Council of the European Union

Brussels, 19 June 2019
(OR. en)

10472/19

LIMITE

CYBER 210
CFSP/PESC 500
COPS 196
RELEX 631
JAIEX 103
TELECOM 265
POLMIL 67
COPEN 282
JAI 729
ENFOPOL 308

'I' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
No. prev. doc.:	9764/2/19 REV 2
Subject:	Narrative paper on an open, free, stable and secure cyberspace in the context of international security - text for submission to Coreper for approval

1. At the meetings of the Horizontal Working Party (HWP) on Cyber Issues of 29 May and 5 June 2019, delegations examined the narrative paper on an open, free, stable and secure cyberspace in the context of international security, as prepared by the EEAS[1].

2. Following the outcome of these meetings and on the basis of delegations' contributions and written comments, a revised version[2] of the above-mentioned narrative paper was prepared by the EEAS in view of the Horizontal Working Party (HWP) on Cyber Issues of 19 June 2019.

1 9764/19 and 9764/1/19
2 9764/2/19

3. At that meeting, the revised text was agreed by Member States and finalised as set in the Annex.

4. On that basis, COREPER is invited to approve the narrative paper on an open, free, stable and secure cyberspace in the context of international security as set out in Annex.

ANNEX

Narrative paper on an open, free, stable and secure cyberspace in the context of international security

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 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[3].

As the Internet becomes more embedded in our lives, some 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 infringement 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 these activities, including in the European Council Conclusions of June and October 2018[4], and most recently in the Declaration by the High Representative on behalf of the EU on the respect of the rules-based order in cyberspace[5] in April 2019. These activities undermine the rules-based international order and raise the risks of conflict.

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[6]. 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, while at the same time respecting the division of competencies between the EU and its Member States.

---

3 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.

4 10086/18. Council conclusions, EU coordinated response to Large-Scale Cybersecurity Incidents and Crises.

5 https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace

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

In cyberspace, like elsewhere, the EU aims to i) prevent conflicts, ii) to build stability and iii) promote and enhance cooperation.

Preventing conflicts: In order to prevent conflicts and reduce tensions stemming from the use of ICTs, the EU and its Member States' aim to strengthen cyber security and resilience, increase awareness of businesses and citizens, build capacities of its international partners and promote increased transparency on cybersecurity issues. More specifically, the EU and its Member States are committed to:

- Increase cyber security by developing capacity to achieve and strengthen resilience and protection of networks and infrastructure at the national, regional and international level. The EU considers that the promotion of adequate protective capacities and more secure digital products, processes and services will contribute to a more secure and trustworthy cyberspace. It recognizes the responsibility of all relevant actors to develop capacity in this regard;

- strengthen global cyber resilience, 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 threats;

- bridge the digital divide and share the economic benefits of the internet through providing targeted capacity building to third countries, as one of our responsibilities, to advance conflict prevention and stability in cyberspace, to support the prevention, detection, deterrence and response to malicious cyber activities. We are also committed to advance understanding on the importance of an open, free, stable and secure cyberspace for social, political and economic development that contributes to transparency and reliability to avoid room for misinterpretation of actions and escalation to conflict, including the interpretation of how international law applies to the use of ICTs by states[7].

[7] 7737/19 Council conclusions on cybersecurity capacity and capabilities building in the EU.

- contribute to advancing cyber stability in line with the Sustainable Development Goals; notably, by preventing online hate speech and crime, promoting the rule of law in cyberspace and accountable and more transparent institutions, ensuring public access to information and protecting fundamental freedoms while strengthening relevant national institutions and promoting the application of human rights online as well as offline, without discrimination.

- advance and implement the existing rules-based international order in cyberspace, including the application of international law and adherence to the norms of responsible state behaviour repeatedly endorsed by the UN General Assembly. We stand ready to continue assistance to third countries to further develop common understanding on the security of and in the use of ICTs, on the application of international law and derived norms, rules and principles of responsible State behaviour, enshrined in UNGGE reports from 2010[8], 2013[9] and 2015[10], and raising awareness of the need to increase global cyber resilience among all stakeholders[11] to ensure their universal acceptance and effective implementation to maintain an open, free, stable and secure cyberspace; Building on the existing rules-based order is essential to peace and stability in cyberspace, and avoids lengthy discussions on a new binding instrument that would not only divert efforts, but also risks entering into a divisive and lengthy process, as well as undermining practical endeavours to advance the implementation of previously agreed rules, norms and principles of responsible State behaviour and regional confidence building measures which contribute to conflict prevention and stability in cyberspace;

---

8 A/65/201. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2010).

9 A/68/98. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013).

10 A/70/174. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015).

11 7925/18. Council conclusions on malicious cyber activities.

Building stability in cyberspace: The European Union and its Member States actively promote the rules-based international order, effective multilateralism and effective global governance, as the core of a consensus based approach, and with the aim to advance stability in cyberspace. In this regard, the EU and its Member States are committed to:

- respect international law, and uphold the consensus that international law apply in cyberspace, as well as continued dialogue and cooperation to advance shared understanding on the application of international law to the use of ICTs by States. Such a shared understanding of the application of existing international law, including the UN Charter in its entirety, and international principles deriving from the UN Charter[12], will contribute to conflict prevention and stability and strengthens the rules-based order in cyberspace;

- guide its use of ICTs by existing international law, as well as through the adherence to the norms, rules and principles of responsible State behaviour in cyberspace, as articulated in successive reports from the United Nations Group of Governmental Experts (UN GGE) in 2010, 2013 and 2015, and which have been unanimously endorsed by the UNGA;

- the application of international humanitarian law to state behaviour in cyberspace in armed conflict, including the principles of precaution, humanity, military necessity, proportionality and distinction.

- continue to inform on their national positions on their 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;

---

12 Which are, inter alia, apply to State use of ICTs: sovereign equality; non-intervention in the internal affairs of other States; the settlement of international disputes by peaceful means in such a manner that international peace, security, and justice are not endangered; the right to respond, including by non-forcible countermeasures, to internationally wrongful acts committed through the use of ICTs; refraining in international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations (UN); the inherent right to self-defence against an armed attack; respect for human rights and fundamental freedoms.

- emphasize that States should not conduct, or knowingly allow their territory to be used for, malicious activities using ICTs as stated in the 2015 UN GGE report. The EU and its Member States are, therefore, strongly committed to further developing efforts to facilitate global understanding and cooperation with third countries to reinforce principles of due diligence and states' responsibility in cyberspace;

- ensure full respect for the protection of human rights online as well as offline, in particular the right to freedom of opinion and expression and the right to privacy and the protection of personal data;

- recognise the UN's leading role in developing, by consensus, norms of responsible State behaviour in cyberspace and, to ensure their universal acceptance and effective implementation to maintain an open, free, stable and secure cyberspace;

- in the interest of developing a truly universal framework for responsible State behaviour , the views of other stakeholders such as civil society, the technical community, business and academia should be shared with both the OEWG as well as the UNGGE, without undermining existing multi-stakeholder processes or expanding the mandate of either process;

- seeing the new UN GGE build on the consensus reached by previous UNGGEs, to further advance the consensus on responsible state behaviour in cyberspace. The work in the Open-ended Working Group (OEWG) should focus on raising awareness, building common understanding and supporting and advancing implementation of previously agreed rules, norms and principles of responsible State behaviour, as guided by previous GGE reports. The OEWG's mandate provides a role for all stakeholders, and is a valuable platform for the exchange of positions and discussion, including fostering a stronger common understanding of threats faced in cyberspace.

Promoting cooperation: The EU and its Member States view increased cooperation as fundamental to developing the trust required for promoting an open, free, stable and secure cyberspace. They will continue to deepen their regular dialogue with partners, to develop and implement effective confidence-building measures and to demonstrate their willingness to settle international disputes by peaceful means, as well as respond to incidents, including through the Framework for a joint EU diplomatic response to malicious cyber activities, when appropriate. More specifically, the EU and its Member States are committed to:

- demonstrate commitment to the settlement of international disputes in cyberspace by peaceful means. Efforts to prevent conflict in this regard include diplomatic, economic and political measures to protect the integrity and security of the EU, its Member States and its businesses and citizens. To this end the Council agreed in June 2017 on a framework for a joint EU diplomatic response to malicious cyber activities, the "cyber diplomacy toolbox"[13] that allows the EU and its Member States to make full use of measures within the Common Foreign and Security Policy (CFSP), including, if necessary, restrictive measures, to respond to malicious cyber activities that threaten the EU and its Member States' security and integrity or are contrary to international obligations. The European Union has established a sanctions regime against cyber-attacks threatening the Union and/or its Member States in May 2019[14];

- strengthening bilateral and regional dialogues with a broad range of partners to advance, promote and implement the strategic framework for conflict prevention and stability in cyberspace. Enhanced cooperation and dialogue contributes to building trust and confidence, for exchanging best practices, promoting human rights, democracy and the rule of law, improving security, as well as tackling issues of common concern to better prevent, detect, deter and respond to malicious cyber activities;

---

13 10474/17. Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

14 7299/19. Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

- further develop and implement cooperative regional confidence building measures between States, as an essential element in increasing cooperation and transparency to help reduce the risk of conflict. Implementing cyber confidence building 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