Council of the European Union

Brussels, 19 October 2017
(OR. en)

13475/17

CYBER 155
TELECOM 242
ENFOPOL 472
JAI 941
MI 733
COSI 237
JAIEX 80
RELEX 881
IND 266

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
Subject:	Cybersecurity 2.0:Follow-up to European Council and Tallinn Digital Summit - Policy debate

The European Commission published an ambitious cybersecurity package in September 2017, which in particular acknowledges exponentially growing cyber threats and the fact that malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. The core elements of the package are the Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, the legislative proposal for a Cybersecurity Act, renewing ENISA's mandate and proposing a certification framework, which should be adopted by the end of 2018, and a Blueprint outlining the European level coordinated response to large-scale cybersecurity incidents and crises.

The Council has rapidly undertaken several steps in response to the Commission's ambition with a view to the actual implementation of the package. Firstly, the work has already started and progressed to consolidate the views of the Council in a set of conclusions dedicated to the Joint Communication, to be approved by the General Affairs Council on 20 November. In parallel, the Presidency has already finalised the implementing guidelines for the Joint EU Diplomatic Response to Malicious Cyber Activities, creating a framework for the EU to use all of its political and diplomatic tools within the CFSP to respond to malicious cyber activities against the EU or its Member States.

Furthermore, the Presidency is set to start the examination of the "Cybersecurity Act" on 20 October, with the aim to report on progress to the TTE Council in December. Meanwhile, the Presidency is closely observing the implementation of the NIS Directive by Member States within the remits of the Cooperation Group and the CSIRTs Network. Progress in both groups' work is critical to the full implementation of the NIS Directive, which lays the ground for proceeding with further work on cybersecurity. Those steps are reflected in the priorities of the cyber programme of the Presidency trio[1], which also charts a way forward in other cybersecurity areas.

Cybersecurity questions were addressed at length by the Heads of States and Government at the Tallinn Digital Summit on 29 September 2017. It was clear that for the leaders in Tallinn, credible and efficient cybersecurity was clearly linked to the development of our Digital Single Market. In his Conclusions from that debate, the Estonian Prime Minister Ratas stated that "*We should make Europe a leader in cybersecurity by 2025, in order to ensure the trust, confidence, and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet*."

[1] WK 7101/2017.

Besides setting this ambition, our leaders emphasised in Tallinn the need to secure the integrity and legitimacy of democratic processes and to clearly focus on the need for the EU to have more of a common and comprehensive approach to cybersecurity, with particular emphasis on:

- specifying the need to work towards state-of-the-art security certification, a single cybersecurity market;
- improving both our national and EU-level preparedness to respond jointly and effectively to large-scale cybersecurity incidents and tackling robustly illegal content online;
- strengthening fight against cybercrime and the criminal use of internet, including by terrorists;
- improving cooperation between Member States on cybersecurity training, education and awareness-campaigns;
- the need to work more closely with the private sector, and the need for investments into secure and novel technologies that could contribute to the security of all sectors of the economy;

Delivery on this ambition requires a clear commitment of political will and resources from both EU Institutions and Member States and, particularly given the sensitivities related to cybersecurity, an active role for Member States in steering the implementation of the cyber package. With that in mind, the Presidency proposes to draw up a specific implementation timeline that would reflect the consolidated vision outlined in the draft Council Conclusions. The trio Presidencies have also agreed to create an Action Plan for the implementation of the cybersecurity package, which should serve as a living document, regularly reviewed. This will allow assessment of the progress at working level (by the Council Horizontal Working Party for Cyber Issues) with further reporting to the Council and its preparatory bodies.

Against this background, Ministers are invited to provide their views on:

- concrete actions that Member States intend to take to accelerate the implementation of the NIS Directive and improve cyber resilience and preparedness;
- the initiatives presented in the cybersecurity package and how they should be prioritised in the Action Plan;
- steps that could be taken to promote investment in cyber security in order to achieve the aims of the Strategy, including from private, public and European sources.