035382/EU XXVI. GP
Eingelangt am 19/09/18

Council of the
European Union

Brussels, 19 September 2018
(OR. en)

12186/18

CYBER 195
CFSP/PESC 828
COPS 321
RELEX 750
JAIEX 109
TELECOM 292
POLMIL 140

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	12095/18
Subject:	EU Lines to take on cybercrime developments in the framework of the UN

Delegations will find in annex the "EU Lines to take on cybercrime developments in the framework of the UN" endorsed by the COREPER of 17 September 2018.

www.parlament.gv.at

ANNEX

EU Lines To Take on cybercrime developments in the framework of the UN

– The EU welcomes the progress achieved in the field of addressing cybercrime worldwide by UNODC, CoE, Interpol and other international organisations and fora. The UN Intergovernmental Expert Group on Cybercrime (UNIEG) has been a major forum for UN Member States to discuss relevant issues in inclusive manner.

– Meetings of the UN CCPCJ and UN Congresses for Crime Prevention and Criminal Justice have effectively addressed the need to step up the fight with cybercrime, resulting in several resolutions adopted by the CCPCJ. These provide excellent guidance for the UN Member States for further efforts in combating cybercrime.

– Therefore, the creation of parallel discussion on cybercrime matters in the UNGA in New York will not add value to the process and might be counterproductive to the efforts achieved by UNIEG so far. It will be unfortunate to fragment the efforts, and divert the related discussions from the cybercrime expert community in Vienna.

– Cyber-crime is already addressed in the annual GA resolution on Crime Prevention, tabled (by IT) under the GA agenda item on Crime Prevention and Criminal Justice, and in the Secretary-General's annual report to the GA on crime prevention. There is no need for a new GA resolution, SG report, or GA agenda item dealing specifically with cyber-crime. The GA agenda is already overloaded, and it would be much more efficient to continue to address cyber-crime issues under existing agenda items and through regular resolutions and reports. The language on cyber–crime on those texts could potentially be strengthened, rather than launching duplicative new initiatives.

www.parlament.gv.at

– The EU recognizes the need to further advance capacities of law enforcement and judicial authorities, to develop national cybercrime legislation and to promote international cooperation in the fight with cybercrime globally.

– As urgent priority, it will be necessary to promote international cooperation to investigate and prosecute cybercrime, and maximise the number of countries with comprehensive domestic cybercrime legislation that supports international cooperation.

– The EU will continue its current efforts, in cooperation with other international organisations, to support the development of national cybercrime legislation, and increase capacities of law enforcement and judicial authorities in its partner countries. In recent years, the vast majority of the UN Member States have undertaken reforms to adopt national legislation that criminalises cybercrime.

– Meetings of the UN CCPCJ and UN Congresses for Crime Prevention and Criminal Justice have effectively addressed the need to step up the fight with cybercrime, resulting in several resolutions adopted by the CCPCJ. These provide excellent guidance for the UN Member States for further efforts in combating cybercrime.

– The majority of the UNIEG members recognised that the existing international law, including the Council of Europe Convention on Cybercrime (Budapest Convention) and the UN Convention on Transnational Organised Crime provide a sufficient legal framework for international cooperation in fighting cybercrime, and standards for national legislation.

– The EU will not support the creation of new international legal instruments for cybercrime. There is no minimum consensus found on the need for new instrument among the UN Member States. Furthermore, any discussion on new international legal framework might jeopardise current work on technical and judicial assistance in developing countries.

www.parlament.gv.at

– The Budapest Convention, being also open to the accession of countries that are not parties to the Council of Europe, has proved to be a valid framework for national legislation and international cooperation. The Convention serves as an effective standard, which is also technology-neutral, so that the substantive criminal law offences may be applied to current and future technologies.

– Some two thirds of the UN Member States use the Budapest convention as a guideline or a reference document when preparing domestic legislation. The Convention has currently 71 signatory countries. Among the G77 group, Argentina, Bosnia and Herzegovina, Cabo Verde, Chile, Columbia, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Panama, Paraguay, Peru, Philippines, Senegal, South Africa, Sri Lanka, Tonga and Tunisia are parties which have ratified or been invited to accede the Convention.

– Due to urgent need to focus on actual capacity building of law enforcement and judiciary authorities in developing countries, the EU will pledge additional funding to global efforts in fighting with cybercrime in 2019-2020 within its several assistance instruments.

***

www.parlament.gv.at

BACKGROUND

RF draft resolution to UNGA "Countering the Use of Information and Communication Technologies for Criminal Purposes" attempts to reopen the discussion on the need for a new UN cybercrime instrument. As a resurfacing theme in the UNIEG, CCPCJ and other fora, it is now proposed to be brought up in the UNGA format. The most serious issue with changing the format from Vienna to New York is the possible over-politisation of cybercrime topic by UNGA. This might put to the risk the current collective EU/CoE/Europol and UNODC efforts to assist developing countries, which has been very successful so far. In recent years, some two thirds of the UN member countries have started to develop their domestic cybercrime legislation, and many of them receive assistance from the EU.

The draft resolution that has been circulated by RF does not specifically mention the need for a new instrument, but it is made clear in the accompanying memo that this is the ultimate goal of the initiative. The draft resolution requests a new SG's report dealing specifically with Cyber-crime, and the inclusion of cyber-crime on the agenda of the 74th session of the General Assembly (2019-2020.) GA agenda items usually have quite a broad thematic focus, and it would be unusual to have a dedicated item dealing specifically with cyber-crime when this could be addressed under the agenda item on crime-prevention Rather than tabling a new resolution and requesting a new SG's report, it would be preferable if RF would seek to strengthen language on cyber-crime issues in existing texts, including the IT-led resolution on crime prevention.

Budapest Convention as a global framework. With some 20 developing and non-European nations to accede the Budapest Convention, the latter has become a global instrument of reference. There is no need to divert efforts to parallel discussions on the new UN convention. In addition, the draft proposal by the RF includes elements that go beyond the cybercrime, and might be used for legitimizing censorship and content control.

www.parlament.gv.at

Cybercrime is a global problem and the Council of Europe '*Convention on Cybercrime' (known as the Budapest Convention)*, which took many years to develop still represents a valid model for national legislations and a valuable framework for international cooperation. 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 Budapest Convention is the best model for countries seeking to develop their own national legislative approach. The Budapest Convention is an effective template that allows countries to identify what they need to put in place to be able to work effectively with other countries. Most countries are already motivated to have and will establish comprehensive legislation that supports effective international cooperation

The Budapest Convention is technology-neutral so that the substantive criminal law offences may be applied to both current and future technologies involved, while its overseeing Cybercrime Convention Committee is mandated to issue Guidance Notes to facilitate the effective use and implementation of the Convention, also in the light of legal, policy and technological developments.

The Budapest Convention currently counts 61 Parties[1] and a further 10 States that have signed it or been invited to accede: about one third of UN Members have joined or expressed their commitment to join the Budapest Convention. More than twenty of these States are not Member States of the Council of Europe.

The number of Parties continues to grow constantly, with new accessions every year: in 2018 there has already been 5 new ratifications. In 2017, five new ratifications and one new signatory. In 2016 there were four new ratifications.

[1] Most Members of Council of Europe as well as Argentina, Australia, Cabo Verde, Canada, Chile, Costa Rica, Dominican Republic, Israel, Japan, Mauritius, Morocco, Panama, Paraguay, Philippines, Senegal, Sri Lanka, Tonga and USA.

www.parlament.gv.at

A further 60 to 70 States – that is a further one third of UN Members – have made use of the Budapest Convention as a guideline or at least as a source when preparing domestic legislation. Most of these States have participated in capacity building activities supported by the Council of Europe and many have been seeking specific advice in the drafting of domestic legislation in line with the Budapest Convention. At least two thirds of all States worldwide thus make use of the Budapest Convention as a guideline or reference already.

EU assistance programs to fight cybercrime

The EU assistance is closely coordinated with the UNODC Global Programme on Cybercrime.

Alongside the UNODC's Global Programme, there are a number of other capacity building programmes run by the Council of Europe and the European Union. 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. This programme serves also as a facility to help any country requesting support with developing or revising its cybercrime and electronic evidence legislation.

Moreover, the EU has also launched region-specific programmes jointly with the Council of Europe, such as the Cybercrime@EaP supporting 6 countries in Eastern Europe to cooperate effectively against cybercrime (2,4 MEUR between 2011 and 2017) and the iPROCEEDS programme targeting cybercrime proceeds in 6 countries in South Eastern Europe and Turkey with an EU contribution of 5 MEUR. Plans for increasing the EU's investment in its Global Action on Cybercrime are underway (10 MEUR in 2019-2020), as well as financing additional regional programmes. New programmes will start in the EU Eastern Neighbourhood (7 MEUR in 2019-2022), and other regions soon.

EU 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.

www.parlament.gv.at

UNODC, CCPCJ and UNIEG

The UN Intergovernmental Expert Group on Cybercrime (IEG) has been created by the UN Commission on Crime Prevention and Criminal Justice "to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime" [paragraph 42 of the Salvador Declaration].

The IEG had a first meeting in Vienna from 17 to 21 January 2011 and a second meeting in Vienna from 25 to 28 February 2013. At the second meeting, the UNODC Secretariat submitted a "Comprehensive Study on Cybercrime – Draft February 2013", which included a section on "Key Findings and Options" that was largely not deduced from the substantive part of the draft study. That meeting did not reach agreement on the draft Study nor the options proposed.

In February 2016, the draft Study was made available in the six official languages of the UN and Member States were invited to submit comments by May 2016. Comments received from 22 States and the European Union have now been published.

Both on the occasion of the second meeting of the IEG and at the subsequent 22nd UN Crime Commission (CCPCJ, Vienna, April 2013), coordination of EU Member States and institutions with other "like-minded partners" was instrumental to defend what in the meanwhile has been consolidated in the **EU official position**, expressed in the Council Conclusions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (11357/13, 25 June 2013) and confirmed in the Council Conclusions on Cyber Diplomacy (6122/15, 10 February 2015):

"RECOGNISING that international law, including 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, the International Covenant on Economic, Social and Cultural Rights provide a legal framework applicable in cyberspace. Efforts should therefore be made to ensure that these instruments are upheld in cyberspace; *therefore the EU does not call for the creation of new international legal instruments for cyber issues*" (emphasis added).

www.parlament.gv.at