Informal Meeting of the Telecommunications Ministers

Nevers, March 9, 2022

Nevers Call to Reinforce the EU's Cybersecurity Capabilities

The recent cyberattacks which targeted Ukraine in a context of rising geopolitical tensions have shown how important the cyber dimension is in today's conflicts. While recognizing the importance for the EU to strongly support Ukraine's cyber resilience, the possible spillover effect of such cyber-attacks to European networks also highlights the need for the EU to move forward with an ambitious and comprehensive plan for its cybersecurity.

Critical infrastructure such as telecommunications networks and digital services are of utmost importance to many critical functions in our societies and are therefore a prime target for cyberattacks. Providers and operators of such infrastructures and services are key for EU cybersecurity and their role should be leveraged upon by ensuring the cybersecurity of their products and services through regulations and incentives, and by structuring their cooperation with national cyber authorities, where appropriate, to better detect and prevent cyberattacks.

*

Due to the current geopolitical landscape, we wish to undertake immediate cybersecurity reinforcement actions.

Consequently, we, the ministers in charge of telecommunications unanimously:

1. **Acknowledge the importance of strengthening the Union and its Single Market** by enhancing cooperation between the public sector and trusted cybersecurity stakeholders. In addition, Member States will continue to promote an open, free, stable and secure cyberspace in a multi-stakeholder model together with the private sector and the civil society.

2. **Underline that the EU seizes the possibilities offered by the current revision of the Network and information security directive**, striving to better protect its entities from cyber threats. **We are therefore looking forward to the rapid adoption of the NIS2 directive**.

3. **Invite the Commission to finalize the adoption of key proposals, swiftly implement the already existing legislation, notably the operationalization of the Competence Center,** to ensure that digital infrastructures, technologies, products and services are secured, in order to send a clear signal about the EU's ambitions on this topic and to support and help companies rise up to the challenge. Further progress could be made with the

establishment of common cybersecurity standards for connected devices and services through the Cybersecurity Resilience Act. **We therefore wish for a prompt integration of these topics in the upcoming Cyber Resilience Act and for a quick publication.**

4. **Urge the European Union and its Member States to ensure the cybersecurity and resiliency of Europe's communications infrastructures and networks**. In addition, **we invite the relevant authorities, such as the Body of European Regulators for Electronic Communications (BEREC), the European Union Agency for Cybersecurity (ENISA) and the Network & Information Security (NIS) Cooperation Group, along with the European Commission, to formulate recommendations, based on a risk assessment, to Member States and the European Commission** in order to reinforce the communications networks and infrastructures' resiliency within the European Union, including the implementation of the 5G toolbox.

5. **Encourage the strengthening of EU cooperation and reinforce our solidarity and mutual assistance building upon the existing networks**, both at the technical and operational levels with CSIRTs-Network and EU CyCLONe as well as at the political level in the Council, in order to ensure our security and resilience within the digital field.

6. **Increase EU funds to significantly reinforce Member States' efforts in increasing the overall cybersecurity level, for example by encouraging the emergence of trusted cybersecurity service providers**, such as cybersecurity audit and incident response. Encouraging the development of such EU providers should be a priority of the EU industrial policy in the cybersecurity field. In order to both develop our cybersecurity ecosystem whilst reinforcing the cybersecurity of at-risk operators, which would definitely be targeted in the event of a conflict, we believe that such funding would prove efficient and rapidly raise the level of cybersecurity within the EU.

7. **Endorse the implementation of a new Emergency Response Fund for Cybersecurity to be put in place by the Commission**. The current geopolitical landscape and its impacts in cyberspace strengthen the need for the EU to fully prepare to face large-scale cyberattacks. Such a fund will directly contribute to this objective.

8. **Strongly believe that EU institutions, agencies and bodies should take measures to further strengthen their cyber and information security** as the EU has become a key strategic player whose role on the international stage requires to secure its data and networks against cyber threats.

Finally, we reiterate our firm commitment to keep the Ukrainian digital infrastructure and telecommunications networks functional, while bolstering the cyber resilience of Ukraine with both, short and long term assistance.