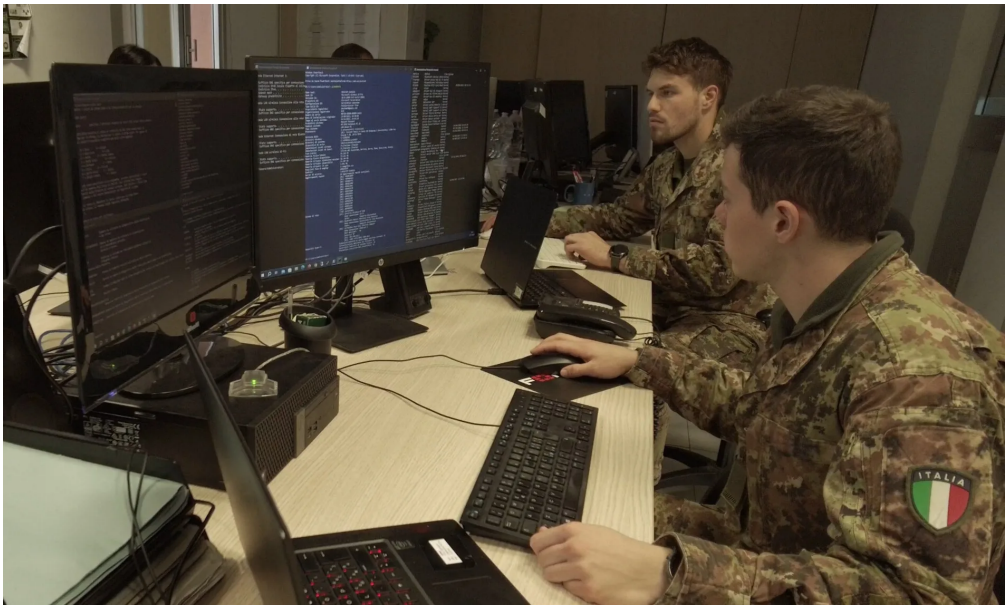


Cybersecurity and Critical Infrastructures: Italy at the Center of the Digital War

Published on 22/08/2025

The European energy sector, and in particular the Italian one, has become one of the main fronts of the global cyber war. This is confirmed by the new **report from the Cybersecurity Competence Center of Maticmind**, which depicts a situation in constant deterioration: in 2024, cyber attacks on the energy sector increased by **40% worldwide**, with a forecast of further growth of **21% for 2025**. Europe alone absorbs almost **60% of global attacks**, and our country is among the most exposed targets.

A Threat to National Security

The digitalization of power grids and the spread of IoT and Scada systems have exponentially expanded the attack surface. Every sensor, every connected node can become a vulnerability exploitable by hostile actors. It is no coincidence that attackers target both large operators and

local entities, which are less equipped defensively.

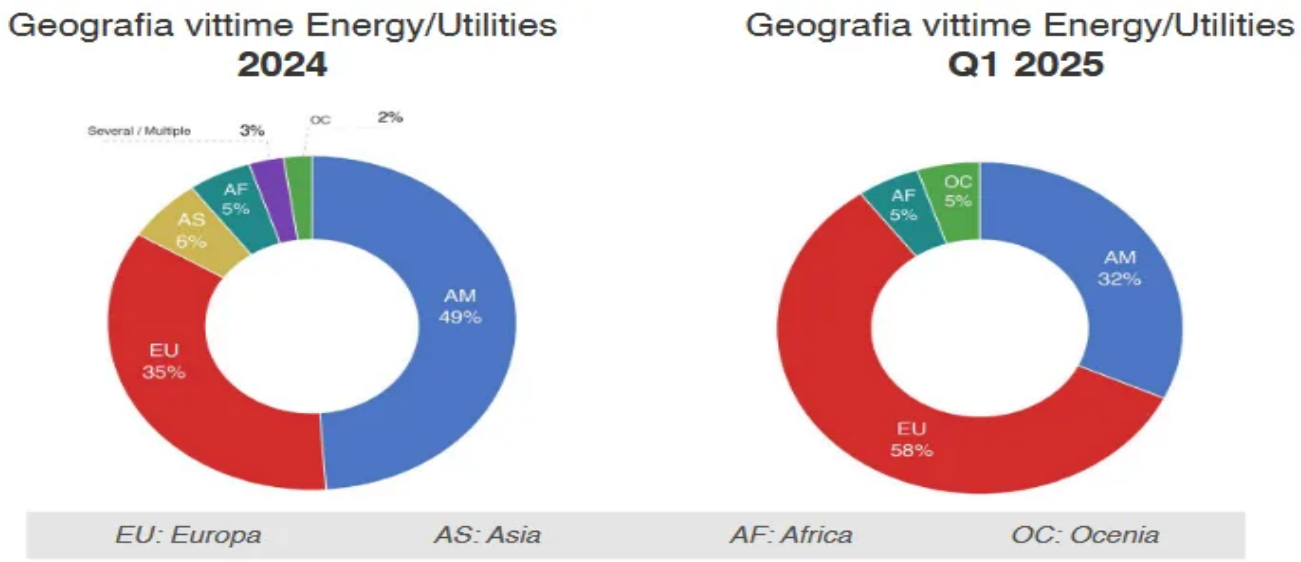
The most alarming data, however, concerns the very nature of the attacks: **over 58% of the incidents in 2025 have political or ideological motivations**. No longer just organized crime seeking economic ransom, but real **hacktivist and state groups** using the cyber domain as a tool of strategic pressure.

Cybersecurity and Critical Infrastructures: Italy at the Center of the Digital War

Italy, a Prime Target

Episodes of **DDoS attacks** have seen an increase of 107% in the first months of 2025, while **ransomware** has marked +64% in Italy and +80% globally in the 2023–2024 biennium. Groups like **LockBit, AlphV, and Qilin** have focused their efforts on energy infrastructures, attracted by the high strategic value of the information and the fragility of industrial systems.

At the same time, although mentions of the energy sector on the dark web have dropped by 75%, analysts report that this is an “apparent retreat”: the discussion has shifted to **closed forums and encrypted environments**, where references to Italy remain very high.



Cybersecurity and Critical Infrastructures: Italy at the Center of the Digital War

European Response and Structural Challenge

The EU has introduced tools like the **NIS2 directive**, which requires reporting incidents within 72 hours and provides for fines of up to 2% of turnover. The **European Network Code** for the security of power grids also aims to raise the level of protection. However, as highlighted by the Maticmind report, the real critical issue remains the obsolescence of infrastructures: in the United States, the average age of electrical systems exceeds 40 years. A similar situation is found in Europe, where legacy systems constitute a vulnerability that is difficult to remedy with mere regulatory compliance.

The Strategy for the Future

Analysts call for a radical change: not just limiting to defense, but adopting a proactive and resilient approach. The main directions:

- **Zero Trust Architecture**, to reduce internal and external risk;
- **Advanced Threat Intelligence**, with the integration of Osint sources and classified feeds;
- **Collaboration between the private sector, institutions, and Armed Forces**, in an integrated defense logic;
- **Digital Twin** to test complex scenarios and simulate attacks before they happen.

As **Pierguido Iezzi, Cyber Security Director of Maticmind**, emphasizes, «energy is no longer just production and consumption. It is geopolitics, economy, and national security.

Resisting is not enough: we must anticipate and react promptly».

In a scenario where the boundary between conventional conflict and hybrid warfare is increasingly blurred, the protection of energy infrastructures represents a **strategic challenge for the country's sovereignty**.

News link: https://www.maticmind.it/soluzioni-it/cyber-security