The Technological Centre for Development and Experimentation in Jaén will meet the need for disruptive technology-related military capabilities

Technological revolution on the battlefield

Major General (r) Jesús Carlos Gómez Pardo
Dr. Ordnance Engineer

WE live in a convulsive world, and in our haste to systematise, we refer to this world as VUCA (volatile, uncertain, complex, and ambiguous), an acronym that has defined our environment since the fall of the Berlin Wall. The year 2020 witnessed the emergence of a new black swan, the COVID-19 pandemic, which profoundly affected our lives. The term FANI (fragile, anxious, non-linear, and incomprehensible) was coined in the wake of the pandemic to describe the fragility of these times. While VUCA focuses on the factors causing uncertainty and complexity, FANI focuses on the effects they have on organisations.

The stable, known, parametrisable, and future-predictable world of blocs that characterised the Cold War is now history. The fall of the Berlin Wall in 1989 upset the geopolitical balance and precipitated a series of events. In Europe, the 2013 Ukrainian Euromaidan uprising was followed by Russia's illegal annexation of the Crimean Peninsula in 2014, and the subsequent invasion of another part of Ukraine's territory in 2022. The impact on our society is proving to be enormous.

Instability prevails in the rest of the world. Thus, the Gaza conflict, US-China tensions, the melting of the Arctic or the weakening of transatlantic relations lead us to think that the world we have lived in will never be the same.

Spain is not excluded from this complicated geopolitical reality that poses huge challenges to global security. As part of Spain's commitment to our partners, our Armed Forces participate in 17 operations abroad with over 3,000 soldiers and civil guards on four continents.

On the other hand, this instability and uncertainty in global geopolitics is catalysed by the technological revolution in which we are immersed. Our society is evolving at a dizzying pace with the emergence of new technologies that are bringing about profound changes in the way we think and act, and are accelerating the transition to the digital era.

Our Armed Forces, which are an integral part of society, are undergoing a process of digital transformation that is changing the art of war. Examples of a reality that is significantly modifying current operational concepts include a transparent, digitised and hyper-connected battlefield; network operations; well-equipped combatants who serve as nodes in the warfighting network; and the widespread use of unmanned vehicles, autonomous systems, drones, and armed robots acting individually or in a collaborative manner.

The only way we can overcome technological challenges, unknown futures, and huge security issues is by developing agile structures, adapting constantly to the rapidly changing environment, and creating more adaptable and resilient organisations that allow us to survive and operate in an increasingly uncertain and complex environment.

The extensive use of drones is one of the fundamental changes that has been highlighted in Ukraine

LESSONS LEARNED

From the war in Ukraine we can cautiously draw the first lessons learned, as set out in a paper produced by the Joint Concept Development Centre (JCDC) of the Joint Chiefs of Staff.

Russia's illegal invasion of Ukraine seems to have brought us back to a conventional high-intensity conflict, although with certain exceptions: both parties are making extensive use of specific emerging and disruptive technologies characteristic of modern conflicts; there is also a clear confrontation between Russia and the West in the "grey zone"; and all this against the backdrop of the nuclear threat. Operations are being carried out in the multidomain operational environment, which integrates both the physical (land, sea, air, and outer space) and the non-physical (cyberspace and cognitive space) domains established by the Spanish doctrine.

Moreover, some significant changes in battle, associated with digitalisation, have been identified, with the extensive use of drones standing out as particularly noteworthy.

From this terrible and highly attritional conflict, and focusing on its technological aspects, we can draw the following conclusions: that intelligence, surveillance, reconnaissance and target acquisition capabilities are key to operational superiority; that on the battlefield it is critical to have long-range precision fires to hit targets, minimising collateral damage and moving away from counter-battery actions; that heavy firepower is necessary to saturate the adversary; that the battlefield is becoming digital, and that it is now evident that in order for network operations to be possible, we need to ensure that sensors and combat systems are interconnected with management centres and fire-producing or effector elements; and finally, that it is crucial to have robust, redundant, and highly mobile command and control systems (C2) in order to ensure this interconnection. Additionally, electronic warfare capabilities must be able to operate in the electromagnetic spectrum with the necessary superiority in order to guarantee operability in degraded environments and freedom of action in the five operational domains.

It is therefore essential to have powerful electronic warfare systems capable of jamming the adversary's PNT (position, navigation and timing) signals, but without affecting our own systems. The situation is similar in the Gaza conflict. The widespread use of Israeli electronic warfare prevents Hamas, Hezbollah, and any other group operating in the area without PNT supremacy, from effectively utilising their weapons systems. This is known as navigation warfare (NAVWAR).

NEW MILITARY CAPABILITIES

These lessons have led to the need to equip our soldiers with new military capabilities in light of the disruptive technologies emerging on the battlefield, which are described below.

• Navigation warfare

Most sensors and systems used on the battlefield (command and control systems, communications or navigation and guidance subsystems) use the satellite navigation signal to ensure precise PNT. However, they are highly vulnerable as the satellite navigation signal may be degraded or denied. Due to their heavy reliance on this signal, these systems are particularly sensitive to spoofing and jamming attacks. If we bear in mind that the use of jammers has become widespread in all types of

conflicts due to their efficiency, low cost and ease of implementation, we can understand the enormous vulnerability of these systems.

The loss of the satellite navigation signal increases positioning errors and, therefore, weapon systems using satellite navigation in unstructured environments (degraded or denied signal) are rendered useless for combat. Navigation warfare is defined as the set of actions and technical measures that ensure the superiority of PNT information. NAVWAR is responsible for protecting our navigation systems —those that provide geographical positioning and those that offer reference timing signals— and for degrading the adversary's positioning, navigation and timing information.

There are three ways to ensure a robust PNT signal: by protecting our satellite navigation systems through various techniques; generating an independent timing reference; or using alternative navigation systems, such as terrain-based navigation systems.

In the Ukrainian conflict, we have been able to see the state-of-the-art electronic warfare equipment used by the Russian military. In particular, their GPS (Global Positioning System) jammers are capable of operating at a distance of over 500 km, which allows them to jam Ukraine's satellite guidance and positioning signals, thus preventing the use of precision-guided munitions, equipped with GPS/inertial terminal guidance, or the operation of Ukrainian drones. These Electronic Warfare (EW) capabilities, which are among the most important in the world, have seriously hampered the actions of the Ukrainian military. The issue is of such relevance that the US Department of Defense created the Joint Navigation Warfare Centre in 2004.

CETEDEX will be a benchmark in the fields of autonomous and connected vehicles, anti-drone defence and AI

As a result, we need to develop technologies that allow us, on the one hand, to ensure a robust PNT signal for those systems that use satellite navigation, such as the Excalibur precision-guided munition, or the combat vehicle navigation systems, and, on the other, to deny the adversary's signal.

• Anti-drone defence

Another important aspect of the conflict in Ukraine is the massive use of drones for intelligence gathering, surveillance, target acquisition, reconnaissance, or the destruction of tactical targets —either used as low-cost precision weapons or to collapse air defences through swarm attacks—.

In its operations, the Russian military is using simple drones, such as the Orlan-10, for surveillance, reconnaissance and electronic warfare missions. It also has higher capacity drones, such as the Iranian Shahed-136, which causes terrible physical and psychological effects when used in swarms and as loitering munition.

A swarm drone attack is, therefore, a real threat for which we are not yet adequately prepared. In this regard, NATO requires anti-drone systems or C-UAS (Counter-Unmanned Aerial Systems) to have a minimum set of capabilities.

The development of technologies to counter drones has become a top priority due to their rapid evolution and drone usage tactics. It is paramount to have C-UAS systems capable of locating, identifying and tracking the single or swarming drone threat, by developing different types of technologies, such as two- or three-dimensional radars, IR/VIS (infrared-visible) detectors, RF drone detection and location systems, or threat location and identification systems that use the Mavlink protocol. They must also be capable of neutralising the drone threat, using either electronic warfare techniques such as jamming or spoofing, that act on the drone's radio link or geolocation signal (soft kill), or physical destruction techniques, such as kinetic effectors, laser weapons, nets, electromagnetic pulses, defensive swarms, etc. (hard kill).

Furthermore, artificial intelligence applications will need to be created for a thorough simulation of the battle environment and for an efficient C-UAS integrated combat management system to ensure the security of any operation.

• Autonomous vehicles

Autonomous land vehicles are also being used extensively in the Ukrainian conflict, and particularly naval autonomous vessels, a domain in which Ukraine is achieving great success in its Black Sea operations.Therefore, robotics and autonomous vehicle technologies must be developed in order to automate drive-by-wire systems, as well as to develop advanced driver-vehicle interfaces, and technologies for interaction between unmanned ground vehicles and unmanned aerial vehicles (UGV-UAV).

In addition, other critical technologies have been identified that require AI (Artificial Intelligence) models and algorithms for their maturation, including sensor fusion, precise positioning in complex environments, autonomous navigation in unstructured environments, development of automation algorithms, route planning and collaborative operation.

• Logistics transformation and AI

Alongside the enormous current computing capacity, technological tools are emerging such as artificial intelligence (AI), cyber-physical

systems, machine learning, cloud systems, big data, etc. And, as a result, the twelve technologies associated with Industry 4.0 that optimise logistics processes. The Army and Navy logistic support commands are undergoing a profound transformation of their structures, evolving from reactive-preventive logistics to predictive logistics (logistics 4.0), based on digital transformation.

The new logistical processes will make it possible to maximise the operational availability of weapons systems, which is the ultimate goal of military logistics. It is therefore a top priority to have the capability to develop technologies and tools aimed at the predictive maintenance of buildings and weapons systems through the use of Industry 4.0 technologies.

AI is conceived as a cross-cutting enabling tool. We have seen that both the technologies associated with NAVWAR and the development of autonomous vehicles and anti-drone systems need the support of AI applications. Thus, AI developments in this field should focus on the automatic and intelligent analysis of massive amounts of data from weapons system sensors; the development of technologies for the predictive maintenance of platforms; and the intelligent analysis of information sources to aid in decision-making.

CETEDEX PROJECT

We are witnessing terrible conflicts that are affecting global security and posing major challenges to our way of life. Disruptive technologies have been used in these conflicts and have significantly altered military operations. The lessons learned highlight the need to equip our soldiers with military capabilities beyond what was previously anticipated.

We must therefore develop technologies, in the form of advanced weapons systems, that give fighters a clear operational advantage on the battlefield. And the Technological Centre for Development and Experimentation (CETEDEX) in Jaén was conceived specifically for this scope of action. It was designed as a centre for the agile development of those security and defence technologies that will enable us to successfully deal with new threats to global security.

CETEDEX was established to respond to this need. Its mission is to develop, certify and experiment dual-use technologies that offer groundbreaking and transformative solutions in the fields of autonomous and connected vehicles, anti-drone defence and AI. An opportunity project that will start operating by the end of 2026 and will be fully operational by the end of 2028.