Council of the
European Union

Brussels, 19 June 2017
(OR. en)

10474/17

CYBER 98
RELEX 554
POLMIL 77
CFSP/PESC 557

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	19 June 2017
To:	Delegations
No. prev. doc.:	9916/17
Subject:	Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017

Delegations will find in the annex the Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), adopted by the Foreign Affairs Council at its 3551st meeting held on 19 June 2017.

ANNEX

COUNCIL CONCLUSIONS ON A FRAMEWORK FOR A JOINT EU DIPLOMATIC RESPONSE TO MALICIOUS CYBER ACTIVITIES ("CYBER DIPLOMACY TOOLBOX")

The Council of the European Union adopted the following conclusions:

1. The EU recognises that cyberspace offers significant opportunities, but also poses continuously evolving challenges for EU external policies, including for the Common Foreign and Security Policy, and affirms the growing need to protect the integrity and security of the EU, its Member States and their citizens against cyber threats and malicious cyber activities.

The EU recalls its conclusions on the EU Cybersecurity strategy[1], in particular its determination to keep cyberspace open, free, stable and secure where fundamental rights and the rule of law fully apply. It also recalls its Conclusions on Cyber Diplomacy[2], in particular that a common and comprehensive EU approach for cyber diplomacy could contribute to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations.

The EU and its Member States note the importance of the ongoing EU cyber diplomacy engagement and of the need for coherence among the EU cyber initiatives to effectively strengthen the cyber resilience, and are encouraged to further intensify their efforts on cyber dialogues within the framework of effective policy coordination, and emphasise the importance of cyber capacity building in third countries.

2. The EU is concerned by the increased ability and willingness of State and non-state actors to pursue their objectives by undertaking malicious cyber activities of varying in scope, scale, duration, intensity, complexity, sophistication and impact.

---

[1] 12109/13.
[2] 6122/15.

The EU affirms that malicious cyber activities might constitute wrongful acts under international law and 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 internationally wrongful acts using ICTs, as it is stated in the 2015 report of the United Nations Groups of Governmental Experts (UN GGE).

3. The EU recalls its and its Member States' efforts to improve cyber resilience in particular through the implementation of the NIS Directive and the operational cooperation mechanisms provided therein, and that malicious cyber activities against information systems, as defined under EU law, constitute a criminal offence and that effective investigation and prosecution of such crimes remains a common endeavour for Member States.

The EU and its Member States take note of the ongoing work of the United Nations Groups of Governmental Experts on Developments (UN GGE) in the Field of Information and Telecommunications in the context of international security, building on the 2010, 2013 and 2015 reports[3], and are encouraged to strongly uphold the consensus that existing international law is applicable to cyberspace. The EU and its Member States have a strong commitment to actively support the development of voluntary, non-binding norms of responsible State behaviour in cyberspace and the regional confidence building measures agreed by the OSCE[4] to reduce the risk of conflicts stemming from the use of information and communication technologies.

The EU reaffirms its commitment to the settlement of international disputes in cyberspace by peaceful means, and that all of the EU's diplomatic efforts should as a priority be aimed at promoting security and stability in the cyberspace through increased international cooperation, and at reducing the risk of misperception, escalation and conflict that may stem from ICT incidents. In that regard the EU recalls the UN General Assembly call to the UN Member States to be guided by the UNGGE reports' recommendations in their use of ICTs.

---

[3] A/68/98 and A/70/174.

[4] PC.DEC/1106 of 3 December 2013 and PC.DEC/1202 of 10 March 2016.

4. The EU stresses that clearly signaling the likely consequences of a joint EU diplomatic response to such malicious cyber activities influences the behavior of potential aggressors in cyberspace thus reinforcing the security of the EU and its Member States. The EU reminds that attribution to a State or a non-State actor remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of State responsibility. In that regard, the EU stresses that not all measures of a joint EU diplomatic response to malicious cyber activities require attribution to a State or a non-State actor.

5. The EU affirms that measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities and should encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in a long term. The EU will work on the further development of a Framework for a joint EU diplomatic response to malicious cyber activities, guided by the following main principles:

- serve to protect the integrity and security of the EU, its Member States and their citizens,
- take into account the broader context of the EU external relations with the State concerned,
- provide for the attainment of the CFSP objectives as set out in the Treaty on the European Union (TEU) and the respective procedures provided for their attainment,
- be based on a shared situational awareness agreed among the Member States and correspond to the needs of the concrete situation in hand,
- be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity,
- respect applicable international law and must not violate fundamental rights and freedoms.

6. The EU calls on the Member States, the European External Action Service (EEAS) and the Commission to give full effect to the development of a Framework for a joint EU diplomatic response to malicious cyber activities and reaffirms in this regard its commitment to continue the work on that Framework in cooperation with the Commission, EEAS and other relevant parties by putting in place implementing guidelines, including preparatory practices and communication procedures and to test them through appropriate exercises.