The State of Civilian-Defence Cyber Cooperation in the EU: Strategic Gaps and a Path Forward

Ambassador Timo Koster, Cyber Dacians Strategic Advisor

As cyber threats grow in scale and sophistication, the European Union (EU) faces an urgent need to enhance civilian-defence cooperation in cybersecurity. From Russian cyberattacks on Ukraine to ransomware targeting critical infrastructure, Europe's digital security is under constant threat. However, significant gaps hinder effective civilian-defence collaboration.

Europe's fragmented approach, slow response mechanisms, and limited public-private cooperation leave it vulnerable to cyberattacks. Unlike the United States, where defence agencies work closely with the private sector through federal organisations like the DOD Defense Innovation Unit and the Cybersecurity and Infrastructure Security Agency (CISA), the EU struggles with bureaucratic inefficiencies, uneven capabilities across member states, and insufficient funding for cybersecurity innovation.

To close these gaps, **Europe must develop a more integrated cyber defence ecosystem**, one that fosters intelligence sharing, accelerates public-private partnerships, and builds a rapid-response cyber force. Let's examine the existing challenges and explore opportunities to strengthen EU civilian-defense cyber cooperation.

Strategic Gaps Undermining EU Cybersecurity

1. Fragmentation and Lack of Coordination

Cyber defence responsibilities remain divided among national governments, EU institutions and private entities, leading to inefficiencies and slow responses. While agencies like ENISA (European Union Agency for Cybersecurity) and CERT-EU (Computer Emergency Response Team for EU institutions) play key roles, there is no unified operational command for civilian-defence cyber cooperation. European countries also differ in their cyber defence policies, leading to inconsistent protection levels.

2. Insufficient Threat Intelligence Sharing

Unlike NATO's Cyber Threat Intelligence (CTI) program, the EU lacks a centralized and mandatory intelligence-sharing framework between civilian and military entities. Private-sector companies often hesitate to share cyber threat data due to liability concerns and regulatory complexities, limiting situational awareness and coordinated responses. Moreover, intelligence is shared largely after an attack has taken place, systems are compromised and damage is done, whilst predictive and preemptive capabilities are now available in the private sector.

3. Slow Cyber Crisis Response and Recovery Mechanisms

The EU has no dedicated rapid-response cyber unit capable of countering large-scale cyber attacks in real time. While initiatives like Cyber Rapid Response Teams (CRRTs) exist under PESCO, their deployment remains limited, and they lack clear operational mandates for civilian-military collaboration. The so-called NATO cyber rapid response team has, so far, not been allowed by any individual ally to assist in case of a cyber attack

4. Underinvestment in Cybersecurity Innovation

Europe lags behind the U.S. and China in funding for cybersecurity R&D, particularly in AI-driven threat detection, quantum cryptography, and cyber resilience technologies. The lack of strong defense-industry partnerships means that cutting-edge civilian cybersecurity innovations often do not translate into military-grade cyber capabilities.

5. Regulatory and Procurement Barriers

The EU's complex regulatory landscape slows down procurement and innovation adoption in cybersecurity. Unlike the U.S. Defense Innovation Unit (DIU), which accelerates partnerships with startups and private firms, the EU's procurement process is bureaucratic and discourages rapid technology deployment. Procurement cycles are too long and different in every European capital, to allow start ups and scale ups with cutting edge technology to compete in a sustainable way.

Options for improvement

To address these gaps, Europe must adopt a multi-pronged approach that strengthens governance, accelerates intelligence sharing, and fosters innovation. Despite well known institutional issues NATO-EU cooperation must now deepen further. This will also give credibility to those European NATO members who are under pressure to organize their own defense without American support.

1. Establish a Unified EU-NATO Cyber Command

Develop a centralized EU Cyber Defense Command to coordinate civilian-military cyber operations. It should coordinate national cyber units into a shared operational framework for faster incident response.

Strengthen cooperation with Cooperative Cyber Defence Centre of Excellence (CCDCOE), which is officially neither NATO nor EU, to align strategies and best practices.

2. Set up an Integrated Threat Intelligence-Sharing Framework

Create a European Cyber Intelligence Hub that requires real-time threat data exchange between government agencies, private firms, and military organizations.

Provide legal protections and incentives for companies to share cyber threat intelligence without fear of liability.

Leverage AI-driven analysis to enhance early warning capabilities.

3. Expand Cyber Rapid Response Capabilities

Strengthen Cyber Rapid Response Teams (CRRTs) to enable real-time intervention in major cyber incidents affecting critical infrastructure.

Develop a Joint NATO-EU Cyber Task Force that includes both civilian experts and military cyber units for coordinated responses to hybrid threats.

Conduct regular joint exercises between both organizations, civilian institutions and national military cyber units to improve crisis preparedness.

4. Boost Cybersecurity R&D and Innovation

Establish an EU Cyber Defense Innovation Hub, modeled after the U.S. Defense Advanced Research Projects Agency (DARPA), to accelerate breakthrough cybersecurity technologies.

Increase funding for AI-driven predictive threat detection, quantum encryption, and cyber resilience projects and promote dual-use cybersecurity solutions that benefit both civilian and military applications.

Abolish duplication between NATO (DIANA) and EU (EDA).

5. Reform Procurement and Regulatory Barriers

Streamline procurement rules to fast-track adoption of innovative cybersecurity solutions by defense agencies.

Introduce a Fast-Track Cybersecurity Initiative that provides direct funding to startups and research institutions working on next-gen cyber defense technologies.

Reduce bureaucratic delays in cross-border cybersecurity projects to enhance Europe wide resilience.

Conclusion

Cyber threats do not recognise borders, and neither should Europe's response.

The future of European security depends on a cyber strategy that is well funded, unified, proactive, and innovation-driven.