



Next goal to combat the global wave of cyber-attacks: create a common European defense framework

Leaders from the European Parliament, the Joint Cyberspace Command, the business world and academia have defined during DES2024 the keys to shielding against new conflicts in the digital era

Madrid, 13 June 2024. – The potential of exponential technologies has opened the window to new business and development opportunities, although it has also led to the emergence of unprecedented risks, with cyber-attacks being the main protagonists. Thirty-two percent of cyberattacks recorded in 2023 targeted Europe, according to a market report. *"Physical and cyber wars are no longer separate. Cyberspace has no borders, just a playing field where anyone with an Internet connection is a player,"* said **Enrique Pérez de Tena**, Head of IR and cooperation section of the Joint Cyberspace Command, during his participation at [DES – Digital Enterprise Show](#).

The event has analyzed the keys to effectively manage a cyber crisis with a focus on reputation strategy, operational response and communication tactics. In addition, it explored how governments should deal with conflicts that go beyond face-to-face and improve defense strategies. *"EU regulations need to prepare for new forms of warfare,"* said **Timea Lapsanszki**, Policy Advisor for foreign affairs and defense at the European Parliament.

Along similar lines, **Manuel Antonio Fernández-Villacañas**, professor and Director of the Master in Economic Intelligence for Security Management at UNIR, has expressed that the VUCA world (volatile, uncertain and complex) has evolved into the BANI world (fragile, anxious, non-linear and incomprehensible), where disinformation has an important weight. *"Forms of warfare occur all the time at the international level. The '3rd World War 5.0' is very different from previous conflicts"*, so he has considered that we need adapted tools to counter it. At the same time, he advocated promoting public-private collaboration, financial intelligence and cyber-intelligence in order to have new economic warriors. Likewise, *"we need a common European defense through the creation of armed forces and a community defense plan at a conjunctural level"*.

Rosa Kariger, Global Security Analysis & Prospective at Iberdrola, was along the same lines and said that *"there is no common EU regulator in cyberspace to protect against or deal with multiple cyberattacks"*, which is why it is vital to have European coordination. *"The EU has an important role to play in ensuring that we can operate in a more secure and democratic cyberspace,"* he said.

Immature governments for cybercrisis management

"Governments are very used to managing reputational crises. But do they also manage cyber crises? The answer is no". This is how categorical **Iván Monforte**, Head of Communication, Ecosystem and Cybersecurity Culture at the Cybersecurity Agency of Catalonia, was during his speech at DES. Monforte recalled how in March 2023, the second largest hospital in Catalonia suffered a ransomware cyberattack that forced ambulances to be diverted to nearby healthcare centers.



In this context, he has revealed the importance of not only dealing with the incidence at the cybersecurity level, but also with notoriety. *"It has to be managed between the CEO and the communication team, who can understand how the media will act and how the information about the offensive will be published."* The representative of the Catalan organization considered it essential to act quickly in order to gain leadership: *"You have to analyze the 'storytelling' of the hacker group and publish your own story faster than they do. Otherwise, you have to fight against their false narrative and convince people to believe yours"*.

A technological plan B and analog option for protection

In view of the growing escalation of cyber-attacks, **Rosa Kariger**, Global Security Analysis & Prospective at Iberdrola, opened the debate on the need to have a plan B to secure the information and systems of companies, especially at an important time of migration of services and information to the cloud. For his part, **Jesús Mérida**, Iberia's Chief Information Security Officer, assessed as a solution different actions being carried out by many companies. *"They are making backups in very different technologies that cannot be affected by the same technology, or even have part of their services and information in physical resources that ensure their maintenance in the event of any event"*.

[About DES | Digital Enterprise Show \(June 11th-13th, 2024, FYCMA, Málaga\)](#): DES - Digital Enterprise Show is an event of Nebext - Next Business Exhibitions in collaboration with the City of Malaga and the Junta de Andalucía. Along its seven editions, it has become the largest European professional event on exponential technologies and one of the global benchmarks that offers senior management of companies the latest solutions and products to accompany large corporations, SMEs and European Public Administrations towards digital transformation. Throughout 3 days, we combine technology and innovation with digital leadership, technological solutions to improve customer and employee experience, optimization of operational processes and the identification of new business models, services and products for all industries.