Council of the European Union

Brussels, 13 May 2020
(OR. en)

7825/1/20
REV 1

LIMITE

CYBER 70
CFSP/PESC 366
COPS 144
RELEX 314
JAIEX 35
TELECOM 62
POLMIL 50
COPEN 110
JAI 342
ENFOPOL 110
CONOP 23

NOTE

From:	EEAS
To:	Delegations
Subject:	EU contribution to UN Secretary General request pursuant to operative paragraph 2 of the resolution A/RES/74/28 "Advancing responsible State behaviour in cyberspace in the context of international security"

Delegations will find in Annex a draft EU contribution to UN Secretary General request pursuant to operative paragraph 2 of the resolution A/RES/74/28 "Advancing responsible State behaviour in cyberspace in the context of international security". The text is drafted based on agreed language and has been revised following written comments received from Member States.

Changes are highlighted in ~~strikethrough~~ for deletions and **bold underlined** for additions in relation to the previous document.

This document is put **under informal silence procedure for HWP CI agreement until tomorrow, Thursday 14 May 2020**, cob (Brussels time). If no objections are made by that deadline, the document will be considered agreed by delegations.

The package of EU contributions to the UN will be transmitted by CONOP to the UN on Friday 15 May 2020.

ANNEX

A/RES/74/28 "Advancing responsible State behaviour in cyberspace in the context of international security" – EU contribution to UN Secretary General request pursuant to operative paragraph 2 of the resolution.

Cyberspace, and in particular the global, open Internet has become one of the backbones of our societies. It offers a platform that drives connectivity and economic growth. The EU and its Member States support a global, open, stable, peaceful and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply, with a view to societal well-being, economic growth, prosperity and the integrity of free and democratic societies.

As the Internet becomes more embedded in our lives, a number of the same issues we face in the physical world arise in cyberspace. In the international context, some States appear to have embraced a vision for cyberspace which involves a high degree of government control, raising concerns over the infringements of human rights and fundamental freedoms. There has also been a worrying increase in malicious cyber activities by State and non-state actors. The EU and its Member States have regularly expressed concern about such malicious activities that undermine the rules-based international order and increase the risks of conflict.

(a)Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

The EU and its Member States strongly support the aforementioned vision of an open, free, stable and secure cyberspace, through advancing and implementing an inclusive and multifaceted strategic framework for conflict prevention and stability in cyberspace, including through bilateral, regional and multi-stakeholder engagement. As part of this strategic framework the EU works to strengthen global resilience, advance and promote a common understanding of the rules-based international order in cyberspace, and develop and implement practical cooperative measures, including regional confidence building measures between States. Strengthening global cyber resilience is a crucial element in maintaining international peace and stability, by reducing the risk of conflict and as a means to address the challenges associated with the digitalisation of our economies and societies. Global cyber resilience reduces the ability of potential perpetrators to misuse ICTs for malicious purposes and strengthens the ability of States to effectively respond to and recover from cyber incidents.

The cybersecurity strategy "An Open, Safe and Secure Cyberspace"[1], as well as other subsequent policy documents cited below, represent the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. These aim at promoting EU values and ensuring that the conditions are in place for the digital economy to grow. Certain specific actions are aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defence.

In February 2015, the Council of the European Union stresses in its Council Conclusion on Cyber diplomacy[2] the importance of further developing and implementing a common and comprehensive EU approach for cyber diplomacy which promotes human rights and fundamental EU values, ensures free expression, promotes gender quality, advances economic growth, combats cybercrime, mitigates cybersecurity threats, prevents conflicts and provides stability in international relations. The EU also calls for a strengthened multi-stakeholder model of Internet governance and for enhanced capacity-building efforts in third countries. In addition, the EU recognises the importance of engagement with key partners and international organisations. The EU also stresses **the application of existing international law in the field of international security and** the relevance of norms of behaviour ~~and the application of existing international law in the field of international security~~, as well as the importance of Internet Governance as an integral part of the common and comprehensive EU approach for cyber diplomacy.

Based on a review of 2013 Cybersecurity Strategy, the EU further strengthened its cybersecurity structures and capabilities in a coordinated manner, with the full cooperation of the Member States and the different EU structures concerned, while respecting their competencies and responsibilities. In 2017, the Joint Communication on “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU”[3] sets out the scale of the challenge and the range of measures envisioned at EU level, to ensure that the EU is better prepared to face the ever-increasing cybersecurity challenges.

---

1 JOIN (2013) 1 final. 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.

2 6122/15 Council Conclusions on Cyber Diplomacy.

3 JOIN (2017) 450 final. Joint communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

Concerns about ever-increasing cybersecurity challenges gave an impetus to the development of a framework for a joint EU diplomatic response to malicious cyber activities, the cyber diplomacy toolbox[4]. The increasing ability and willingness of state and non-state actors to pursue their objectives through malicious cyber activities should be of global concern. Such activities may constitute wrongful acts under international law and could lead to destabilising and cascading effects with enhanced risks of conflict. **The EU and its Member States are committed to the settlement of international disputes in cyberspace by peaceful means. To this end,** the framework for a joint EU diplomatic response is part of the EU's approach to cyber diplomacy, which contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. The framework encourages cooperation, facilitate mitigation of immediate and long-term threats, and influence the behaviour of malicious actors in the long term. **It also provides due coordination with the EU's crisis management mechanisms, including the Blueprint for Coordinated Response to Large Scale Cybersecurity Incidents and Crises.** The European Union and its Member States call on the international community to strengthen international cooperation in favour of a global, open, stable, peaceful and secure cyberspace where human rights, fundamental freedoms and the rule of law fully apply. They are determined to continue their efforts to prevent, discourage, deter and respond to malicious activities and seek to enhance international cooperation to this effect.

The EU's international cyberspace policy promotes the respect of EU core values, defines norms for responsible behaviour, advocates the application of existing international laws in cyberspace, while assisting countries outside the EU with cyber-security capacity-building, and promoting international cooperation in cyber issues.

(b)The content of the concepts mentioned in the reports of the Group of Governmental Experts;

Existing and emerging threats

The EU and its Member States recognise that cyberspace offers significant opportunities for economic growth, as well as sustainable and inclusive development. Nonetheless, recent developments in cyberspace present continuously evolving challenges.

[4] 10474/17. Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

The EU and its Member States are concerned by the rise of malicious behaviour in cyberspace, including the abuse of Information and Communications Technologies (ICTs) for malicious purposes, by both state and non-state actors, as well as the increase of cyber-enabled theft of intellectual property. Such behaviour undermines and threatens economic growth, as well as the integrity, security and stability of the global community, and can lead to destabilising and cascading effects with enhanced risks of conflict.

More recently, as the coronavirus pandemic continues, the European Union and its Member States have observed cyber threats and malicious cyber activities targeting essential operators in Member States and their international partners, including in the healthcare sector. The European Union and its Member States condemn this malicious behaviour in cyberspace and underline their continued support to increase global cyber resilience.

Any attempt to hamper the ability of critical infrastructures is unacceptable **and can put people's lives at risk**. ~~The EU and its Member States urged perpetrators~~ **Any actor should** ~~to immediately~~ refrain from conducting ~~such~~ irresponsible and destabilising activities in cyberspace~~, which can put people's lives at risk. We have~~ **The EU and its Member States** call upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law and the 2010, 2013 and 2015 consensus reports of the United Nations Groups of Governmental Experts (UNGGEs). The EU and its Member States emphasize again that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs and should also respond to appropriate requests by another State to mitigate malicious cyber activities emanating from their territory.

In addition, as recognized by previous UN GGE reports, given the unique character of ICT technologies, our approach to address cyber issues in the context of international security must remain technology neutral. This is consistent with the concept and UN acknowledgement that existing international law applies to new areas, including the use of emerging technologies.

The EU and its Member States can only support the development and use of technologies, systems or ICT-enabled services, in full respect of applicable international law and norms, particularly the UN Charter, as well as international humanitarian law and its derived principles and human rights.

How international law applies to the use of ICTs

The EU and its Member States strongly support an effective multilateral system, underpinned by a rules-based international order, which delivers results in tackling present and future global challenges in cyberspace.

A truly universal cyber security framework can only be based on existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law. In addition, the EU and its Member States reiterate the applicability of existing international law to state conduct in cyberspace as recognised by the UN GGE reports from 2010, 2013 and 2015, as well as the principles established in the paragraphs 28(a) to 28(f) of the 2015 GGE report.

International law, including international humanitarian law, including the principles of precaution, humanity, military necessity, proportionality and distinction, applies to state conduct in cyberspace and is wholly protective, by setting clear boundaries for its legality, also in times of conflict. The EU underlines its conviction that international law is not an enabler of conduct; rather, international law delineates the rules governing military operations to limit their effects, and in particular to protect civilian populations.

Furthermore, human rights and fundamental freedoms as enshrined in the relevant international instruments must be respected and upheld equally online and offline. The EU and its Member States welcome that these principles have also been affirmed by the UN Human Rights Council[5] and General Assembly.

For these reasons, the EU and its Member States do not call for and do not see the necessity for the creation of new international legal instruments for cyber issues at this stage, as there is an international legal framework already.

The EU and its Member States reaffirm their support for continued dialogue and cooperation to advance a shared understanding on the application of existing international law to the use of ICTs by States, as well as their support to efforts to bring legal clarity on how existing international law applies, as it will contribute to maintaining peace, ~~conflict prevention~~ prevent conflict and ensuring global stability.

[5] A/HRC/RES/20/8

We continue to support ongoing efforts to promote the application of existing international law to cyberspace, including on exchanging information and best practices on the application of existing international law in cyberspace. We are committed to continue to inform on national positions on ~~interpretation of~~ how international law applies to the use of ICTs by states, as it promotes transparency and advances global understanding on national approaches, which is fundamental to maintaining long-term peace and stability and reduce the risk of conflict through acts in cyberspace. Further focus should be placed on raising awareness on the applicability of existing international law as a mean to promote stability and to prevent conflict in cyberspace.

Norms, rules and principles for the responsible behaviour of States

The EU and its Member States encourage all States to build on and advance the work repeatedly endorsed by the UNGA, notably in resolution 70/237, and on further implementation of these agreed norms and confidence building measures, which play an essential role in conflict prevention.

The EU and its Member States will be guided in their use of ICTs by existing international law, as well as through adherence to **voluntary** norms, rules and principles of **responsible** State behaviour **and their implementation** in cyberspace, as articulated in successive UN GGE reports in 2010, 2013 and 2015. We believe that a practical way forward should encourage increased cooperation and transparency to share best practices, including on how UN GGE **existing** norms are applied, through related initiatives and frameworks, such as regional organizations and institutions, to facilitate raising awareness and to effectively implement agreed norms of responsible **State** behaviour.

Confidence-building measures

Building effective mechanisms of state **cooperation and** interaction in cyberspace are critical components in conflict prevention. Regional fora have proven to be a relevant platform to create space for dialogue and cooperation among actors with shared concerns but common interests in order to address effectively challenges from a regional perspective.

Developing and implementing cyber confidence building measures, including cooperation and transparency measures, in the Organization for Security and Co-operation in Europe (OSCE), ASEAN Regional Forum (ARF), the Organization of American States (OAS) and other regional settings will increase predictability of state behaviour and reduce the risk of misinterpretation, escalation and conflict that may stem from ICT incidents thereby contributing to long term stability in cyberspace.

International cooperation and assistance in ICT security and capacity-building

In order to prevent conflicts and reduce tensions stemming from the misuse of ICTs, the EU and its Member States aim to strengthen resilience globally, with particular emphasis on developing countries, as a means to address the challenges associated with the digitalisation of economies and societies, as wells as to reduce the ability of potential perpetrators to misuse ICTs for malicious purpose. Resilience strengthens the ability of States to effectively respond to and recover from cyber threats.

The EU and its Member States support a range of tailored programmes and initiatives to assist countries with developing their skills and capacities to address cyber incidents, as well as initiatives to enabling the exchange of best practices, whether through direct engagement, bilateral contacts or engagement through regional and multilateral institutions.

The EU and its Member States recognize that the promotion of adequate protective capacities and more secure digital products, processes and services will contribute to a more secure and trustworthy cyberspace. We recognize the responsibility of all relevant actors to engage in capacity development in this regard and further call for stronger cooperation with key international partners and organisations to support capacity-building in third countries.

~~How international law applies to the use of ICTs~~

~~The EU and its Member States strongly support an effective multilateral system, underpinned by a rules-based international order, which delivers results in tackling present and future global challenges in cyberspace.~~

~~A truly universal cyber security framework can only be based on existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law. In addition, the EU and its Member States reiterate the applicability of existing international law to state conduct in cyberspace as recognised by the UN GGE reports from 2010, 2013 and 2015, as well as the principles established in the paragraphs 28(a) to 28(f) of the 2015 GGE report.~~

~~International law, including international humanitarian law, including the principles of precaution, humanity, military necessity, proportionality and distinction, applies to state conduct in cyberspace and is wholly protective, by setting clear boundaries for its legality, also in times of conflict. The EU underlines its conviction that international law is not an enabler of conduct; rather, international law delineates the rules governing military operations to limit their effects, and in particular to protect civilian populations.~~

~~Furthermore, human rights and fundamental freedoms as enshrined in the relevant international instruments must be respected and upheld equally online and offline. The EU and its Member States welcome that these principles have also been affirmed by the UN Human Rights Council[6] and General Assembly.~~

~~For these reasons, the EU and its Member States do not call for and do not see the necessity for the creation of new international legal instruments for cyber issues at this stage, as there is an international legal framework already.~~

~~The EU and its Member States reaffirm their support for continued dialogue and cooperation to advance a shared understanding on the application of existing international law to the use of ICTs by States, as well as their support to efforts to bring legal clarity on how existing international law applies, as it will contribute to peace, conflict prevention and global stability.~~

[6] A/HRC/RES/20/8

~~We continue to support ongoing efforts to promote the application of existing international law to cyberspace, including on exchanging information and best practices on the application of existing international law in cyberspace. We are committed to continue to inform on national positions on interpretation of how international law applies to the use of ICTs by states, as it promotes transparency and advances global understanding on national approaches, which is fundamental to mainlining long-term peace and stability and reduce the risk of conflict through acts in cyberspace. Further focus should be placed on raising awareness on the applicability of existing international law as a mean to promote stability and to prevent conflict in cyberspace.~~