Council of the European Union

Brussels, 7 October 2019
(OR. en)

12814/19

LIMITE

PE-QE 110

REPLY TO PARLIAMENTARY QUESTION

From:	Working Party on General Affairs
To:	Permanent Representatives Committee/Council
Subject:	DRAFT REPLY TO QUESTION FOR WRITTEN ANSWER E-001323/2019 - Dita Charanzová (ALDE) 'EU cyber-defence corps'

1. Delegations will find attached:

   – the text of the above question for written answer;

   – a draft reply prepared by the Working Party on General Affairs at its meeting on 3 October 2019.

2. This draft reply is submitted to the Permanent Representatives Committee (Part 1) and to the Council for approval.

Question for written answer E-001323/2019
to the Council
Rule 130
Dita Charanzová (ALDE)

Subject: EU cyber-defence corps

Cyber-warfare in the form of disinformation campaigns, corporate espionage and attacks on critical infrastructures has only increased as more and more devices and systems are connected to the internet.

The Member States have all adopted national strategies to counter this risk, but attacks are often cross-border in nature, with targets in multiple countries.

What is the Council doing to coordinate these national defence measures in order to increase their effectiveness and ensure that there are no gaps in the EU's protection?

What measures are in place to aid a Member State or its companies in the event of an attack, including joint countermeasures with other Member States, and sharing information on threats?

Besides the European Union Agency for Network and Information Security (ENISA), does the Council support the creation of an EU cyber-defence corps under the Common Security and Defence Policy (CSDP) or other intergovernmental measures?

EN
E-001323/2019
Reply

The conclusions on Cyber Diplomacy adopted by the Council on 11 February 2015 gave an ambitious mandate to the EU and its Member States to uphold freedom, security and prosperity in the cyberspace: this includes inter alia, promotion and protection of human rights, application of international law and norms of responsible state behaviour, internet governance, fight against cybercrime, protection of networks and systems of government and critical infrastructure, international cooperation, capacity building, competitiveness in the digital market, strategic engagement with key partners.

On 20 November 2017, the Council underlined the need to address cybersecurity with a coherent approach at national, EU and global level[1]. This call was repeated in the conclusions of the Council and the Member States of 19 February 2019[2]. Furthermore, on 26 June 2018 the Council adopted conclusions on an EU coordinated response to large-scale cybersecurity incidents and crises[3], which called upon the EU and its Member States to jointly work towards the development of European cybersecurity crisis cooperation. This cooperation would put in place the practical operationalisation and documentation of all the relevant actors, processes and procedures within the context of existing EU crisis management mechanisms, in particular the Integrated Political Crisis Response arrangements.

The Union has already taken important steps to ensure cybersecurity, such as the adoption of Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union[4] on 6 July 2016. The Directive provides for the setting up of the Computer Security Incident Response Teams network (CSIRTs network), where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents.

---

1 14435/17.
2 6573/1/19 REV 1.
3 10086/18.
4 OJ L 194, 19.7.2016, p. 1.

More recently, the Council adopted the Regulation known as the EU Cybersecurity Act[5], which reinforces the mandate of the European Union Agency for Network and Information Security (ENISA). With this renewed and permanent mandate, ENISA will be able to play an important role in improving the EU's resilience against cyber-attacks, notably by capacity-building but also by exchanging information and providing analyses.

Furthermore, at the request of one or more Member States, ENISA shall assist Member States in the assessment of incidents having a substantial impact by providing expertise and facilitating the technical handling of such incidents. It can also provide support to ex-post technical inquiries. Moreover, ENISA provides the secretariat for the CSIRTs network.

Cyber-attacks often have an external dimension and in this respect the Council refers to its conclusions of 19 June 2017 on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (cyber diplomacy toolbox). The cyber diplomacy toolbox sets out measures, including restrictive measures, which can be used to prevent and respond to malicious cyber activities. On 28 June 2018, the European Council, in its conclusions, called on institutions and Member States to implement the measures referred to in the Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats[6], including the work on attribution of cyber-attacks and the practical use of the cyber diplomacy toolbox[7].

---

5 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (OJ L 151, 7.6.2019, p. 15).

6 Join (2018) 16 final.

7 EUCO 9/18.

On 18 October 2018, the European Council adopted conclusions calling for work on the capacity to respond to and deter cyber-attacks through EU restrictive measures to be taken forward[8]. As a follow-up, on 17 May 2019, the Council adopted the necessary legal acts establishing a framework[9] for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. Where deemed necessary to achieve CFSP objectives in the relevant provisions of Article 21 of the Treaty on European Union, these acts also allow for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations.

---

[8] EUCO 13/18.

[9] Council Regulation (EU) 2019/796 (OJ L 129I, 17.5.2019, p. 1) and Council Decision (CFSP) 2019/797 (OJ L 129I, 17.5.2019, p. 13) of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.