May 2025 Cyber News

On behalf of the Yuval Ne'eman Workshop for Science, Technology and Security, we are happy to share some of the most interesting events and developments that took place in May 2025.

May 9 – Philippines Established New Center to Safeguard Electoral Integrity by Countering Disinformation – The Philippines' Task Force for the Protection of Electoral Integrity (KKK sa Halalan), under the Commission on Elections (Comelec), launched a new Election Threat Monitoring Center to address threats to electoral integrity, including the spread of disinformation. The center brings together experts from various government agencies — such as the Presidential Communications Office (PCO), the Department of Information and Communications Technology (DICT), and the Cybercrime Investigation and Coordinating Center (CICC) — to collect and respond rapidly to reports of false information. Teams will flag false content and submit takedown requests to the platforms where it appears, in coordination with companies such as Google, X, TikTok, and Meta. If disinformation has already spread widely, the task force will issue public rebuttals to correct the record. In parallel, members of the task force will employ dedicated tools to identify AI-generated disinformation.

May 12 – Swedish Report: Doppelgänger Was a Component of Kremlin's Multi-Front Influence Effort – The Swedish Psychological Defence Agency (MPF) released a report based on over 3,100 leaked documents from the Russian IT firm SDA – the company responsible for orchestrating the campaign. The findings reveal that Doppelgänger — previously considered a standalone disinformation campaign — was part of two larger Russian operations between 2022 and 2024: CCI, which aimed to discredit Ukraine by spreading false information about Ukrainian refugees, and CCE, which sought to promote pro-Russian parties ahead of the 2024 European Parliament elections. The report suggests that Western media attention to Doppelgänger may have prompted the Kremlin to increase SDA's funding. It also criticizes the fragmented nature of the West's response, as civil society groups and private firms investigated the campaign separately, limiting overall strategic insight. The authors call for stronger collaboration across sectors, including the establishment of joint centers for strategic analysis. They also recommend a dual approach to countering Russian influence: A strategic response, focused on promoting fact-based, pro-Western narratives, and ~~a~~ proactive strategy, involving the creation of Western equivalents to SDA that would target Russian audiences directly, forcing SDA to divert resources inward.

May 13 – ENISA Launched NEW EU Database for Cybersecurity Vulnerabilities – ENISA unveiled the European Cyber Vulnerability Database (EUVD) — a key milestone in implementing the NIS2 Directive. The database provides reliable, actionable information on cybersecurity vulnerabilities in ICT-based products and services, along with practical mitigation guidance. The EUVD includes three dashboards that provide insights into major vulnerabilities, currently exploited threats, and coordinated responses at both national and EU levels through the CSIRT network. By enhancing transparency and situational awareness, the platform supports better cyber risk management across the EU. The database draws data primarily from EU Member States with Coordinated Vulnerability Disclosure (CVD) policies and will incorporate information from international sources like CISA's KEV catalog. Starting in September 2026, manufacturers will also be required to report vulnerabilities under the Cyber Resilience Act (CRA) via a unified reporting platform. Throughout 2025, ENISA will gather feedback from users and stakeholders to ensure the EUVD meets evolving threat landscapes and operational needs.

May 16 – EON Reality Launches XR-AI Initiative to Boost Romanian Defense Readiness – U.S. tech company EON Reality introduced a strategic initiative to support Romania's role in defending NATO's Eastern Flank, with a focus on the Black Sea region. The project integrates Extended Reality (XR) and Spatial AI to accelerate the development of immersive training tools for Romanian military forces. The initiative includes four key elements: (1) the deployment of the EON-XR platform to rapidly create secure simulations for advanced military systems such as the F-16 fighter jets; (2) the creation of a training and certification pathway for military personnel operating in the Black Sea, using XR scenarios; (3) the use of AI tools to map emerging skill needs and build personalized career tracks for defense and industry professionals; and (4) the rollout of a new curriculum covering technical skills, human-AI collaboration, and operations in complex electronic warfare environments.

Make sure you don't miss the latest on cyber research

Join our mailing list