Informal meeting of the EU Ministers for Telecommunication
on 4-5 March 2025 in Warsaw
Warsaw Call on cybersecurity challenges

Rapid advancements in the field of digital technologies, the rise of new cyber threats and shifts in the geopolitical situation have brought the EU and its Member States to a turning point. As we work to maintain a strong and secure economy, the need for fortified cybersecurity across all sectors has never been more urgent.

Russia's ongoing war of aggression against Ukraine has provided a new strategic context and confirmed the need for the EU, its Member States, and their partners to further strengthen the resilience to face cyber threats and increase our common cybersecurity and cyber defence against malicious behaviour and acts of aggression in cyberspace.

Acknowledging that preparedness and cooperation are indispensable for cybersecurity, we, the ministers in charge of cybersecurity, unanimously:

1. **Call for a timely adoption of the EU Blueprint for cybersecurity crisis management (Cybersecurity Blueprint),** a necessary tool to address the current challenges and complex cyber threat landscape, strengthen existing networks, enhance cooperation, and break silos between organisations, utilising to this end first and foremost existing structures. Emphasise the need **to exercise** the Cybersecurity Blueprint after its adoption.

2. Highlight the need to further **enhance cooperation and information exchange on cybersecurity between** Member States and the EU entities through existing structures.

3. Recall **the need to enhance the civilian-military cooperation** in the cyber domain, in particular covering strategic areas such as situational awareness and crisis management, including EU-NATO cooperation, while fully respecting the principles of inclusiveness, reciprocity, and the decision-making autonomy of both organisations.

4. Call for the continuation and further development of **cybersecurity risk assessments**, including risk scenarios at the EU level for all

essential sectors, initiated by the Nevers Call and the Council conclusions on the development of the European Union's cyber posture.

5. Underline the need for the sustained and strategic **use of the full spectrum of measures within the Cyber Diplomacy Toolbox** and the enhancement of links with the Hybrid and FIMI toolboxes, when appropriate, in order to prevent, deter and respond to malicious cyber activities from state and non-state actors.

6. Reiterate that **the NIS 2 Directive should be the main horizontal legislation on cybersecurity** and strongly caution against fragmentation, duplication or overlap of cybersecurity legislation across the EU by sector-specific initiatives or lex specialis.

7. Stress the need to focus on **the harmonised and innovation friendly implementation of cybersecurity legislation and to find ways for simplification** and burden reduction, such as establishing single entry points for notifications.

8. Underline the need to engage in a regular dialogue and strengthen the EU's **cyber foresight expertise** in order to better anticipate and be prepared for future cyber threats.

9. Stress the need for a **roadmap on new technologies impacting cybersecurity** that would address opportunities and risks, taking into account the Roadmap for the transition to Post-Quantum Cryptography.

10. Emphasise the importance of further harmonising actions towards **investments in cybersecurity**, and of supporting the mission of the European Cybersecurity Competence Centre (ECCC) to create a strong and competitive European ecosystem of cybersecurity companies. Underline the benefit of creating synergies between **defence and civilian investments** and between the research, investment and business sectors in cybersecurity to achieve the greatest benefits.

11. Call for increased efforts **to combat the shortage of cybersecurity professionals in the EU,** for example under the umbrella of the Cybersecurity Skills Academy, including by promoting implementation of the European Cybersecurity Skills Framework, developed by the EU Agency for Cybersecurity (ENISA) and by involving Member States through the ECCC and the NCC Network.

12. Recognise **ENISA's key supportive role** for improving the level of cybersecurity in the EU and the Member States and the need for a strengthened, clearly-defined and focused ENISA's future mandate**.**

13. Encourage stronger and more concerted efforts to enforce **the protection of the submarine cable infrastructure** against threats, both physical and cyber, with due respect to Member States' exclusive competences in particular on national security. We take note of the Cable Security Action Plan presented by the Commission and High Representative, and look forward to its implementation across the whole EU in light of the recent incidents, notably in the Baltic Sea.

This Warsaw Call underscores our dedication to building a more secure and resilient economy and protect our European way of life. We remain focused on assuring that the digital transformation is underpinned by strong cybersecurity foundations rooted in international law and human rights all across the EU.

We call on the EU and its Member States to maintain their commitment to strengthening cybersecurity across all sectors, in order to ensure that the EU's digital infrastructure remains resilient in the face of rapidly evolving threats and new security challenges.