Council of the
European Union

Brussels, 13 September 2019
(OR. en)

12196/19

CYBER 255
CFSP/PESC 685
COPS 276
RELEX 835
JAIEX 135
TELECOM 299
POLMIL 88
COPEN 352
JAI 934
ENFOPOL 395

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7693/1/19
Subject:	EU contribution in response to the UN SG call for views on "countering the use of information and communications technologies for criminal purposes"

Delegations will find in Annex the text on the abovementioned subject as agreed by the Horizontal Working Party on cyber issues.

ANNEX

UNGA Resolution

"Countering the use of information and communications technologies for criminal purposes"

EU Contribution

In December 2018, the UN General Assembly adopted a Resolution on "Countering the use of information and communications technologies for criminal purposes". The Resolution "*Requests* the Secretary-General to seek the views of Member States on the challenges they face in countering the use of information and communications technologies for criminal purposes".

In response to the invitation to provide such information to UNODC, the European Union (EU) submits the following contribution:

1. On the global challenges in fighting Cybercrime

Cybercrime is an evolving challenge affecting every country. In order to efficiently address cybercrime, it is necessary to:

1. Maximise the number of countries with adequate, compatible cybercrime-related domestic legislation that supports also international cooperation.
2. Build the cooperation mechanisms, trust and skills to share data to investigate, prosecute and reduce cybercrime.
3. Make sure that no safe havens exist for criminals and increase the capacities of law enforcement and judiciary authorities for effective investigations, prosecutions and convictions of cybercriminals.

To ensure minimum standards for cyber legislation across the European Union, EU Member States have agreed a set of instruments, providing common definitions for criminal offences: a Directive on attacks against information systems, a Directive on combating the sexual exploitation of children online and child pornography, a Framework Decision on combating fraud and counterfeiting.

Many of the issues identified in the Draft Comprehensive Study on Cybercrime (UNODC, February 2013) remain valid: under-reporting, cooperation with private partners and more in general capacity of law enforcement authorities to deal with the continuous proliferation and sophistication of transnational cybercriminal threats.

The European Union has created a specialised structure in Europol: the European Cybercrime Centre (EC3). Six years after its establishment, it has made a significant contribution to the European Union Member States' efforts to thwart cybercrime through an agile crime-fighting model. It is necessary to involve prosecutors in the cybercrime cases from the earliest stages as possible. Establishment of specialised networks, such as European Judicial Cybercrime Network (EJCN) is considered beneficial.

In the framework of the European Union, on 17 April 2018 the Commission presented legislative proposals to improve cross-border access to electronic evidence in criminal investigations.

EU Member States also take part in the current negotiations on a second additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), which will address, among other issues, the need for a better access to electronic evidence.

Considering that any type of offence may entail electronic evidence, all judges, prosecutors and investigators may be confronted with e-evidence and need to have at least basic skills in this respect.

Many countries still need to adopt at least some specific procedural powers to secure electronic evidence and develop the necessary criminal justice capacities to apply procedural powers in practice: capacity building should thus remain the priority for the future.

2. On technical assistance

As the Draft Comprehensive Study on Cybercrime notes, there is a broad consensus that efforts to build capacity to address cybercrime is essential.

The Global Programme on Cybercrime from the UNODC exists already and engagement of all UNODC Members is of the essence. Alongside the UNODC's Global Programme, there are a number of other capacity building programmes that we support, such as those run by the Council of Europe and the EU. For instance, through its programme Global Action on Cybercrime (GLACY) and its extension (GLACY+), the EU has invested 12 MEUR since 2013 and, in partnership with the Council of Europe, has been supporting 9 countries with ambitious and comprehensive capacity building measures, encompassing institutional, legal and operational perspectives that also create the enabling environment for these countries to further serve as regional hubs of South-South cooperation and share experiences with their neighbours. Moreover, the EU has also launched region-specific programmes jointly with the Council of Europe.

The EU believes that we need to work harder to ensure that all capacity building projects are effectively targeted and coordinated to avoid duplication; appropriately designed and sequenced to meet the needs of international cooperation and to ensure sustainable results; as well as efficiently evaluated to measure their impact.

3. On options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime

Cybercrime is a global problem and the Council of Europe Budapest Convention, which represents a valid model for national legislations and a valuable framework for international cooperation. In our interconnected cyber-world, every nation needs assistance from other countries to fight cybercrime. The Budapest Convention, being open to the accession of countries that are not parties to the Council of Europe, provides a flexible instrument of choice for doing so.

The EU does not support calls for development of a new international instrument on cybercrime.

4. On the UN Open-ended Intergovernmental Expert Group on Cybercrime

The UN Open-ended Intergovernmental Expert Group on Cybercrime is and should remain the main process at the level of the United Nations on the topic of cybercrime at least until 2021.

The Intergovernmental Expert Group has yielded results, including with regard to legislative reforms based on existing international standards and in particular in terms of capacity building.

The past six years have shown good progress in terms of legislative reforms, in particular where countries have made use of existing international standards.

These changes need to be taken into account and the work of the Intergovernmental Expert Group is of paramount importance for updating the Draft Comprehensive Study on Cybercrime that was presented in 2013: much progress has been made and examples of good practice are available since the draft Study was published.

Many organisations have set up capacity building programmes. These efforts need to continue and be further expanded.

The EU would suggest that the UN via UNODC deliver these goals and that UNODC is guided towards focusing on providing assistance and support in specific areas where this can have a real impact against the threat of cybercrime; such areas are:

1. Raising police and law enforcement skills for both general and specialist training;
2. Developing technical assistance in developing nations;
3. Analysis of gaps in international cooperation to identify priority areas;
4. Support for public awareness campaigns to strengthen crime prevention and build civil society and business cooperation with law enforcement;
5. Strengthening existing operational mechanisms such as the 24/7 network;
6. Collecting data on cybercrime threats;
7. Collecting best practices and case studies in tackling cybercrime (with UNODC as a repository).