## THE SENATE WILL STRENGTHEN CYBERSECURITY TO PROTECT MEXICO FROM DIGITAL THREATS

Radio Formula.mx - Alejandro Moreno, president of the Cybersecurity Commission in the Senate of the Republic, warned of more than 40 billion attempted cyberattacks in the first half of 2025 and urged the creation of a General Cybersecurity Law. He cautioned that Mexico faces an alarming scenario in terms of digital security.

## SENATE APPROVES NAVY'S ABILITY TO CONDUCT CYBER DEFENSE AND CYBERSECURITY OPERATIONS – MEXICO

LATINUS - Despite opposition condemnation as a further step toward militarization, the Morena majority in the Senate approved the new Organic Law of the Mexican Navy, which empowers the Secretariat of the Navy (Semar) to intervene against crimes committed in maritime spaces and participate in cyber defense and cybersecurity activities. The bill was approved in general by 68 votes in favor from senators of Morena, the Labor Party (PT), and the Green Party (PVEM), and 32 votes against from the Institutional Revolutionary Party (PRI), the National Action Party (PAN), and the Citizens' Movement. Subsequently, the bill was approved in detail, and since the Senate made no changes to the version passed by the Chamber of Deputies, it was sent to the Executive Branch for promulgation.

## THE DOMINICAN REPUBLIC FOCUSES ON THE GREAT CHALLENGE OF THE DIGITAL ECONOMY

Digital Daily RD - The National Commission for the Defense of Competition (ProCompetencia) kicks off its third annual Competition Week today, an event that promises to dissect the most pressing challenges of the global economy, with an emphasis on the digital transformation of the Dominican Republic. From today until October 31, the Sheraton Hotel will be the epicenter of a debate that seeks to lay the groundwork for fairer, more open, and more innovative markets in the country.

## COP30 INAUGURATES THE ERA OF GREEN DIGITAL DIPLOMACY – BRAZIL

DPL News – COP30, to be held on November 10 in Belém, Pará, Brazil, marks a turning point in the global climate agenda: for the first time, digital transformation will be addressed as a structural driver for the implementation of the Paris Agreement, signed by 195 countries. Under the joint coordination of the Brazilian presidency of the conference and the United Nations, the digital innovation focus was formally incorporated into the event's preparations and featured prominently in the "Solutions Dialogues" series, organized by the UN and COP30 to develop concrete proposals for technological cooperation.

## ECUADOR AND THE EUROPEAN UNION STRENGTHENED THEIR COOPERATION TO COMBAT TRANSNATIONAL CRIME

Lapatilla - Ecuador and the European Union (EU) are seeking to strengthen their cooperation in the fight against transnational organized crime. To this end, they have established the fifth Technical Security Roundtable in the Andean country, where they have analyzed ongoing projects and explored new lines of joint work on issues such as cybersecurity and social violence prevention.

## 65 COUNTRIES SIGN FIRST GLOBAL TREATY AGAINST CYBERCRIME

DPL News – Amid hope and criticism, 65 countries, including Brazil, signed the first UN international treaty aimed at combating cybercrime. The United Nations Convention against Cybercrime seeks to establish a global framework for preventing, investigating, and prosecuting crimes committed using digital technologies. At a ceremony held in Hanoi, Vietnam, the countries formalized their commitment to the agreement, which establishes a framework for international cooperation in combating cybercrime.

## THE HUMAN LINK IN CYBERSECURITY

elrancaguino - In times when technology advances and evolves daily, it's common to think that more powerful firewalls (computer security systems), artificial intelligence platforms, and complex algorithms are enough to protect a company against cyberattacks. But recent data shows that this approach is utopian if it's not accompanied by an internal security culture.

## EPA PUBLISHES CYBER RESPONSE TEMPLATES AND CHECKLISTS TO STRENGTHEN WATER INFRASTRUCTURE SECURITY – USA

Industrial Cyber - The U.S. Environmental Protection Agency (EPA) published new and updated planning tools that water systems across the country can use to help prevent and respond to cybersecurity incidents. These tools will help public water systems protect access to safe water and aid systems in conducting risk and emergency planning for cybersecurity. The agency developed these resources to better address potential vulnerabilities and ensure all water systems have the best information and emergency safeguards available to protect drinking water and wastewater treatment operations.

## NORTH KOREA LED THE WORLD IN NATION-STATE HACKING IN Q2 AND Q3

Cybersecurity Dive - Hackers affiliated with the North Korean government accounted for a plurality of nation-state cyberattacks between April and September, according to a threat report that Trellix published on Thursday. Pyongyang's cyber army has been deploying more sophisticated hacking techniques, including malware-free intrusion methods. North Korean cyberattacks "are deepening and diversifying, from phishing and espionage to employment-based infiltration," Trellix said in its report, "thus demanding a more dynamic, intelligence-led response from organizations and governments alike."

## NVIDIA ANNOUNCES NEW QUANTUM-INTEGRATED COMPUTING ARCHITECTURE

NextGov - NVIDIA will undertake a new partnership to bring advanced artificial intelligence and quantum computing capabilities to the Department of Energy's national laboratory apparatus, the company's CEO, Jensen Huang, announced at the NVIDIA GTC event Tuesday. NVIDIA's NVQLink — a new computing architecture that combines classical computing and early-stage quantum computing systems — aims to offer scientists advanced computing capabilities through access to stabilized qubits.

## HOW CYBERSECURITY AUTOMATION BENEFITS FINANCIAL SERVICES

BizTechMagazine - For financial institutions, cybersecurity risk is a daily operational reality. Banks, insurers and other financial services organizations face a relentless barrage of phishing attempts, ransomware campaigns, insider threats and compliance mandates. For IT and security teams, the sheer volume and velocity of alerts can be overwhelming. That's where artificial intelligence-powered cybersecurity automation, combined with managed detection and response services, are transforming the landscape.

## CAN CYBERSECURITY WITHSTAND THE NEW AI ERA?

WEF - What if the secret to unlocking global business growth wasn't more money but smarter, affordable tools that companies of all sizes could use? Artificial intelligence (AI) is redefining industries, economies and societies, but it is also reshaping the threat landscape at unprecedented scale and speed. Attackers no longer need years of experience to develop advanced tactics: they can access the same AI tools that fuel innovation on the defensive side. Cyberattacks are faster, more targeted and adaptive than many existing defences can withstand.

## HOW MODERN CYBERATTACKS EXPOSE THE RISKS OF OUTSOURCING AND WHAT COMPANIES CAN LEARN

Forbes - Modern cyber incidents are providing powerful, real-world examples of how a cyberattack can cause a domino effect across a company's entire supply chain. For example, what started as a detected intrusion in September 2025 at Jaguar Land Rover (JLR) has led to the possibility of a prolonged production shutdown, with industry experts suggesting the disruption could last into November. Incidents like this highlight a crucial, often overlooked vulnerability: the potential for over-reliance on outsourced IT and security services and the threat posed by sophisticated cybercriminal groups.