Council of the
European Union

Brussels, 10 April 2018
(OR. en)

7517/18

CYBER 50
COPS 74
JAI 252
COPEN 78
DROIPEN 36
RELEX 267

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
Subject:	Draft Council conclusions on malicious cyber activities - approval

1. At the meeting of the Horizontal Working Party (HWP) on Cyber Issues of 22 February 2018 delegations exchanged views on the follow-up to some recent cyber attacks considering the possibilities envisaged within the Framework for Joint EU Diplomatic Response to malicious cyber activities. During that discussion Member States clearly indicated the importance of providing an appropriate EU response to such activities and flagged different options that could be considered as a course of action.

2. At the HWP on Cyber Issues meeting of 5 March 2018 these options were further elaborated with the assistance of EEAS and discussed by Member States. That discussion pointed out as a preferred option the provision of a EU response in the form of Council Conclusions. EEAS undertook the task to prepare a draft text for Council Conclusions on malicious cyber activities which was submitted to the Council on 19 March 2018[1].

[1] doc. 7309/18.

3. Two rounds of delegations' written comments on the draft text provided by 27 March and by 4 April 2018 respectively, allowed the Presidency to revise and consolidate the initial text according to Member States views[2] in preparation for its discussion and finalisation in the HWP on Cyber Issues meeting of 10 April 2018.

4. During that meeting delegations requested some further minor adjustments of the text which were agreed within the meeting. That made it possible for the Presidency to successfully complete the negotiations on these draft Council Conclusions and prepare the final compromise text[3] which was endorsed by PSC also on 10 April 2018.

5. On this basis, COREPER is requested to invite the Council to approve the draft Conclusions of the Council on malicious cyber activities, as set out in the Annex.

---

[2] doc. 7584/18 and 7584/1/18 REV1.
[3] doc. 7584/2/18 REV2.

ANNEX

Draft Council Conclusions on malicious cyber activities

The EU stresses the importance of a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply for the social well-being, economic growth, prosperity and integrity of our free and democratic societies.

The EU recalls its Conclusions on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities[1] which contributes to conflict prevention, cooperation and stability in cyberspace by setting out the measures within the EU's Common Foreign and Security Policy, including restrictive measures, that can be used to prevent and respond to malicious cyber activities.

The EU expresses its serious concern about the increased ability and willingness of third states and non-state actors to pursue their objectives by undertaking malicious cyber activities and will continue to bolster its capabilities to address cyber threats. The EU recognizes that the interconnected and complex nature of cyberspace requires joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced and calls on these stakeholders to recognize and take their specific responsibilities to maintain an open, free, secure and stable cyberspace.

The EU firmly condemns the malicious use of information and communications technologies (ICTs), including in Wannacry and NotPetya, which have caused significant damage and economic loss in the EU and beyond. Such incidents are destabilizing cyberspace as well as the physical world as they can be easily misperceived and could trigger cascading events. The EU stresses that the use of ICTs for malicious purposes is unacceptable as it undermines our stability, security and the benefits provided by the Internet and the use of ICTs.

[1] 9916/17.

The EU will continue strongly to uphold that existing international law is applicable to cyberspace and emphasises that respect for international law, in particular the UN Charter is essential to maintaining peace and stability. The EU underlines that States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts as expressed in the 2015 report of the United Nations Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

The EU stresses that compliance with voluntary non-binding norms of responsible state behaviour in cyberspace contribute to an open, secure, stable, accessible and peaceful ICT environment. The EU emphasises that States should not conduct or knowingly support ICT activities contrary to their obligations under international law, and should not knowingly allow their territory to be used for malicious activities using ICTs as it is stated in the 2015 report of the UNGGE.

The EU expresses its willingness to continue working on the further development and implementation of the voluntary non-binding norms, rules and principles for the responsible State behaviour in cyberspace as articulated in the 2010, 2013 and 2015 reports of the respective UNGGE, within the UN and other appropriate international fora.