“The Army and Future Challenges” Conference 2024

Cyberspace operations

Major General Fernando Luis Morón
Director for Research, Doctrine, Organisation and Materiel of the MADOC

ON 6 and 7 May 2024, the Training and Doctrine Command (MADOC) hosted the eighth edition of “The Army and Future Challenges Conference, entitled “The Army and Cyberspace Operations”, in the University of Jaén’s aula magna. At this event, prominent figures from various fields discussed the implications of this new cyberspace domain for military operations.

The conference was presided over by the Chief of the Army Staff, Army General Amador Enseñat, who, after the inauguration, gave the floor to the Lieutenant General commander of the MADOC and to the Rector of the University of Jaén. Both speakers discussed the geopolitical environment, which is defined by the pervasiveness of digital devices and our extreme reliance on them. They also talked about the opportunities and risks that new developments in cyberspace-related technology bring for security and how they affect military operations.

The conference programme was organised into three initial conferences and three round tables. Lieutenant General José María Millán, Director General of the Centre for Information and Communications Systems and Technologies (CESTIC), described the capabilities that this centre provides to the Armed Forces’ operational structure. These capabilities include hyperconnectivity, ensuring freedom of action in cyberspace, attaining information superiority and the development of multi-domain operations.

In addition to the previous strategic approach, in the second lecture, Vice Admiral Francisco Javier Roca, Commander of the Joint Cyberspace Command (MCCE), analysed the operational dimension provided by the current war in Ukraine, and the lessons that may be drawn from it. He stressed that in Ukraine we are witnessing the most technologically advanced war in the history of mankind, due to the successful use of a new area of operations: cyberspace.

Major General Guillermo Ramírez Altozano, Head of Information Systems, Telecommunications and Technical Assistance (JCISAT), gave a lecture that concluded this initial transversal view. He focused on the tactical level and the Army’s specific role, sharing his view on the present and future of land operations in cyberspace and the effort the Army is making by maintaining 15 to 20% of its personnel specially trained to operate in the cyberspace domain while contributing with some 2,000 troops to the joint effort.

Following this complementary perspective from the three levels, strategic, operational and tactical, the first panel of speakers, moderated by cybersecurity journalist José de la Peña, focused on “Cyberspace as a New Operational Environment”.

Colonel Francisco José Oliva of the JCISAT, the first speaker, provided an introduction to cyberspace, a new global domain that has arisen with the popularity of the Internet. Its physical components are connected via the electromagnetic spectrum, carrying information that can have an impact on other physical and/or cognitive domains, constituting seamless unity.

Cyberspace-related technologies pose security risks and have an impact on military operations

Colonel Ignacio Javier Simón, the MCCE representative, provided numerous examples of the role played by cyberspace in recent conflicts. He mentioned navigation and positioning warfare, satellite communications, observation satellites and electronic warfare, the latter, for example, having proven to be a very effective means in the fight against unmanned aerial systems.

Colonel Bonifacio Gutiérrez de León of the MADOC continued his detailed explanation of how new disruptive technologies, mainly artificial intelligence, are revolutionising the operations space, particularly in cyberspace, in areas such as decision-making, situational awareness, and secure communications, enabling so-called multi-domain operations.

Manuel Medina, a Constitutional Law Professor at the University of Seville, concluded this vision of cyberspace as a new operational environment by introducing us to its legal framework. He highlighted how current regulations exclude security and defence systems from the safeguards of people's rights when using automated systems and AI. It is hence necessary to find an interpretation in international law, even though it precedes the rise of the cyberspace domain.

The second round table, Convergence of Cyber and Electromagnetic Activities, was moderated by María Teresa Martín, professor of ADP languages and systems at the University of Jaén.

The round table was opened by Manuel Lucena, a professor of computer science and AI at the University of Jaén. He approached the topic from the point of view of information security, whose protection mechanisms have evolved in tandem with the development of the technologies themselves.

Colonel Manuel Sasot of the JCISAT then spoke about the coordination between the two different types of operations, cyberspace and electromagnetic, thus introducing the CEMA (Cyber Electromagnetic Activities) concept. CEMA comprises the integration of the different activities for coordination and synchronisation in cyberspace and the electromagnetic spectrum, while access to such activities by the adversary is denied or degraded.

Following the conceptual framework, Colonel Victor Valero of the High Readiness Land Headquarters, clarified how the CEMA concept is developed in NATO, although there is still no unified doctrine on the subject. To conclude the round table, Colonel Miguel Ángel San Segundo, commander of the 31st Electronic Warfare Regiment, explained how military cyber defence is implemented at the tactical level.

And going from the general to the particular, Colonel Javier Bermejo of the National Institute for Aerospace Technology (INTA) moderated the last round table on "Disruptive and Emerging Technologies in Cyberspace", which focused on enabling technologies.

Lieutenant Colonel Carlos Herrero, from the Army's Logistic Support Command, provided us with a conceptual introduction to quantum computing and the threat it poses to our current cryptography.

Manuel Pérez, from GMV, explained the importance of positioning, navigation and timing (PNT) signals, and how their attack and defence has become a separate chapter of great importance in modern conflicts.

Roberto Amado, expert at S2Grupo, presented the security challenges posed by the growing convergence of the Internet of Things in information technologies and operational technologies. The advantages of hyperconnectivity and the unimpeded flow of data are countered by growing cybersecurity vulnerabilities, which we must mitigate with the use of tools such as AI.

Finally, the presentation by José Martínez, from Jaén-based company INNOVASUR, focused on the application of fifth-generation technologies to the field of military communications and their usefulness in developing capabilities, such as the combat cloud in the tactical environment.

Lastly, before the closing remarks by the Lieutenant General commander of the MADOC, a summary of the conference's conclusions was presented. It emphasised that any successful operational activity now requires the deployment of increasingly complex, interoperable and resilient information and communications technology and systems capabilities, as these have become an essential enabler.

In conclusion, "The Army and Future Challenges" Conference is once again consolidating its position as the primary venue for thought, debate and foresight at the Army's academic level, in perfect synergy with the "Army, Business and Innovation Forum" (Foro 2E+I), which focuses on the technological environment and the industrial sector.