WEEKLY BULLETIN OF THE MCCE

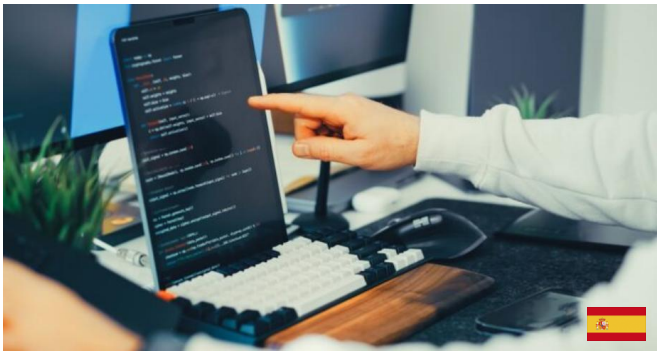
From 14 to 21 August 2026



Spain urgently needs its own industrial cyberdefence ecosystem to guarantee its sovereignty

Spain's technological sovereignty and strategic autonomy cannot be sustained solely on the private or commercial cybersecurity sector. To guarantee deterrence capacity and protection in the military cyber domain, it is essential to articulate a sovereign industrial and technological cyberdefence ecosystem (hub) with sustainable investment programmes in the medium and long term.

+ More information



Security forces update cyberterrorist intelligence

The evolution of the jihadist threat towards self-radicalisation on networks and the use of the Dark Web forces adaptation of investigation methods. Tools such as the undercover computer agent and cyber-patrolling techniques overcome the opacity of encrypted channels under strict judicial control.

+ More information



Digital companies assume greater cybersecurity requirements

The Spanish regulatory framework requires online platforms to implement biometric verification, reinforced authentication and constant code audits. These requirements seek to guarantee the integrity of transactions, the protection of personal data and the prevention of financial fraud.

+ More information

WEEKLY BULLETIN OF THE MCCE

From 14 to 21 August 2026



Connected vehicles pose new risks to security

Modern cars massively collect geolocation, biometrics and telecommunications data through multiple integrated sensors and linked mobiles. This constant accumulation of information turns vehicles into potential vectors of espionage for public bodies and strategic personnel.

+ More information



Fragmented digital footprint facilitates attacks with artificial intelligence

The dispersion of personal data across multiple platforms exposes users to automated cyberattacks through social engineering. The combination of public information on social networks allows cybercriminals to create highly precise impersonation and identity falsification campaigns.

+ More information

Other news

The USA recruits private companies for its active cyberdefence

The United States Government will allow private companies to execute offensive actions to dismantle cybercriminal infrastructure within its security strategy. Participating companies will require prior approval from National Security and a deposit to cover possible sanctions during their operations.

+ More information

Cybersecurity awareness declines among the young population

The majority of young people in Spain suffer digital incidents due to the lack of adequate protection measures on their mobile phones. Although this group uses technology regularly, their knowledge of cybersecurity remains at reduced levels.

+ More information