PRESS RELEASE

Date Release :
27/03/2025

OMEC Webinar Highlights Cybersecurity Challenges and Solutions for the Energy Sector

Today, OMEC convened a webinar titled "Critical Infrastructure & Cybersecurity in the Energy Sector," bringing together leading cybersecurity experts, researchers, and energy sector professionals to explore the evolving digital threats facing critical infrastructure and to discuss strategies for resilience and risk mitigation.

Held online, the event featured insightful interventions from a distinguished panel of speakers, including: *James Shires, Co-Director, Virtual Routes,, Gabriele Marchionna, Associate Researcher at Luiss Mediterranean Platform and Cyber Strategy Advisorm Ilan Scialom, Research Fellow in Geopolitics, GEODE and Head of Strategy at Zalis, Giuseppe Brando, Head of Cyber Threat Analysis and Research, ENI, Lucrezia Tunesi, Cyber Intelligence Analyst, SNAM.*

Opening the session, James Shires provided an overview of the cyber threat landscape affecting energy systems, emphasizing the diversity of malicious actors and the complexity of cyber operations. He underlined the growing risk to operational technology and the strategic importance of threat-based and agnostic defenses.

Building on this, Gabriele Marchionna drew attention to the Mediterranean's strategic role in both digital and physical energy corridors. He advocated for a Mediterranean pact for cyber resilience, underlining the need for intelligence sharing, common risk assessment standards, and cross-border coordination. Ilan Scialom placed cyber risks within a broader geopolitical context, underscoring how cyber threats can undermine sovereignty and regional stability, particularly as the energy transition accelerates.

The session then turned to corporate experiences. Giuseppe Brando presented ENI's dual approach to cybersecurity and cyber threat intelligence, clarifying their complementary roles and highlighting how external monitoring, scenario planning, and intelligence gathering feed into risk prevention and mitigation strategies.
Lucrezia Tunesi shared SNAM's integrated security approach, combining public-private partnerships, employee training, and advanced monitoring tools. She addressed rising threats like ransomware and deepfakes and how the company has built holistic defenses to protect both infrastructure and trust.
Participants raised questions on employee awareness, deepfakes, AI-generated attacks, and the need for coordinated EU policies. Speakers agreed on the urgent need to upgrade internal protocols, improve public-private cooperation, and embed cybersecurity across governance frameworks.

Next Steps :

- OMEC will circulate a summary of the webinar and presentations to participants and members.
- Speakers have encouraged direct follow-ups for more information.
- A key recommendation was to improve regional cooperation, implement employee training, and prioritize cybersecurity in all energy transition initiatives, particularly in the Mediterranean.

This webinar is part of OMEC's broader efforts to spotlight strategic challenges in the Mediterranean energy landscape and foster dialogue across stakeholders to build a secure, sustainable, and interconnected energy future.

For more information visit : www.omec-med.org

OMEC
32bis boulevard Haussmann
75009 Paris – FRANCE

Tel. : +33 (0) 170 169 120
Fax : +33 (0) 170 169 119
E-mail : omec@omec-med.org