Council of the European Union

Brussels, 3 April 2018
(OR. en)

7584/18

LIMITE

CYBER 51
COPS 75
JAI 260
COPEN 85
DROIPEN 40
RELEX 269

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Council conclusions on malicious cyber activities

Delegations will find in Annex a revised version of the Draft Council conclusions on malicious cyber activities as prepared by the Presidency on the basis of the written comments received.

Written comments on the revised text are welcomed by **4 April 2018 (cob)** to the following email cyber@consilium.europa.eu. The preparation of a new revised version might be considered by the Presidency on the basis of the comments received by that deadline.

The draft Council Conclusions will be discussed at the Horizontal Working Party on Cyber Issues meeting of 10 April 2018.

Deletions are marked with ~~strikethrough~~ and additions with **bold and underlined**.

ANNEX

Draft Council Conclusions on malicious cyber activities

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

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 ~~allows the EU~~ **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~~ **The EU firmly** condemns ~~concrete incidents of~~ malicious use of information and communications technolog**y**~~ies~~**,** ~~such as~~ **including in** Wannacry and NotPetya~~, that~~ **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** ~~increase the risks of instability and misperception of~~ events. **The EU stresses that the use of information and communications technology for malicious purpose is [completely] unacceptable as it undermines the economic and social benefit enabled by the Internet and the use of information and communications technology.**

[1] 9916/17.

The EU emphasises that the respect for ~~the obligations arising out of~~ international law, ~~including~~ **in particular** the UN Charter, and ~~the adherence to~~ **for** voluntary non-binding norms of responsible state behaviour ~~are~~ **is** essential to maintaining peace and stability ~~and promoting an open, free, secure, peaceful and accessible cyberspace. States must meet their international obligations regarding internationally wrongful acts attributable to them~~. In this respect**, the EU underlines that States should not conduct or knowingly support information and communication technology activities contrary to their obligations** under international law~~. In this respect, states must not use proxies to commit internationally wrongful~~**, and should not knowingly allow their territory to be used for malicious** act**ivitie**s using information and communications technolog**y**~~ies, and should seek to ensure that their territory is not used by non-state actors to commit such acts~~.

The EU will strongly continue to uphold the consensus that existing international law is applicable to cyberspace. The EU expresses its willingness to continue working on the **development and** implementation of the **voluntary non-binding** norms of responsible State behaviour in cyberspace as articulated in the 2010, 2013 and 2015 reports of the respective United Nations Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, within the UN and other appropriate international fora.

The EU recognizes that the interconnected and complex nature of cyberspace require joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced and calls on all stakeholders to recognize and take their specific responsibilities to maintain an open, free, secure and stable cyberspace.