LESS TALK, MORE SECURITY:

CYBER LESSONS LEARNED FROM MUNICH

OVERVIEW

Awareness of cyber threats has risen dramatically in recent years. Policymakers, industry leaders, and security practitioners now broadly acknowledge that cybersecurity is a core component of national and economic security. That recognition is an important first step — but awareness alone does not automatically translate into meaningful action.

In many cases, growing urgency has produced a cascade of regulations, reporting requirements, and compliance frameworks without clear measures of success. Too often, bureaucratic processes create the illusion that compliance equals security. Real cybersecurity, however, requires actionable steps, operational capability, and measurable outcomes that demonstrably reduce risk.

In February 2026, on the sidelines of the Munich Security Conference and the Munich Cyber Security Conference, Trusted Future and the Center for European Policy Analysis (CEPA) co-hosted a private discussion exploring how to move toward a results-oriented cybersecurity model. The discussion was co-chaired by Admiral Michael Rogers (ret.), former Director of the National Security Agency and Commander of U.S. Cyber Command, and Ieva Ilves, Cyber Policy Advisor to the Government of Ukraine.

Held under the Chatham House Rule, the roundtable brought together cybersecurity experts, policymakers, and practitioners from more than thirteen countries, primarily across Europe.

AVOIDING THE "COMPLIANCE TRAP"

A central theme of the discussion was the need to avoid what participants described as the "compliance trap."

European cybersecurity policy — particularly the implementation of NIS2 — illustrates a growing paradox. While median organizational information security spending in Europe has reportedly doubled (from approximately €0.7 million to €1.4 million), cyber incidents across the EU increased year-over-year according to the ENISA Threat Landscape 2025 report.

Europe is investing more in the administration of cybersecurity but that does not translate into better security.

Efforts such as the EU's proposed Digital Omnibus aim to streamline compliance obligations and reduce regulatory burden. While simplification is welcome, optimizing paperwork does not necessarily improve resilience against adversaries. One participant summarized the challenge succinctly: organizations increasingly hire for compliance expertise rather than defensive capability — despite the fact that effective cybersecurity ultimately depends on operational readiness, not documentation.

Participants noted that an estimated 89 percent of small and medium-sized enterprises (SMEs) expect to need additional cybersecurity staff to comply with NIS2, even as defensive talent shortages persist. At the same time, ENISA data indicates that roughly 59 percent of organizations struggle to fill cybersecurity roles, underscoring a widening capability gap.

The group discussed Ukraine's wartime cyber defense as a contrasting model. Ukrainian institutions have increasingly adopted outcome-based performance metrics similar to private-sector Objectives and Key Results (OKRs), measuring success through real-world impact — for example, reduced service disruption or fraud losses — rather than procedural completion.

This approach may be particularly relevant as digital payment fraud continues to rise across Europe, reaching roughly €4.2 billion annually, or about 20 percent of total fraud losses according to ECB and EBA reporting.

Awareness has grown. What remains missing is execution.

RETHINKING INFORMATION SHARING

Participants agreed that both governments and industry must fundamentally rethink information sharing. Cyber threat intelligence is still too often treated as a competitive or sovereign asset rather than a collective defense mechanism. By contrast, aviation security provides a powerful model: safety and threat intelligence are shared internationally in near real time because airline safety is universally recognized as urgent, operational, and non-competitive.

Cybersecurity deserves the same treatment.

Incident response cooperation — not simply information reporting — should sit at the center of resilience strategies. Faster sharing of indicators, tactics, and mitigation strategies can dramatically reduce the spread and impact of attacks.

Company-to-company collaboration is equally important. The discussion emphasized that cybersecurity is no longer merely an IT risk; it is a core business risk affecting corporate survival, market stability, and national competitiveness. While CEO-level awareness has improved, participants agreed that cyber risk still lacks consistent board-level prioritization across Europe.

European attitudes toward cybersecurity are evolving, but the infrastructure for effective EU-wide operational coordination remains fragmented. Several participants suggested that stronger industry-led initiatives may be required to bridge institutional gaps.

LESSONS FROM UKRAINE — AND EUROPE'S STRUCTURAL CHALLENGES

Ukraine's experience under sustained cyberattack offers important lessons for Europe. Participants stressed that these lessons should be shared more systematically across allied governments and private-sector networks.

A recurring concern was Europe's tendency to default to regulatory solutions when addressing cybersecurity challenges. While regulation plays an important role, an overemphasis on rulemaking can crowd out implementation and measurable outcomes.

Several additional structural challenges were identified:

- Ransomware is increasingly viewed as a national security threat, neither the European Union nor NATO has developed a fully unified operational response framework.
- Europe still lacks a true single market for cybersecurity, resulting in fragmented procurement, certification, and incident response approaches.
- Cyber workforce shortages remain acute, exacerbated by comparatively lower salary competitiveness relative to the United States.
- Unlike the United States, the EU lacks a centralized governmental "buyer" capable of driving security standards through large-scale procurement — a "buy secure, comply secure" model that has influenced U.S. market behavior.

Participants repeatedly returned to workforce readiness as a defining challenge: organizations recognize the need for cybersecurity talent, but recruitment, retention, and training systems are struggling to keep pace with demand.

SECURITY—PROOFING POLICY

Another major theme was the absence of systematic security screening in European technology policymaking.

European legislation routinely undergoes environmental impact assessments, yet comparable security impact reviews are rarely applied to major digital or economic regulations.

The Digital Markets Act (DMA), for example, was developed largely without structured input from operational security experts — a decision some participants believe is reflected in challenges with implementation. More broadly, national security and cyber agencies from EU member states are often consulted late in legislative processes rather than positioned at the front end of policy design.

This contrasts with the United States, where agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Office of the National Cyber Director (ONCD) are routinely integrated into policy discussions affecting digital infrastructure.

Participants also noted that globally recognized standards — including the Common Criteria cybersecurity certification framework long supported by European governments — have not always been fully leveraged in newer legislation such as the Cyber Resilience Act. Existing technical standards, they argued, represent underused resources.

Collaborative policymaking matters. The success of frameworks such as the NIST Cybersecurity Framework demonstrates how government-industry cooperation can create shared ownership, voluntary adoption, and lasting impact.

TO CLOSE

The Munich discussions reinforced a simple conclusion: cybersecurity policy must move from process to outcomes.

European legislation routinely undergoes environmental impact assessments, yet comparable security Europe has successfully elevated cybersecurity onto the strategic agenda. The next phase requires translating awareness into operational capability — measuring success not by regulations written or reports filed, but by attacks prevented, systems kept online, and economic losses reduced.

LESS TALK. MORE SECURITY.