Council of the European Union

Brussels, 26 June 2018
(OR. en)

10496/18

CYBER 151
COPEN 231
COPS 238
COSI 163
DATAPROTECT 140
JAI 698
JAIEX 73
POLMIL 98
TELECOM 203
DAPIX 206

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	26 June 2018
To:	Delegations
No. prev. doc.:	10072/18
Subject:	EU External Cyber Capacity Building Guidelines - Council conclusions (26 June 2018)

Delegations will find in the annex the Council conclusions on EU External Cyber Capacity Building Guidelines, adopted by the General Affairs Council at its 3629th meeting held on 26 June 2018.

ANNEX

COUNCIL CONCLUSIONS ON EU EXTERNAL CAPACITY BUILDING GUIDELINES

The Council of the European Union,

1. RECOGNISING the importance of a global, open, free, stable and secure cyberspace for the continued prosperity, growth, security, connectivity and integrity of our free and democratic societies and STRESSING the importance of protecting the rule of law, human rights and fundamental freedoms in cyberspace;

2. REITERATING that cyberspace is important for continued global development and prosperity. Cybersecurity is therefore a global challenge, which requires international engagement, collaboration and coordination in the EU and necessitates effective global cooperation amongst all stakeholders to preserve a functioning and stable cyberspace;

3. EMPHASISING the importance of access to and unhindered, uncensored and non-discriminatory use of open and secure information and communication technology (ICT) for fostering open societies and enabling economic growth and social development globally;

4. AFFIRMING that existing international law, including the UN Charter and international conventions such as the Council of Europe Convention on Cybercrime ('Budapest Convention') and relevant conventions on international humanitarian law and human rights, such as the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, applies in cyberspace;

5. UNDERSCORING the importance of all stakeholders' involvement in the governance of the internet, including academia, civil society and the private sector;

6. RECALLING its Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[1], on the EU Cybersecurity Strategy[2], on Cyber Diplomacy[3], on Internet Governance[4], on Security and Defence in the context of the EU Global Strategy[5], on mainstreaming digital solutions and technologies in EU development policy[6] and on Digital for Development (D4D)[7]; as well as the EU Human Rights Guidelines on Freedom of Expression online and offline[8], and the Joint Framework on countering hybrid threats[9];

7. STRESSING the role of cyber capacity building in partner countries and regions as a strategic building block of the EU's cyber diplomacy efforts to promote and protect human rights, gender digital equality, the rule of law, security, inclusive growth and sustainable development, and as a key dimension of the EU's Digital4Development strategy;

---

1 14435/17 and (Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN (2017) 450 final)).

2 12109/13 and 6225/13 (Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (COM JOIN (2013) 1 final)).

3 6122/15.

4 16200/14 and 6460/14 (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Internet Policy and Governance: Europe's role in shaping the future of Internet Governance (COM(2014) 72 final)).

5 9178/17.

6 14682/16.

7 14542/17.

8 9647/14.

9 7688/16 (Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats: A European Union Response).

8. RECOGNISING that cyber capacity building mainly entails systematic efforts with partner countries and relevant organisations to enhance national, institutional and organisational capacities which improve the resilience of critical digital services and networks as well as the protection of critical information infrastructure; support criminal justice reforms to address cybercrime; fight the use of the Internet for terrorist purposes; improve cyber-security skills and competencies; and facilitate awareness raising and effective cooperation on these issues at national, regional and international level;

9. RECALLING that cyber capacity building is becoming one of the most important topics on the international cyber policy agenda, as demonstrated in relevant outcome documents, including in the reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[10]; in the UN General Assembly Resolution on ICT for Development[11]; in the World Summit on the Information Society (WSIS+10) outcome document[12]; in the Doha Declaration of the 13th UN Congress on Crime Prevention and Criminal Justice[13]; as well as within the Global Cyberspace Conference or 'London Process', which in 2015 created the Global Forum on Cyber Expertise (GFCE) and led to the adoption of the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building[14] in 2017;

10. NOTING the increasing importance placed on cyber capacity building by the relevant international, inter-governmental and regional organisations, such as the Council of Europe (CoE), the Organisation for Security and Co-operation in Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the UN and its specialised organisations and agencies, the Commonwealth, the African Union and its Regional Economic Communities, the Organisation of American States (OAS), and the Association of Southeast Asian Nations (ASEAN);

---

10 A/65/2013 (2010), A/68/98 (2013), A/70/174 (2015).
11 71/212.
12 70/125.
13 A/CONF.222/17 (2015).
14 Available at: https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique.

11. WELCOMING the work on strengthening the civilian aspects of CSDP especially by incorporating therein cyber security activities with a focus on building resilience and capacities of third countries;

12. RECOGNISING that cyber capacity building efforts are important in order to develop the minimum capacities that are necessary for the implementation of regional cybersecurity confidence building measures (led by the OSCE, the ASEAN Regional Forum and the OAS), as well as for the implementation of the rules, norms and principles of responsible state behaviour as set out-in the 2013 and 2015 reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE);

13. ACKNOWLEDGING the EU-NATO cooperation on cybersecurity and defence including coordinating the support to building the capacities of partners to counter cyber threats in full respect of the principles of inclusiveness, reciprocity and decision-making autonomy of the EU and in accordance with its relevant Conclusions, including those of 6 December 2016 on the implementation of the Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation[15];

14. CONSIDERING the growing demand for external cyber capacity building efforts and TAKING INTO ACCOUNT the increasing number of stakeholders globally involved in such processes, which creates opportunities for synergies and burden-sharing but also poses challenges in terms of coordination and coherence;

[15] 15283/16.

15. RECOGNISING that the EU's external cyber capacity building efforts serve multiple objectives which are mutually reinforcing, most notably: supporting cyber resilience building in partner countries that contributes to an improved global digital ecosystem; fostering strategic alliances aimed at supporting the notion of a global, open, free, stable and secure cyberspace in line with the EU's core values and principles, the rule of law, human rights and fundamental freedoms; encouraging the creation of formal and informal cooperation frameworks between partner countries and regions and the EU and its Member States; and promoting the EU's development commitments and the implementation of the 2030 Agenda for Sustainable Development;

HEREBY

16. ACKNOWLEDGES the leading role that the EU and its Member States have played in global cyber capacity building efforts and its approach of systematically linking these efforts with its Common Foreign and Security Policy and development policy, in particular since the adoption of its 2013 Cybersecurity Strategy;

17. EMPHASISES the importance of promoting the EU's political, economic and strategic interests in the face of expanding and complex international discussions on cyber issues, and ensuring that the international cyber capacity building and cooperation efforts led by the EU and its Member States follow overarching guidance to ensure a coherent, holistic and effective approach which also supports the EU's broader digital, development and security and strategic autonomy[16] agendas;

[16] 13202/16.

18. RECALLS the principles of the EU approach to cyber diplomacy at global level as defined in the 2015 Council Conclusions on Cyber Diplomacy, and REITERATES that the EU's core values and principles for cybersecurity – as defined in the 2013 EU Cybersecurity Strategy – should serve as the underlying framework for any external cyber capacity building action, to ensure that it:

- incorporates the understanding that the existing international law and norms apply in cyberspace;
- is rights-based and gender-sensitive by design, with safeguards to protect fundamental rights and freedoms;
- promotes the democratic and efficient multi-stakeholder internet governance model;
- supports the principles of open access to the internet for all, and does not undermine the integrity of infrastructure, hardware, software and services;
- adopts a shared responsibility approach that entails involvement and partnership across public authorities, the private sector and citizens and promotes international cooperation;

19. UNDERLINES that lessons from development cooperation[17] should be taken into account in external cyber capacity building efforts in order to enhance their effectiveness and sustainability by:

- ensuring ownership of the development priorities in relation to cyber resilience by the partner countries;

[17] Set out in the Global Partnership for Effective Development Cooperation ('Busan Partnership') outcome document, 1 December 2011.

- focusing on sustainable results through the promotion of broader policy, legal and technical reform processes instead of ad hoc, one-off activities;

- recognising the need for promoting partnerships, namely the participation of all stakeholders, in recognition of the diversity and complementarity of their functions;

- ensuring that trust, transparency, accountability and shared responsibility are the driving forces behind any assistance;

20. STRESSES the need to prioritise the EU's cyber capacity building efforts in its neighbourhood and in developing countries with fast connectivity growth, as indicated in its Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[18] and in general to pursue evidence-based prioritisation on the basis of internet access growth statistics, strategic interests and threat assessments such as Europol's Internet Organised Crime Threat Assessment (iOCTA) and ENISA's Threat Landscape Reports, with the aim of closing the cyber capability gap;

21. REITERATES that external cyber capacity building initiatives by the EU and its Member States should prioritise addressing cybercrime and increasing cybersecurity in partner countries and regions, with a focus on reforms across the main pillars of cyber resilience, namely by supporting an overarching strategic framework, promoting legislative reforms and increasing the capacities of the criminal justice system, developing and increasing incident management capabilities, developing education, professional training and expertise in this field and promoting cyber hygiene and awareness as well as a culture of security assessment of digital products, processes and services, in compliance with European and international standards and best practices and applying a whole-of-society approach;

---

[18] 14435/17 (Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN (2017) 450 final)).

22. CALLS ON the EU and its Member States to promote, through their capacity building actions, the Council of Europe Convention on Cybercrime ('Budapest Convention') as the international effective legal standard for developing national cybercrime legislation in partner countries, and to develop the necessary investigation and prosecution capacities on this basis; to cooperate in fighting cybercrime at global level within the existing international framework offered by the Budapest Convention; and to use elements of the Directive on security of network and information systems (NIS Directive) on national capabilities and critical sectors as inspiration for the development of cybersecurity legislation in partner countries;

23. NOTES that cyber capacity building is an integral part of mainstreaming digitalisation into EU development policy as identified in its Conclusions[19] and in the Commission Staff Working Document on 'Digital4Development: mainstreaming digital technologies and services into EU Development Policy'[20]; and RECOGNISES that due to the cross-cutting aspects of electronic evidence and cyber-enabled systems, infrastructure and services, a holistic and consistent rights-based approach is necessary also on other relevant external capacity building activities that touch on justice and security, in particular in counter-terrorism and organised crime programmes;

24. STRESSES the need to ensure coherent and efficient use of resources by the EU and its Member States, to make full use of the relevant EU external financial instruments and programmes, and to leverage the expertise of EU Member States' national competent cyber authorities, the EU's relevant specialised agencies (notably ENISA, EC3 at Europol, Eurojust, CEPOL and eu-LISA), and networks (e.g. European Cyber Crime Training and Education Group, European Judicial Cybercrime Network) as well as existing expert, academic, technical and industry networks (for example GÉANT, FIRST and Meridian);

---

[19] 14682/16, 14542/17.
[20] SWD(2017)157.

25. CALLS ON the EU and its Member States to adapt their capacity building actions in partner countries and regions according to local specificities and work towards creating self-sustainable local expert hubs with the support of EU expertise and good practices; and ENCOURAGES inter-regional, South-South and triangular cooperation and a differentiated approach according to countries' cyber maturity when implementing cyber capacity building actions;

26. ENCOURAGES the EU and its Member States to continuously engage with key international and regional partners and organisations as well as with civil society, academia and the private sector in this field with the aim of avoiding duplication of effort given the limited resources; and WELCOMES the coordination initiative by the Global Forum of Cyber Expertise, as well as efforts to elevate the issue by international convening fora such as the World Economic Forum, the Internet Governance Forum and others;

27. WELCOMES the proposal to set up an EU External Cyber Capacity Building Network to mobilise the collective expertise of EU Member States for EU-funded external cyber capacity building programmes, support effective coordination of EU-funded external cyber capacity building activities, and increase training opportunities in light of proliferating initiatives in partner countries and regions and the growing demand for cyber-related training; cooperating with and complementing the GFCE network;

28. WELCOMES the development of 'operational guidance' by the Commission on 'the EU's Cyber Capacity Building in third countries'[21] as well as on 'Integrating the rights-based approach in EU external cooperation actions addressing Terrorism, Organised Crime and Cybersecurity'[22];

---

21 Final study to be published in June 2018.

22 Study available in English and French at https://ec.europa.eu/europeaid/operational-human-rights-guidance-eu-external-cooperation-actions-addressing-terrorism-organised_en

29. CALLS ON the European External Action Service and the Commission to continue the prioritisation and exchange of information on cyber capacity building activities in their bilateral dialogues with strategic partners as well as at relevant international and regional fora;

30. CALLS ON the Commission to regularly report to the Horizontal Working Party on Cyber Issues on external cyber capacity building, and on Member States to share information on their respective efforts.