1970 — 2020

ieee.es

Instituto Español de Estudios Estratégicos

Documento
Opinión

[Visitar la WEB](http://www.ieee.es) [Recibir BOLETÍN ELECTRÓNICO](http://www.ieee.es)

35/2021 22 de marzo de 2021

Ángel Segundo Gómez González *

Trends in the evolution of military intelligence

Trends in the evolution of military intelligence

Abstract:

Military intelligence has been, is and will continue to be a fundamental pillar of the success of military operations, a key element to guide deterrent action, to plan operations, to conduct them and to assess the effects of campaigns and tactical actions. Its essence is immutable but its organization, its processes and its material resources have evolved throughout history. They have done so driven by the evolution of military art, of the operational environment, of technology and of the available knowledge. It will continue to do so. The novelty in the coming decades will come mainly from rapid geopolitical and technological changes and from the added complexity of incorporating non-physical domains into military operations. Technological advances may become disruptive —game changers— and the ongoing reconfiguration of the world order will change the catalogue of threats and possible operational contexts.

Keywords:

Transformation, situational awareness, technological disruption, JISR, algorithmic camouflage, intelligence cycle, cognitive domain.

Cómo citar este documento:

GÓMEZ GONZÁLEZ, Ángel Segundo. *Trends in the evolution of military intelligence*. Documento de Opinión IEEE 35/2021. http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO35_2021_ANGGOM_Inteligencia_ENG.pdf y/o enlace bie[3] (consultado día/mes/año)

NOTA:** Las ideas contenidas en los ***Documentos de Opinión son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

The immutable.

> *"Joshua, the son of Nun, sent from Shittim two spies secretly, saying to them, Go, reconnoiter the land, and especially Jericho."* [1]

Military intelligence is as old as war itself. Its essential elements, its raison d'être, have remained unchanged throughout history. Neither the changes in the conception of war and its execution, nor the possibilities of the available tools -always growing- have made, nor will make, that essence mutate.

Intelligence is dedicated, as is well known, to dispelling uncertainty, to providing understanding of the operational environment and to giving military leaders and their staffs the ability to anticipate, as well as contribute to the neutralization of threats through knowledge of them. That is what it has done for millennia and that is what it will undoubtedly continue to do. The weather forecast continues to predict a persistent Clausewitzian fog[2] over the battlefield for the coming decades and it will be up to intelligence to clear it up.

The vision, understanding, clarity and agility that our strategy, as well as our operational and tactical action, will require in the volatile, uncertain, complex and ambiguous environments of the future will have to be underpinned to a large extent by our military intelligence.

The changes

> *"...this globalized world is characterized by a permanent increase in the speed of change, in which disruptive events are becoming more and more frequent."* [3]

> *"If we want everything to remain as it is, we must change everything."* [4]

The nature of military intelligence has not changed, nor does it look like it will change.

[1] Deuteronomy. Book of Joshua 2:1, in relation to the battle of Jericho. 1400 BC

[2] "War is the realm of uncertainty; three-fourths of the factors on which action in war is based are shrouded in a fog of greater or lesser uncertainty." Vom Kriege/On War. Carl von Clausewitz. 1832.

[3] Panorama de tendencias geopolíticas. Horizonte 2040. Ministerio de Defensa. Secretaría general técnica. 2018 ISBN 978-84-9091-380-2

[4] Il Gattopardo. Giuseppe Tomasi di Lampedusa

However the characteristics and magnitude of the challenge it faces have undoubtedly evolved and will do so much more in the time horizon (2035-2040) on which the transformation and capability development efforts of the Armed Forces are currently being focused.

The accelerated pace of ongoing change and the foreseeable continuity of change as a defining feature of our era, will be the main characteristics of the coming decades. Change will perhaps be the only permanent element, the only thing about which we can be completely certain.

That is why military intelligence, its processes, its organizations and also its strategies with the objectives, lines of effort and resources to be employed, will have to maintain their capacity to adapt to the likely changes. Some of those changes are already underway and we can observe them. Others have not yet arrived, and we should therefore maintain the capacity to respond flexibly to the occurrence of surprises along the way, of unexpected events. Unforeseen events in the field of technology, geopolitics or threats. Surprises that may sometimes mean a change in the rules of the game. Faced with such a contingency, we will have to be able, in spite of everything, to continue to play the game without interrupting it while we adapt.

The multiple dimensions of change

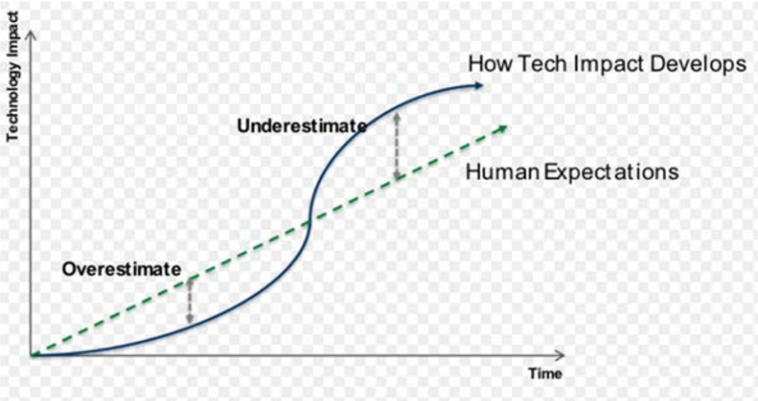
From the military art theory standpoint, the operational environment is understood as the game board of military confrontation, i.e. as the set of elements involved in the actual confrontation or having an impact on it. Technical advances and other changes related to technology have led us to identify and define new spaces of confrontation, new realms of the operational environment.

The non-physical operational domains are still novel elements[5] but their future preponderance is undeniable. Some national doctrines of our allies already consider kinetic actions in the real world -physical destruction and movement- as just supporting activities to the information manoeuvre, which will be the actual main effort of military operations. Cyberspace and the cognitive domain will therefore attract much of our attention and resources in the coming decades. Intelligence will have to position itself - it

[5] Cyberspace was officially declared as an operational domain by NATO during the Warsaw summit. 2016

is already doing so and not without some initial discomfort - on the borderline between the physical and non-physical domains, while maintaining its ability to act in both and to integrate them into its gaze and analysis.

Advances in technology and the significant acceleration in the development of old and new technologies surprise us every day. We can imagine that their impact on military activities and in particular on military intelligence processes will be very important in the coming decades. The well-known AMARA law[6] warns us that technology and its impact on our processes will exceed our expectations in the medium and long term. We can be sure that the 2040 technological horizon will enable, even urge, changes in military intelligence. It may not be enough to simply revamp the intelligence building. We may need to build a new one.



The geopolitical and security situation will change almost as rapidly as technologies. It is already doing so and it never ceases to surprise us. The changes underway and those we will see in the coming decades will force us to reorient priorities and ways of working in military intelligence and also to keep an eye on aspects and dimensions that we have neglected so far. The SARS COVID 19 pandemic has already given us some clues in this regard.

In addition to the change in the balances of military power and in global or regional geopolitical dynamics, there will also be changes in the typology of conflicts for which we will have to be prepared. Some types of conflict that have been forgotten for decades, such as high-intensity symmetric (peer-to-peer) confrontation, are once again on the geopolitical horizon. Both changes, together with new scenarios for the employment of

[6] "We tend to overestimate the effect of technology in the short run and underestimate in the long run" (Roy Charles Amara)

the armed forces in support of civilian authorities, make up a varied catalogue of operational contexts (OC). These diverse OCs will have new intelligence requirements and will demand an adaptation effort from our military intelligence, which will be major in some cases.

There will also be important changes in relation to human resources and the socio-cultural context. Men and women have been, and will continue to be, the essential element of the Armed Forces. Leaving aside demographics and their quantitative impact on the problem of generating and maintaining military forces, the qualitative aspect must also be considered. The new generations, digital natives, will have difficulty understanding the physical world. However, the physical world and the lethal confrontation will continue to exist despite the preponderance of information manoeuvre. In extreme cases of military confrontation, fighting on land, at sea and in the air will be the decisive element in the outcome of the conflict. The ability to understand that the objects represented on our screens correspond to real objects in the world and that trending topics have the hearts and minds of real people behind them, will be an essential skill for future intelligence analysts. It seems clear that they will not bring it "as standard" when they´ll join the Armed Forces.

Military intelligence 2040. Some broad features.

Technology. Solution provider and transformation promoter.

In the recent paper "Science & Technology Trends 2020-2040. Exploring the S&T Edge", NATO makes an interesting technology foresight study that gives guidance on what we can expect from technology in the coming decades.

There are some areas where exponential development is expected. Many of them will have a major impact on military activity in the coming years and could be grouped, based on their nature, into 4 broad categories: smart technologies, digital technologies, distributed technologies and interconnected technologies[7].

The combination of advances in intelligent and digital systems will lead to astonishing progress in the "battle of precision", both in the field of acquisition and in the field of positioning and navigation. Future networks will be digital and interconnected, with

[7] https://www.sto.nato.int/pages/tech-trends.aspx . Read on 20.02.2021

network elements distributed and expanded to link the cyber, cognitive and physical domains. In this last dimension, the implementation of IoBT / IoMT (internet of the battlefield things / internet of the military things) and D2D (device to device communication) will be important.

The combination of intelligent and distributed technologies will lead to an unprecedented expansion of autonomous systems, an autonomy that will find its limits in laws and ethics rather than in the ever-decreasing shortcomings of technology.

Many disciplines will experience a remarkable breakthrough: data science, quantum computing, artificial intelligence, biotechnology, autonomous systems, space, hypersonic speed and new materials. Combinations of achievements in some of these fields will produce truly disruptive effects on military intelligence and will drive major changes in its processes and organizations.

In relation to the collection disciplines, there are so many examples of the impact of technology that there is not enough space in this short document even for a simple enumeration. I will mention though, as a paradigmatic example, how the oldest and most classic Intel collection discipline, human intelligence (HUMINT), will also be drastically affected. HUMINT will continue to exist as we know it, but remote human interaction (cyberHUMINT), automated linguistic translation, lie detection by biometric & gestural processing, or indirect personality profiling of human sources through the use of artificial intelligence will be implemented.

JADC2ISR[8] . Agility and multidomain transversality.

The Atlantic alliance's JISR initiative (launched at the Chicago 2012 summit) has enhanced NATO's capabilities in intelligence support to operations, especially in relation to events requiring urgent response and high agility. This is especially visible in the support to situational awareness for ongoing operations and in the field of targeting, especially time sensitive targeting. Its modernizing effect on efficiency and interoperability is not yet complete though[9].

The tempo of the operations is expected to continue to rise and the need for immediate

[8] JADC2ISR: Joint All Domain, Command, Control, Intelligence, Surveillance and Reconnaissance

[9] NATO´s JISR initiative reached IOC (intermediate operational capability) in 2015/16 but no FOC (final operational capability) timeline and criteria was established

response will demand increased efficiency and agility from intelligence and JISR. That is to say: from their organizations, processes, networks, services and functional systems. In addition, the multi-domain approach to operations and the relationship between physical and non-physical domains will add complexity to that challenge and force the JISR to reinvent itself[10]. For example, multi-domain X-cueing[11] processes will have to be implemented to help improve the dynamic part of ISR operations[12] by integrating collection in the physical and non-physical realms into a single collection operations management system.

New operational contexts. New threats.

Changes in the geopolitical environment will force military intelligence to maintain the capability to deal with a wide variety of threats and military contenders. Engagement will occur in the various physical and non-physical domains and across the broad spectrum of conflicts, in many cases without leaving the so-called grey zone.

Some of the threats will exploit the opportunities of the vast spaces, with little population and almost no effective governance in the area of the Maghreb, Sahara and Sahel. The ability to monitor these areas without or with a very low density of military occupation, will give more importance to intelligence, surveillance and reconnaissance activities. In this field, among other systems and collection disciplines, wide area surveillance (WAS) sensors, particularly GMTI[13] and optical, infrared or radar imagery sensors, on board piloted, remotely piloted or autonomous aircraft will multiply , as well as the unattended ground sensors.

The operational context of combat in urban and suburban areas, even in megacities, will require new techniques, tactics and procedures, as well as a fresh look at certain old challenges. To give just one example, geographic and infrastructure information will require near real-time updating to navigate around obstructions and destructions

[10] JADC2: Getting to Real-Time Object Data and Tracking in All Battlespace Domains https://www.saic.com/blogs/jadc2/getting-to-real-time-object-data-tracking-from-all-battlespace-domains. Date of consultation: 22.02.2021

[11] X-cueing: Process of activation of a collection asset (platform+sensor) upon the information collected by another collection assets during the conduct of the ISR collection OPS.

[12] Sub-process called *Collection Operations Management (COM) (part of JISR process)*

[13] Ground moving target indicator.

throughout the urban terrain, as well as to identify semi-permanent obstacles. The miniaturization of laser scanning technologies (LIDAR) on board small RPAS will be the solution to this challenge and will be available in the near future. These systems will also make it possible to model in 3D the infrastructures inside which operations will take place.

The situation map. The intelligence contribution to the COP

> *"Treat data as a strategic asset*" [14]

The Common Operational Picture (COP) will become unusually complex in multi-domain operations. The recently coined term DATA BASED COP refers to a multi-layered digital "situation map", configurable on demand and capable of ingesting and presenting a huge volume of raw data, structured or unstructured, with automated infographic presentation and also of already processed objects. High capacity networks will provide connectivity to all types of attended and unattended sensors in the multi-domain environment. The greatly enhanced capability that will be provided by IoBT / D2D and 5/6G[15] will largely be the enabler of this enhanced COP that will be a super-consumer of data. The sources of this data will not be limited to military providers and sensors.

Data exploitation, transmission and storage.

The data traffic that future military networks will support is difficult to estimate. Future intelligence, like the present, will be the most demanding operational community for the CIS networks in terms of information exchange and storage. Autonomous or unattended air vehicles (e.g. RPAS-pseudo-satellites), unattended terrestrial or maritime sensors, and many other multidomain collection resources will produce an enormous volume of data. Our exploitation and fusion capability will face a challenge. Keeping our ingestion and exploitation capability up to the growing demand generated by the massive collection will be one of the keys to success in future multi-domain intelligence.

In its recent ground-breaking document "NATO guide to data collection and management for analysis support to operations"[16], NATO declares that data is the key to success in

[14] US DoD Digital modernization strategy. 2019. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF. Date of consultation: 20.02.202
[15] The 5G is promising data transfer speeds up to 20Gbps, 6G might reach 1Tbps
[16] TR-SAS-111 Science and Technology Organization. Agosto 2020 (NATO UNCLASSIFIED)

future multi-domain intelligence and also that the data never expires. This indisputable statement will also pose a major challenge for the storage of raw or exploited data in our repositories. Their capacity must always be sufficient to accommodate this uninterrupted and ever growing flow of incoming data and information from all domains and areas of the operating environment.

Another interesting aspect is the progressive dissolution of the once rigid boundaries between the strategic, operational and tactical levels of operations. This evolution will be very clear in military intelligence and will force complete connectivity between networks and full access to repositories from all levels with the required restrictions due to security and operational necessity that may be established[17].

Outsourced Intelligence and Security Domain Integration

For several years now, military intelligence has understood the need to undertake the study of the operational environment with an integral approach and a holistic methodology to decipher its multifaceted complexity. The new multi-domain operational environment only adds to the complexity of this challenge.

In the past, both access to information and expertise in matters of interest to military intelligence were found predominantly within the armed forces. This is no longer the case today, and will be even less so in the future. Military intelligence will have to integrate existing capabilities in other organizations (the so-called intelligence reserves) and even the knowledge and talent of individuals working in other areas of the administration or outside it.

This will require secure solutions for the interconnection between classified networks and domains (with different levels), unclassified networks and even the Internet.

Reachback and federated efforts.

There is a trend already underway to try to reduce our footprint on the theatre of operations, our physical presence there. In application of the REACHBACK concept, many elements of analysis and management of processes and sub-processes of the

[17] "Army connecting tactical and enterprise networks for multidomain operations" Andrew Eversden. . Date of consultation: 19.02.2021

intelligence cycle and the JISR process have already been moved out of the operational areas. This trend will grow in the future with collection management units, as well as processing, JISR exploitation and intelligence fusion units, physically separated from the collection units deployed in the area of operations. This will require robust technical solutions to ensure availability of support and continuity of data flow.

Intelligence and Influence.

> "*We are good at killing terrorists and kinetic actions. However, we fail to realize that we can't kill an idea."*[18]

In the new cognitive domain battles, necessarily synchronized with actions in the physical world, military intelligence will have to be an important contributor to the new joint function information. In fact, it always has been, even though no one in the past defined the joint function information or the cognitive domain of operations. As the RAND Corporation states in a recent analysis paper[19], information operations and intelligence have always been an essential part of military operations and "information" in its generic meaning has been and is the essence of both communities.

The contribution of JISR and intelligence to non-lethal influence/targeting actions ("influence artillery rounds"[20]) will mirror its contribution to lethal targeting but with much greater complexity. The development of capabilities in this field and of synergistic collaboration procedures between the intelligence and information/influence communities, will require a great effort of creative modernization. Intelligence processes and their synchronization with the new operational community of influence, will have to be reviewed in order to achieve efficient synergy between the two communities. In this case, as it happens normally between confined areas and processes, the blurred and imprecise boundaries pose a great challenge. A double challenge: duplication of efforts must be avoided as well as the risk of neglecting certain areas or aspects. Coordination,

[18] Future military intelligence CONOPS and S&T investement roadmap 2035-2050. The cognitive war. Edward L. Haugland (US army intelligence/DA DCS G2). 2019. https://nsiteam.com/future-military-intelligence-conops-and-st-investment-roadmap-2035-2050-the-cognitive-war/ . Date of consultation: 17.02.2021

[19] "Intelligence support to operations in the information environment". RAND corporation 2020. https://www.rand.org/pubs/research_reports/RR3161.html. Date of consultation: 28.01.2021

[20] "Special Forces to build 'influence artillery' for online campaigns". Mark Pomerleau. https://www.c4isrnet.com/information-warfare/2021/02/18/special-forces-to-build-influence-artillery-for-online-campaigns/ : Date of consultation: 22.02.2021

division of functions, seamless exchange of information and avoidance of competitive approaches between the two communities should be the basis for synergistic cooperation between the intelligence and influence/information communities.

Intelligence exploitation, fusion and production. Analytical processes.

There is no doubt that quantum computing and artificial intelligence will make the best of the massive flow of data from JISR and many other sources. Correlation, fusion and analytical processes will be transformed, automated. Advanced functional services to support analytical processes and the new, increasingly natural, language-like relationship between the analyst and the information repositories will lead to a new way of producing intelligence. Man-machine teams will be configured in which the database will be much more than a tool, it will be a companion of the human being, the other half of this buddy team[21].

An interesting aspect in this regard has to do with the predictive function of intelligence and the ability to anticipate. Our algorithms will be able to predict enemy action better than the analogical analytical methods we know. In reverse, our opponents, and we ourselves, will develop algorithmic camouflage mechanisms. Thus, similar to the way we used to hide from sight in the physical world, we will also try to hide from algorithmic prediction in the data world. Surprise will be sought through action so irrational or so far from the usual patterns that they are unpredictable for the algorithm.

Dissemination.

The modernization of the dissemination phases of the intelligence cycle or JISR process are already underway. Changes will continue in this field.

Dissemination is and will be one of the major beneficiaries of achievements in information systems and telecommunications. Those of us who are more senior in the armed forces may remember a dissemination based on the conveyance of intelligence products, even on paper in many cases. Moreover, they were distributed in accordance with rather rigid and restricted criteria, through the chain of command. Things have changed and will

[21] Human-machine teaming (JCN 1/18). https://www.gov.uk/government/publications/human-machine-teaming-jcn-118. Date of consultation: 25.01.2021

change even more for this final phase of the intelligence cycle and the JISR process, a seemingly banal phase but much more important and complex than one might often think.

Dissemination is evolving towards a new paradigm. The distribution of data, of exploited information, of intelligence products and also of objects to enrich the representation of the operational environment in COPs and in command and control systems as well as the so-called battle space objects (BSO), will be handled in an automatic but singularized process. Dissemination will be increasingly adapted to the unique needs of each user and each consumer process and will be governed on the basis of profiles taking into account both the user's needs (not just his generic need to know) and his capacity to ingest intelligence or information exploited from the JISR process.

One of the big challenges in dissemination is the extension of advanced Intel and JISR services to the lower tactical levels, for example video streaming services. In the future, small units at the tactical level will have access to many of the data repositories and to the part of the COP that is relevant to the execution of their operation. Holographic display glasses and other technological devices will allow at-a-glance access to the actual terrain, elements of planning and intelligence relevant to the operation, as well as to urgent notifications received while executing the operation, including time sensitive intelligence.

The speed of decision cycles, the requirement for immediacy in urgent operational processes (time sensitive targeting, time-sensitive-actionable-intelligence driven operations) will require conciseness in dissemination. The new culture of brevity and immediacy that is shaping the intellect of the new generations will further underscore this need. Infographics, augmented reality or holograms will give unimaginable possibilities to the dissemination phase of the intelligence cycle and the JISR process.

The old sandbox will be replaced by highly immersive virtual realities for mission rehearsals. Surprises and uncertainty upon entry into unfamiliar terrain or infrastructure will be reduced to a minimum.

Quality control and effects analysis.

Intelligence and JISR processes should establish mechanisms to assess the quality of production and its impact on the processes that consume it. The evaluation of the "strategy" in Intel and JISR - the ends, ways and means - must help improve its contribution to the supported operational processes, to the authorities that decide upon such intelligence and ultimately to the success of the military action. This evaluation will have to be continuous and be fed by numerous indicators that will be processed with the new tools provided by the data science, advanced computing and artificial intelligence.

Countering legal and ethical asymmetry.

While safeguarding the rule of law and, in particular, the individual rights of the citizens, our society and in particular our military intelligence will have to gear itself up with the appropriate regulatory framework for multi-domain conflict. There is no doubt that in handling data and acting on the vectors of the cognitive domain, our foreseeable enemies will have fewer ethical and legal constraints than we do. This situation could lead to losing battles even before they are fought if we do not equip ourselves with the appropriate legal tools.

Adaptability as we approach the VUCA[22] future.

Software developer Eric S. Raymond formulated in his book "The Cathedral & the Bazaar"[23], an attractive theory in relation to his work. Raymond argues that large projects should be conceived, designed and executed more like an Arab, Turkish or Persian bazaar than a Gothic cathedral.

The Gothic cathedral is designed and then construction begins, only to be completed much later. The design is solid, beautiful and adapted to the initial requirement but normally the very perfection and rigidity of the project prevents its modification when, with the project already in execution, time leads us to wish that the final result be different from the one originally conceived[24]. A bazaar, on the contrary, is established on the basis of a few general organizational lines which allow adding and subtracting, modifying and reconfiguring the initial idea as the establishment of the bazaar continues and even when it is already in operation.

[22] VUCA: volatility, uncertainty, complexity and ambiguity. Acronym proposed by the US Army war college including 4 words to describe environments such as the one we are currently facing and (even more) its expected future evolution.

[23] ISBN 1-565-92724-9

[24] https://www.ileon.com/actualidad/101091/la-cupula-que-casi-derrumba-la-catedral-de-leon-y-la-convirtio-hace-175-anos-en-el-primer-monumento-nacional-de-espana . Date of consultation: 20.02.2021

This philosophy of adaptability to change must govern the modernization process of our military intelligence as well. Raymond's concept, conceived for software developments, could and should also be applied to the redefinition of our operational processes and our organizational and systems architectures. Only in this way will we be able to successfully meet the upcoming requirements that the future will bring. Those requirements will not be immutable because, as we all know, the future is a moving target.

*Ángel Segundo Gómez González**
Col. Army. Director. Intel Dept
Higher studies school of the armed forces