



Brussels, 16 May 2017
(OR. en)

7923/2/17
REV 2

LIMITE

**CYBER 48
RELEX 289
POLMIL 31
CFSP/PESC 309**

NOTE

From: Presidency
To: Delegations

Subject: Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")
- approval of the final text

Delegations will find in annex the final text of the draft Council Conclusions as resulting from the discussion during the Horizontal Working Party on Cyber Issues of 12 May 2017 and encompassing the necessary FAC style adaptations as announced at the meeting.

To ease the reading of the document both a clean and a marked version have been prepared.

The draft Council Conclusions are under silence procedure till 17 May 2017, 17:00 h (Brussels time) upon which they will be put on the agenda of PSC and COREPER with a view to their adoption by the Council.

**DRAFT 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 strategy¹, 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 Diplomacy², 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 are encouraged to further intensify their efforts on cyber dialogue 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.

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 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 reports³, 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 OSCE⁴ 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 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, 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.

**DRAFT 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 recallsing its conclusions on the EU Cybersecurity strategy⁵, 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**ing its Conclusions on Cyber Diplomacy⁶, 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 are encouraged to further intensify their efforts on cyber dialogue within the framework of effective policy coordination, and emphasise the importance of cyber capacity building in third countries.

⁵ 12109/13.

⁶ 6122/15.

~~RECOGNISING that cyberspace offer significant opportunities but also pose continuously evolving challenges for EU external policies, including for the Common Foreign and Security Policy,~~

~~AFFIRMING 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, including unfriendly ones,~~

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.

The EU affirmsing 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.

3. The EU recallsing THE EU'sits 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 RECALLING that malicious cyber activities against information systems, as defined under EU law, constitute a criminal offence and 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 reports⁸, and are encouraged to strongly uphold the consensus that existing international law is applicable to cyberspace. ~~RECALLING the~~ **The EU's 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 OSCE⁹ to reduce the risk of conflicts stemming from the use of information and communication technologies.;

The EU reaffirms ~~ing EU's~~ **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 reducing the risk of misperception, escalation and conflict that may stem from ICT incidents.;

~~TAKING 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 reports¹⁰ on international norms of responsible state behaviour in cyberspace and EMPHASIZING that existing international law is applicable to cyberspace,~~

In that regard the EU recalls ~~ing~~ the UN General Assembly call to the UN Member States to be guided by the UNGGE reports' recommendations in their use of ICTs.;

⁸ A/68/98 and A/70/174.

⁹ PC.DEC/1106 of 3 December 2013 and PC.DEC/1202 of 10 March 2016.

¹⁰ A/68/98 and A/70/174.

~~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, and CONCERNED in particular by the cyber-enabled interference in democratic political processes,~~

~~4. The EU stresses~~ing~~ that clearly signaling the likely consequences of a joint EU diplomatic response to such malicious cyber ~~operations~~ 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~~ing~~ that not all measures of a joint EU diplomatic response to malicious cyber activities require attribution to a State or a non-State actor,~~ reminding 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, emphasising 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, noting the importance of the ongoing EU cyber diplomacy engagement and encouraging the EU and its Member States to further intensify their efforts on cyber dialogue within the framework of effective policy coordination and EMPHASIZING the importance of cyber capacity building in third countries,

CONCLUDES,

5. The EU affirms that measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, are ~~the basis~~ **suitable** for a Framework for a joint EU **diplomatic** response to malicious cyber activities **and should encourage cooperation, facilitate** both to mitigation **of** immediate and long-term threats, **and influence the behavior of potential aggressors in a long term** as well as to encourage cooperation. ~~That~~ The EU will work on the further development of a Framework for **a joint EU diplomatic** response to malicious cyber activities, ~~should be~~ 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 INVITES ~~calls on~~ the Member States, the European External Action Service (**EEAS**) and the Commission ~~in order~~ 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** ~~the~~ ~~incoming Estonian Presidency~~ 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 ~~including the relevant parties~~.