Cyber Alert: The Hacker Threat to Critical Infrastructure and the Incident at Linate Radar

Published on 30/06/2025

The UK government, along with its international allies, has exposed **a campaign of Russian cyberattacks targeting Western logistics and technology organizations**, including those involved in assisting Ukraine. In this context, Italy must face the growing global cyber threat, which requires an urgent enhancement of its satellite capabilities to strengthen communication resilience.

The Russian cyberattack campaign

The British government and its allies have recently unveiled a series of cyberattacks conducted by the Russian military intelligence service. **Unit 26165, also known as APT 28, has targeted Western logistics and technical companies,** with a particular focus on those involved in assisting Ukraine. These attacks have exploited common techniques such as

credential guessing*, *spear-phishing, and the exploitation of vulnerabilities in Microsoft Exchange systems. Additionally, there has been an attempt by cyber-attackers to monitor humanitarian aid transports destined for Ukraine, using Internet-connected camera systems located at border crossings.

Threats to logistics organizations

According to the National Cyber Security Centre (NCSC) of the United Kingdom, cyberattacks target not only IT systems but also critical infrastructures, including the defense, IT services, and air traffic management sectors. NATO, of which Italy is a part, is particularly vulnerable to these threats, which could compromise the security of operations vital for international support. Logistics companies and critical infrastructure managers must be aware of the growing vulnerability of these sectors.

Nigel Smart, IT and Development Director of Logistics UK, emphasized the importance of strengthening the cyber resilience of supply chains. **Organizations must adopt immediate security measures to address cyber threats**. NCSC recommendations include continuous monitoring of corporate networks to detect suspicious activities, the adoption of multi-factor authentication with robust security methods, and the timely application of security updates. Organizations involved in assisting Ukraine are particularly exposed to these risks and must act without delay.

Cyber Alert: The Hacker Threat to Critical Infrastructure and the Incident at Linate Radar - brigatafolgo

Cyber Alert: The Hacker Threat to Critical Infrastructure and the Incident at Linate Radar - brigatafolgore.net

The incident at Linate radar and the need for satellite protection

A recent failure of the radar at Milan Linate airport has raised concerns about the vulnerability of Italian infrastructures. Although Enav initially attributed the problem to a technical malfunction, the Cyber threat cannot be ruled out. This event highlighted the **need for robust protection of communication infrastructures, such as radar systems and air navigation networks.** The protection of critical Italian infrastructures, particularly those related to national and international security, requires an enhancement of satellite capabilities.

Satellites for IRIDE - brigatafolgore.net

Expansion of satellite capabilities for Italy

In a rapidly changing geopolitical and technological context, **Italy must enhance its satellite capabilities to strengthen communication resilience and protect critical infrastructures. Satellite networks can ensure the continuity of operations in the event of attacks on terrestrial networks.** The growing spread of satellite constellations like Starlink and Eutelsat Oneweb demonstrates how the private sector is investing to ensure secure connections, even in remote contexts. Italy must accelerate the expansion of these capabilities to strengthen its security and that of vital logistical operations.

Conclusions

The protection of critical Italian infrastructures involves strengthening cyber resilience and expanding satellite capabilities. Cyberattacks, particularly those originating from Russia, represent a growing threat to global security. Italy must face these challenges with advanced technological solutions, including the integration of satellite communications, to protect its infrastructures and ensure the security of international operations. The ability to monitor and coordinate operations in real-time is essential to defend the country from future threats.

News link: https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF