and innovation purposes (Representation in Spain of the European Commission, article 25/1/2024).

Other factors to be evaluated are those involving human intervention in AI processes: *human OUT of the loop*, with total autonomy; *human ON the loop*, the operator's ability to monitor and stop processes; and *human IN the loop,* with complete control by the human operator. For intelligence tasks, the risk of fatalities is lower because they are non-lethal tasks, and therefore allow for the first type, maximum autonomous AI development.

– SEVENTH: AI will have a significant impact on human-machine interfaces and *big data* analysis to increase situational awareness[53] , reducing cognitive load and increasing assisted decision-making processes at all levels. A good example is the *Hyper-Enabled Operator* (HEO) concept, developed by USSOCOM[54] , as an innovative electronic system that includes sensors, processors, augmented reality and all-weather linkage in the cloud and with the foundations where computational and database capabilities for distributed computer processing will lie (MacCalman *et al.,* 2019).



Its objective will be to provide the right information to each warfighter, analyst and decision-maker in a timely manner without saturating them, linking all levels of exploitation (tactical to strategic) of intelligence that is unique to each human link to perform the value-added and creative activities that are unique to them and differentiate them from the AI that assists them in the rest.

– EIGHTH: Overall, the application of AI to the intelligence cycle enables better results.

Both synthetic AI, which processes large amounts of data to extract information, and inductive logic AI, which looks for patterns in the extracted information, producing intelligence within supporting systems in a concrete form, benefit

[53] *Situational Awareness,* SA, *a* term widely used in NATO jargon.
[54] USSOCOM. US Joint Special Operations Command.

decision-makers using the complex intelligence cycle. Early AI intervention at all stages enables accelerated processing to allow immediate dissemination.

Juan Luis Sánchez Sánchez
Colonel of the Army

Bibliography

Abellanas, M. and Lodares, D. (1990). *Análisis de Algoritmos y Teoría de Grafos.* Ra-Ma.

Aranda Vasserot, A. (2023). *Las 36 estratagemas chinas. Manual Secreto del Arte de la Guerra*. Ariel.

Arévalo, A. (2018). *Artificial intelligence, a priority in US defence strategy* [Accessed: 2024]. Available at: http://hdl.handle.net/10654/21066.

Army Pubs (2023). ATP 3-60 - Targeting, US Doctrinal Liaison, Ground Forces Version. [Accessed 5 February 2024]. Available at: https://www.armypubs.org/atp-3-60-targeting/.

Borne, K. D. (2019). Targeting in Multidomain Operations. *Military Review*. [Accessed: 5 February 2024]. Available from: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Borne-Targeting-Multi-domain/.

Boussad, A., Kodjabachian, J. and Meyer, C. (n.d.). *CIA evasion attacks transferability between machine learning models.* [Accessed: 5 February 2024]. Available at: https:

Boyd, J. R. (1995). Command and control warfare and OODA Loop theory. *Dialnet.* [Accessed: 2024]. Available at:_ https://dialnet.unirioja.es>download>article https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiX-Ozw8bmEAxU1gv0HHbA0DiQQFnoECDIQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F4604097.pdf&usg=AOvVaw2z_dQaNnMqiwSTcu8tOkyg&opi=89978449.

Bringas, A. (2019). The Influence of Big Data in the Intelligence Cycle. *The Security Distillery.* [Accessed: 2024]. Available from:_ https://thesecuritydistillery.org/all-articles/the-influence-of-big-data-in-the-intelligence-cycle.

Brown, A. L. (ed.) *et al*. (2022). *A Perilous Future: High-Intensity Conflict and the Implications for SOF. Special Operations Forces and Great Power Competition.* CANSOFCOM Education&Research Centre. Canadian Special Forces Command. [Accessed: 2024]. Available at: https://jsou.edu/Press/PublicationDashboard/218.

Burcher, M. and Whelan, C. (2018). Intelligence-Led Policing in Practice: Reflections From Intelligence Analysts. *Police Quarterly*. Vol. 22. [Accessed 4 February 2024]. Available at: https://www.researchgate.net/publication/327294043_Intelligence-Led_Policing_in_Practice_Reflections_From_Intelligence_Analysts. DOI: 10.1177/1098611118796890.

Clarín (2020). U.S. indicted four Chinese military officers for stealing data on 145 million people. [Accessed: 5 February 2024]. Available at: https://www.clarin.com/mundo/ee-uu-acuso-militares-chinos-robo-datos-145-millones-personas_0_xjx5F8J7.html.

De la Fuente Chacón, J. C. *et al.* (2022). *Autonomous systems and intelligent robotics in defence*. Academy of Military Arts and Sciences. EEC.

Delgado Gamella, J. L. (2020). *Command and Control Systems and their role in humanitarian aid.* GMV. [Accessed: 5 February 2024]. Available at: http://www.gmv.com/media/blog/defensa-y-seguridad/sistemas-de-mando-y-control-y-su-funcion-en-la-ayuda-humanitaria.

Dhamija, P. and Bag, S. (2020). Role of artificial intelligence in operations environment: a review and bibliometric analysis. *The TQM Journal*. ISSN: 1754-2731. [Accessed: 4 February 2024]. Available at: https://www.emerald.com/insight/content/doi/10.1108/TQM-10-2019-0243/full/html. DOI:10.1108/TQM-10-2019-0243.

*USA. Joint Targeting School Student Guide (*2017). [Accessed: 5 February 2024]. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf?ver=2017-12-29-171316-067

Everton, S. F. (2012). *DIFFUSION disrupting Dark Networks.* Cambridge University Press.

Gómez de Ágreda, Á. *et al.* (2019). *Military uses of artificial intelligence, automation and robotics (IAA&R).* Vol. 04/2019.

Gómez González, Á. S. (2021). Trends in the evolution of military intelligence. *IEEE Opinion Paper 35/2021.* [Accessed: 5 February 2024]. Available at:

http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO35_2021_ANGGOM_Inteligencia.pdf.

Heuer, R. J. (1999). *Psychology of Intelligence Analysis.* Central Intelligence Agency.

Heuer, R. J. and Pherson, R. H. (2015). *Structured analytical techniques for intelligence analysis*. Madrid, Plaza y Valdés, S. L.

Herraiz, P. (2023a). Why did CNI agents leak secrets to the US? *El Mundo*. [Accessed: 3 February 2024]. Disponible en: https:

Jiménez, Á. (2021). *Artificial Intelligence and Machine Learning at the service of Intelligence* [Master's thesis]. Nebrija University and ESFAS.

Joint Force Development (2017). *Joint and National Intelligence Support to Military Operations US Joint Publication 2-01.* Vol. 297.

Kilcullen, D. (2010). *Counterinsurgency*. Oxford University Press.

Knight, W. (2017). China plans to use artificial intelligence for global economic dominance by 2030. *MIT Technology Review.* [Accessed: 5 February 2024]. Available at: https://www.technologyreview.es/s/8475/china-planea-utilizar-la-inteligencia-artificial-para-obtener-el-dominio-economico-mundial-en.

Krulak, C. C. (1999). The Strategic Corporal: Leadership in the Three Block War. *Marines Magazine.* Air University. [Accessed 23 November 2023]. Available at: https://www.mca-marines.org/wp-content/uploads/1999-Jan-The-strategic-corporal-Leadership-in-the-three-block-war.pdf.

Lauroba, E. (2021). The importance of IMINT. *Code Space*. [Accessed: 5 February 2024]. Available at: https://codespaceacademy.com/importancia-imint-ciberinteligencia/.

León, G. (2020). *Strategic implications of technological development. Impact of emerging technologies on the strategic positioning of countries.* Madrid, Ministry of Defence.

Leonhard, G. (2023). *Revolution: ChatGPT and its impact similar to the invention of the Internet*. [Accessed: 5 February 2024]. Available at: https://www.mdzol.com/mundo/2023/5/10/revolucion-el-chatgpt-su-impacto-similar-la-invencion-de-internet-336595.html.

Liang, Q. and Xiangsui, W. (1999). *Unrestricted Warfare: China's Master Plan to Destroy America*. Natraj Publishers. New Delhi.

MacCalman, A. *et al*. (2019). The Hyper-enabled Operator. *Small Wars Journal Online.* [Accessed 5 February 2024]. Available from: https://smallwarsjournal.com/jrnl/art/hyper-enabled-operator.

Martínez, L. (2016). *The Complex Intelligence Cycle: an agile tool for operating in a network*. Spanish Institute for Strategic Studies, pp. 1-15.

National Defense Strategy (2018). *Summary of the 2018 National Defense Strategy of The United States of America.* [Accessed: 2024]. Available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Newcomb, T. (2023). Scientists Can Now Use WiFi to see Through People's Walls. *Popular Mechanics*. [Accessed 5 February 2024]. Available at: https://www.popularmechanics.com/technology/security/a42575068/scientists-use-wifi-to-see-though-walls/.

Nieto, I. (2021). The role of the armed forces in the grey zone. *Global Strategy Report*. NO. 41/2021. [Accessed: 5 February 2024]. Available at: https://global-strategy.org/el-papel-de-las-fuerzas-armadas-en-la-zona-gris/.

European Parliament (2023). *EU AI law: first regulation on artificial intelligence.* Topics. [Accessed: 5 February 2024]. Available at: https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial.

Pearl, J. (2009). *Causality: Models, Reasoning, and Inference*. Cambridge University Press, New York.

Pearl, J. and Mackenzie, D. (2018). *The why book. The new science of cause and effect*. Editorial Pasado&Presente, p. 39.

Pérez Triana, J. M. (2023). *Freedom to innovate in an autocracy? Duel for military technological hegemony: China copies, steals and develops, but will it be able to innovate?* [Accessed: 5 February 2024]. Available at: https://www.elconfidencial.com/tecnologia/2023-03-02/hegemonia-tecnologiamilitar-eeuu-china-innovacion_3585169/.

Pérez González, N. and Sánchez, M. (2019). *Artificial Intelligence: the fourth Industrial Revolution.* [Accessed: 5 February 2024]. Available at: https://www.ayming.es/insights-y-noticias/noticias/inteligencia-artificial-la-cuarta-revolucion-industrial/.

Pillsbury, M. (2015). The *Hundred-Year Marathon. China's Secret Strategy to Replace America as the Global Superpower.* Henry Holt and Company. New York. Reissue with St. Martin's Griffin. 2016.

Foreign Policy (2024). Europe breaks new ground on AI. NO. 1358. [Accessed: 18 February 2024]. Available at: https://www.politicaexterior.com/articulo-completo/europa-se-abre-paso-en-materia-de-ia-342290/

Porche, I. R. *et al.* (2013). *Redefining Information Warfare Boundaries for an Army in a Wireless World*. Santa Monica, CA: RAND Corporation. [Accessed: 5 February 2024]. Available at: https://www.rand.org/pubs/monographs/MG1113.html.

Rainer Granados, J. J. *et al*. (2019). *Artificial intelligence applied to defence.* Documentos de Seguridad y Defensa 79. Madrid, Ministry of Defence.

Representation in Spain of the European Commission (2024). *Las Claves de la nueva ley de Inteligencia Artificial*. European Commission. Independent High Level Expert Group on Artificial Intelligence. [Accessed: 4 February 2024]. Available at: https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/las-claves-de-la-nueva-ley-de-inteligencia-artificial-2024-01-25_es.

Request for information Management (n.d.). [Accessed: 5 February 2024]. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiox63giZeEAxX_g_0HHZ2gDBEQFnoECBAQAQ&url=https%3A%2F%2Fresourcehub01.blob.core.windows.net%2Ftraining-files%2FTraining%2520Materials%2F042%2520PKISR%2520RTP%2F042-011%2520PKISR%2520RTP%2520Lesson%25203.4%2520RFI%2520Management.pdf&usg=AOvVaw0DO5ill-4zkGVFb0jcnBRW&opi=89978449.

Roldán, F. S. (2012). Opinion and Intelligence. *IEEE Opinion Paper 1-4*. [Accessed: 2024]. Available at: http://www.ieee.es/contenido/noticias/2012/06/DIEEEO45-2012.html.

Roldán, J. M. *et al.* (2018). *Artificial intelligence applied to defence*. Madrid.

Rosales, I. A. *et al*. (2005). *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional.* Madrid, Ministry of Defence.

Rouhiainen, L. (2018). *Artificial Intelligence: 101 things you should know today about our future artificial intelligence.* Barcelona, Editorial Planeta, S. A.

Ruiz Enebral, A. (2023). Defence installs terminals of the new classified information management system [online]. *El Confidencial Digital.* [Accessed: 5 February 2024]. Available at: https://www.elconfidencialdigital.com/articulo/defensa/defensa-instala-terminales-nuevo-sistema-gestion-informacion-clasificada/20231218000000688906.html#emstrongrenovacion-tecnologica-strong-em.

Russell, S. and Norvig. P. (2004). *Artificial Intelligence, A modern approach*. Madrid, PEARSON Prentice Hall. [Accessed: 2024]. Available at: Evolutionary trends in military intelligence (ieee.es).

Ruvalcaba, E. (2004). Decision Support Systems or DSS. *Gestiopolis*. [Accessed: 2024]. Available at: https://www.gestiopolis.com/sistemas-soporte-decision-dss/.

Saling, J. M. (1999). *Dynamic Re-Tasking: The JFACC and the Airborne Strike Package*. Defense Technical Information Center. [Accessed 5 February 2024]. Available at: https://apps.dtic.mil/sti/citations/ADA398855.

Scott, B. and Michell, A. (2022). Enhancing Situational Understanding through Integration of Artificial Intelligence in Tactical Headquarters. *Army University Press.* [Accessed 4 February 2024]. Available at: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2022/Scott/

Tariq, M. U., Poulin, M. and Abonamah, A. A. (2021). Achieving Operational Excellence Through Artificial Intelligence: Driving Forces and Barriers. *Frontiers in psychology*. Vol. 12, p. 686624. [Accessed 4 February 2024]. DOI: https://doi.org/10.3389/fpsyg.2021.686624 . Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8295597/ .

UK Ministry of Defence (2011). *DCDC. Understanding and Intelligence Support to Joint*

Operations (JDP 2-00).

Urquizu, P. (2009). What is a DSS [online]. *Business Intelligence.* [Accessed: 4 February 2024]. Available at: https://www.businessintelligence.info/dss/dss-apoyo-decisiones.html.