Council of the European Union
General Secretariat

Brussels, 13 March 2019

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (07.12.2020)

WK 3651/2019 INIT

LIMITE

COJUR

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

INFORMATION

From:	Presidency
To:	Working Party on Public International Law
Subject:	EU-US Dialogue - International Law in Cyberspace (background information)

Delegations will find attached a relevant background information in view of preparation of the *International Law in Cyberspace* topic (point 4 on the Agenda) on the EU-US informal Legal Advisers' Dialogue (20 March).

.

United Nations A/RES/73/266

General Assembly

Distr.: General
2 January 2019

Seventy-third session
Agenda item 96

Resolution adopted by the General Assembly on 22 December 2018

[*on the report of the First Committee (A/73/505)*]

73/266. Advancing responsible State behaviour in cyberspace in the context of international security

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, 70/237 of 23 December 2015 and 71/28 of 5 December 2016, as well as its decision 72/512 of 4 December 2017,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this progress the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Confirming that information and communications technologies are dual-use technologies and can be used for both legitimate and malicious purposes,

Stressing that it is in the interest of all States to promote the use of information and communications technologies for peaceful purposes and to prevent conflict arising from the use of information and communications technologies,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States, to the detriment of their security in both civil and military fields,

Underscoring the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies,

Underlining the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies,

Welcoming the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the 2010,[1] 2013[2] and 2015[3] reports transmitted by the Secretary-General,

Stressing the importance of the assessments and recommendations contained in the reports of the Group of Governmental Experts,

Confirming the conclusions of the Group of Governmental Experts, in its 2013 and 2015 reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time,

Confirming also the conclusions of the Group of Governmental Experts that voluntary confidence-building measures can promote trust and assurance among States and help to reduce the risk of conflict by increasing predictability and reducing misperception and thereby make an important contribution to addressing the concerns of States over the use of information and communications technologies by States and could be a significant step towards greater international security,

Confirming further the conclusions of the Group of Governmental Experts that providing assistance to build capacity in the area of information and communications technology security is also essential for international security, by improving the capacity of States for cooperation and collective action and promoting the use of such technologies for peaceful purposes,

Stressing that, while States have a primary responsibility for maintaining a secure and peaceful information and communications technology environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations,

1. *Calls upon* Member States:

(a) To be guided in their use of information and communications technologies by the 2010,[1] 2013[2] and 2015[3] reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security;

[1] A/65/201.
[2] A/68/98.
[3] A/70/174.

(b) To support the implementation of cooperative measures, as identified in the reports of the Group of Governmental Experts, to address the threats emerging in this field and ensure an open, interoperable, reliable and secure information and communications technology environment consistent with the need to preserve the free flow of information;

2. *Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts, to continue to inform the Secretary-General of their views and assessments on the following questions:

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

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

3. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2019 on the basis of equitable geographical distribution, proceeding from the assessments and recommendations contained in the above-mentioned reports, to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States, and to submit a report on the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States, to the General Assembly at its seventy-sixth session;

4. *Requests* the Office for Disarmament Affairs of the Secretariat, through existing resources and voluntary contributions, on behalf of the members of the group of governmental experts, to collaborate with relevant regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations, to convene a series of consultations to share views on the issues within the mandate of the group in advance of its sessions;

5. *Requests* the Chair of the group of governmental experts to organize two two-day informal consultative meetings, open-ended so that all Member States can engage in interactive discussions and share their views, which the Chair shall convey to the group of governmental experts for consideration;

6. *Decides* to include in the provisional agenda of its seventy-fourth session the item entitled “Developments in the field of information and telecommunications in the context of international security”.

65th plenary meeting
22 December 2018

United Nations A/RES/73/27

General Assembly

Distr.: General
11 December 2018

Seventy-third session
Agenda item 96

Resolution adopted by the General Assembly on 5 December 2018

[*on the report of the First Committee (A/73/505)*]

73/27. Developments in the field of information and telecommunications in the context of international security

The General Assembly,

Recalling its resolutions 36/103 of 9 December 1981, 43/78 H of 7 December 1988, 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, 70/237 of 23 December 2015 and 71/28 of 5 December 2016,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Underscoring the aspirations of the international community to the peaceful use of information and communications technologies (ICTs) for the common good of humankind and to further the sustainable development of all countries, irrespective of their scientific and technological development,

Noting that capacity-building is essential for cooperation of States and confidence-building in the field of ICT security,

Recognizing that some States may require assistance in their efforts to bridge the divide in the security of ICTs and their use,

Noting that providing assistance, upon request, to build capacity in the area of ICT security is essential for international security,

Affirming that capacity-building measures should seek to promote the use of ICTs for peaceful purposes,

Confirming that ICTs are dual-use technologies and can be used for both legitimate and malicious purposes,

Expressing concern that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely,

Stressing that it is in the interest of all States to promote the use of ICTs for peaceful purposes, with the objective of shaping a community of shared future for humankind in cyberspace, and that States also have an interest in preventing conflict arising from the use of ICTs,

Noting that the United Nations should play a leading role in promoting dialogue among Member States to develop common understandings on the security of and the use of ICTs, as well as in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour in this sphere, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices,

Expressing concern that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Underlining the importance of respect for human rights and fundamental freedoms in the use of ICTs,

Welcoming the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome reports transmitted by the Secretary-General,[1]

Welcoming also that, in considering the application of international law to State use of ICTs, the Group of Governmental Experts, in its 2015 report,[2] identified as of central importance the commitments of States to the following principles of the Charter of the United Nations and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their 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; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States,

Confirming the conclusions of the Group of Governmental Experts, in its 2013[3] and 2015[2] reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of ICTs can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time,

[1] A/65/201, A/68/98 and A/70/174.
[2] A/70/174.
[3] A/68/98.

Confirming also that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory,

Reaffirming the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, cooperation and friendly relations among States and nations,

Recognizing the duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States,

Stressing that, while States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations,

1. *Welcomes* the following set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 2013[3] and 2015[2] adopted by consensus and recommended in resolution 71/28 entitled "Developments in the field of information and telecommunications in the context of international security", adopted by the General Assembly on 5 December 2016:

1.1. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

1.2. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

1.3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts.

1.4. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

1.5. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 of 5 July 2012[4] and 26/13 of 26 June 2014[5] on the promotion, protection and enjoyment of human rights on the Internet, as well as

[4] See *Official Records of the General Assembly, Sixty-seventh Session, Supplement No. 53* and corrigendum (A/67/53 and A/67/53/Corr.1), chap. IV, sect. A.

[5] Ibid., *Sixty-ninth Session, Supplement No. 53* (A/69/53), chap. V, sect. A.

General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

1.6. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

1.7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

1.8. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

1.9. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.

1.10. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

1.11. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

1.12. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

1.13. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in information space with regard to their potential role;

2. *Calls upon* Member States to promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

3. *Considers* that the purpose of such measures could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

4. *Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,[1] to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

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

(c) The content of the concepts mentioned in paragraph 3 above;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level;

5. *Decides* to convene, beginning in 2019, with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent, an open-ended working group acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building and the concepts referred to in paragraph 3 above, and to submit a report on the results of the study to the General Assembly at its seventy-fifth session, and to provide the possibility of holding, from within voluntary contributions, intersessional consultative meetings with the interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate;

6. *Also decides* that the open-ended working group shall hold its organizational session in June 2019 in order to agree on the organizational arrangements connected with the group;

7. *Further decides* to include in the provisional agenda of its seventy-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

45th plenary meeting
5 December 2018

Council of the European Union

Brussels, 7 June 2017
(OR. en)

9916/17

CYBER 91
RELEX 482
POLMIL 58
CFSP/PESC 476

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. prev. doc.:	7923/2/17 REV 2
Subject:	Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") - Adoption

1. At the PSC meeting of 14 March 2017 the EEAS/Commission services presented a joint issues paper on a joint EU diplomatic response to cyber operations ("Cyber toolbox")[1]. The latter was welcomed by delegations as well as its suggested follow up in the Horizontal Working Party on Cyber Issues (HWPCI). As a result the PSC invited the HWPCI to examine the paper in more detail in consultation with other Council preparatory bodies, where appropriate, before it would revert to the issue by the end of June, taking into account the outcome of that examination.

2. Following the tasking by PSC the joint paper was also presented and discussed at the HWPCI on 22 March 2017. Delegations welcomed the paper, specifying the need to take the necessary time to discuss it in detail. As a way forward, a large number of them voiced a preference for the development of Council conclusions accompanying the toolbox itself.

[1] WK 2569/2017 INIT.

3. In view of this, the Presidency prepared draft Council Conclusions as set out in doc.7923/17 which were presented and examined at two consecutive meetings of the HWPCI meeting, respectively of 19 April and 12 May 2017 where the text was further streamlined and improved according to the comments provided by Member States.

4. On 6 June 2017 the final text of the draft Council Conclusions was submitted to PSC in line with the tasking of March and it was agreed with several additions[2] with a view to their adoption by the Council.

5. Against this background, COREPER is requested to invite the Council to approve the draft Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, as set out in the Annex.

---

[2] WK 6162/2017 REV 1

ANNEX

DRAFT COUNCIL CONCLUSIONS ON A FRAMEWORK FOR A JOINT EU DIPLOMATIC RESPONSE TO MALICIOUS CYBER ACTIVITIES ("CYBER DIPLOMACY TOOLBOX")

The Council of the European Union adopted the following conclusions:

1. The EU recognises that cyberspace offers significant opportunities, but also poses continuously evolving challenges for EU external policies, including for the Common Foreign and Security Policy, and affirms the growing need to protect the integrity and security of the EU, its Member States and their citizens against cyber threats and malicious cyber activities.

The EU recalls its conclusions on the EU Cybersecurity strategy[3], in particular its determination to keep cyberspace open, free, stable and secure where fundamental rights and the rule of law fully apply. It also recalls its Conclusions on Cyber Diplomacy[4], in particular that a common and comprehensive EU approach for cyber diplomacy could contribute to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations.

The EU and its Member States note the importance of the ongoing EU cyber diplomacy engagement and of the need for coherence among the EU cyber initiatives to effectively strengthen the cyber resilience, and are encouraged to further intensify their efforts on cyber dialogues within the framework of effective policy coordination, and emphasise the importance of cyber capacity building in third countries.

2. The EU is concerned by the increased ability and willingness of State and non-state actors to pursue their objectives by undertaking malicious cyber activities of varying in scope, scale, duration, intensity, complexity, sophistication and impact.

---

[3] 12109/13.
[4] 6122/15.

The EU affirms that malicious cyber activities might constitute wrongful acts under international law and emphasises that States should not conduct or knowingly support ICT activities contrary to their obligations under international law, and should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, as it is stated in the 2015 report of the United Nations Groups of Governmental Experts (UN GGE).

3. The EU recalls its and its Member States' efforts to improve cyber resilience in particular through the implementation of the NIS Directive and the operational cooperation mechanisms provided therein, and that malicious cyber activities against information systems, as defined under EU law, constitute a criminal offence and that effective investigation and prosecution of such crimes remains a common endeavour for Member States.

The EU and its Member States take note of the ongoing work of the United Nations Groups of Governmental Experts on Developments (UN GGE) in the Field of Information and Telecommunications in the context of international security, building on the 2010, 2013 and 2015 reports[5], and are encouraged to strongly uphold the consensus that existing international law is applicable to cyberspace. The EU and its Member States have a strong commitment to actively support the development of voluntary, non-binding norms of responsible State behaviour in cyberspace and the regional confidence building measures agreed by the OSCE[6] to reduce the risk of conflicts stemming from the use of information and communication technologies.

The EU reaffirms its commitment to the settlement of international disputes in cyberspace by peaceful means, and that all of the EU's diplomatic efforts should as a priority be aimed at promoting security and stability in the cyberspace through increased international cooperation, and at reducing the risk of misperception, escalation and conflict that may stem from ICT incidents. In that regard the EU recalls the UN General Assembly call to the UN Member States to be guided by the UNGGE reports' recommendations in their use of ICTs.

---

5 A/68/98 and A/70/174.

6 PC.DEC/1106 of 3 December 2013 and PC.DEC/1202 of 10 March 2016.

4. The EU stresses that clearly signaling the likely consequences of a joint EU diplomatic response to such malicious cyber activities influences the behavior of potential aggressors in cyberspace thus reinforcing the security of the EU and its Member States. The EU reminds that attribution to a State or a non-State actor remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of State responsibility. In that regard, the EU stresses that not all measures of a joint EU diplomatic response to malicious cyber activities require attribution to a State or a non-State actor.

5. The EU affirms that measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities and should encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in a long term. The EU will work on the further development of a Framework for a joint EU diplomatic response to malicious cyber activities, guided by the following main principles:

- serve to protect the integrity and security of the EU, its Member States and their citizens,
- take into account the broader context of the EU external relations with the State concerned,
- provide for the attainment of the CFSP objectives as set out in the Treaty on the European Union (TEU) and the respective procedures provided for their attainment,
- be based on a shared situational awareness agreed among the Member States and correspond to the needs of the concrete situation in hand,
- be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity,
- respect applicable international law and must not violate fundamental rights and freedoms.

6. The EU calls on the Member States, the European External Action Service (EEAS) and the Commission to give full effect to the development of a Framework for a joint EU diplomatic response to malicious cyber activities and reaffirms in this regard its commitment to continue the work on that Framework in cooperation with the Commission, EEAS and other relevant parties by putting in place implementing guidelines, including preparatory practices and communication procedures and to test them through appropriate exercises.

Council of the
European Union

Brussels, 9 October 2017
(OR. en)

13007/17

LIMITE

CYBER 142
CFSP/PESC 855
COPS 302
RELEX 836

NOTE

From:	General Secretariat of the Council
To:	PSC
Subject:	Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final text

With a view to the PSC meeting of 11 October 2017, delegations will find attached draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.

ANNEX

DRAFT IMPLEMENTING GUIDELINES FOR THE FRAMEWORK ON A JOINT EU DIPLOMATIC RESPONSE TO MALICIOUS CYBER ACTIVITIES

1. INTRODUCTION

The EU is concerned by the increased ability and willingness of State and non-state actors to pursue their objectives by undertaking malicious cyber activities. Such activities against infrastructure, cyber-espionage, intellectual property theft, cybercrime or cyber conflict and disinformation using cyber means need a response going beyond our current communication and cybersecurity policies. Malicious cyber activities have to be seen also in the context of hybrid threats[1] as well as in the context of the work on resilience that fosters the ability to withstand, adapt to, and recover quickly from stress and shocks[2].

The Council conclusions on Cyber Diplomacy of 11 February 2015 note that a common and comprehensive EU approach for cyber diplomacy could contribute to the "mitigation of cybersecurity threats, conflict prevention and greater stability in international relations through the use of diplomatic and legal instruments". Clearly signalling the likely consequences of a joint EU diplomatic response to such malicious cyber activities influences the behaviour of potential aggressors in cyberspace, thus reinforcing the security of the EU and its Member States. The added value of a joint EU diplomatic response was confirmed by the June 2017 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities[3].

---

1 JOIN(2016) 18 final – Joint Communication on a 'Joint Framework on countering hybrid threats 'a European Union response' and the Joint Staff Working Document on EU operational protocol for countering hybrid threats, the 'EU Playbook', SWD(2016) 227 final.

2 JOIN(2017) 21 final - Joint Communication on A Strategic Approach to Resilience in the EU's external action.

3 Doc. 9916/17 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

This document responds to these Council Conclusions that have set out the main principles for the Framework development. They also call on the Member States, the EEAS and the Commission to put in place implementing guidelines for the Framework that include measures and mechanisms leading to the invocation of the measures, preparatory practices and communication procedures, including exercises. The implementing guidelines are set out in the present document.

The Framework complements the existing activities that the EU is already undertaking against cyber threats through increased prevention, early warning, resilience and coordination. The 2013 EU Cyber Security Strategy, the 2014 EU Cyber Defence Policy Framework, the 2016 Global Strategy for the European Union's Foreign and Security Policy, the 2016 Network and Information Security (NIS) Directive, and the activities of the European Network and Information Security Agency (ENISA), the European Cyber Crime Centre (EC3) at Europol and CERT-EU address these issues for Member States and the EU institutions. The joint framework on countering hybrid threats[4] may be used as well. The importance of EU-NATO cooperation in the field of cybersecurity is recognised herein, in full respect of the principles of inclusiveness, reciprocity and autonomy of the EU's decision-making processes and in accordance with the Council Conclusions 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 NATO.

The Framework should be seen as complementary to, but not as a replacement for, existing EU cyber diplomacy engagement. Current diplomatic efforts and operational actions, such as supporting wider compliance with existing international law[5], including the UN Charter, and specifically its Articles 2(4) (prohibition of the use of force), 33 (peaceful settlement of disputes) and 51(inherent right to act in individual or collective self-defence in response to an armed attack), and International Humanitarian Law, international legal instruments such as the Budapest Convention on Cybercrime and reaching common positions in international fora, will continue unabated.

---

4 JOIN(2016) 18 final – Joint Communication on a 'Joint Framework on countering hybrid threats 'a European Union response' and the Joint Staff Working Document on EU operational protocol for countering hybrid threats, the 'EU Playbook', SWD(2016) 227 final.

5 Tallinn Manual 2.0 provides an example of an academic analysis of how existing international law could apply to cyber operations, including a list of possible measures for States that have been subject to an internationally wrongful act in the cyber domain.

The EU continues its commitment to actively support the outcomes of the United Nations Groups of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security which concluded that international law is applicable to the use of cyber operations by States and which recommends following a number of voluntary, non-binding norms of responsible State behaviour[6]. Furthermore the OSCE has adopted cyber confidence building measures (CBMs), which are promoted by the EU and could be taken into account and used when appropriate in this context.

2. MEASURES WITHIN THE FRAMEWORK

The measures within the Framework for a joint EU diplomatic response to malicious cyber activities should serve to protect the integrity and security of the EU, its Member States and their citizens; take into account the broader context of the EU's external relations with the State concerned; provide for the attainment of the Common Foreign and Security Policy (CFSP) objectives as set out in the Treaty on the European Union (TEU) and the respective procedures for their attainment; be based on a shared situational awareness agreed among Member States and correspond to the needs on the concrete situation at hand; be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the malicious cyber activity; respect applicable international law and must not violate fundamental rights and freedoms.

The Framework includes both measures that are suitable for an immediate response to incidents and elements that should be used to encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term.

These measures, which fall within the CFSP and have been defined under the relevant provisions of the Treaties, are presented as options for consideration, where appropriate, and do not preclude action by any individual Member State or action coordinated between Member States. The provisions in the Treaty on European Union covering the CFSP do not affect the rights and responsibilities of the Member States, as they currently exist, for the formulation and conduct of their foreign policy.

---

[6] A/68/98 and A/70/174.

The measures presented are forms of diplomatic, political or economic actions that can be used to prevent or respond to a malicious cyber activity, including in case of malicious cyber activities that do not rise to the level of internationally wrongful acts but are considered as unfriendly acts. The measures in the framework could be used to prevent or respond to malicious cyber activities which may originate from a State or non-state actor or transit through a States' territory, if that State knowingly allows its territory to be used for such activity or knowingly supports it.

In the case where the malicious cyber activity is being carried out by a State, as well as in the case when a State is deemed responsible for the actions of a non-state actor that is acting under its direction or control, or if this State recognizes and adopts the behaviour of such a non-state actor as its own, the full range of measures in the Framework, including restrictive measures against that State, could be used by the EU and its Member States. In the case of a State that knowingly allows its territory to be used for malicious cyber activities, including international wrongful acts using ICTs, against a Member State or the EU, the measures within this Framework could be used to induce such State to ensure that its territory is not used for such activity. The provisions of the Directive on Attacks against Information Systems (2013/40/EU), including its penalties, would be applicable also in the case of criminal actors without significant ties to a State sponsor.

The measures in this Framework are organised in five categories:

(i) Preventive measures;
(ii) Cooperative measures;
(iii) Stability measures;
(iv) Restrictive measures;
(v) Possible EU support to Member States' lawful responses.

These measures could be used either independently, sequentially or in parallel as part of a coherent strategic approach at EU level designed and implemented to influence a specific actor, and should take into account the broader context of EU external relations and the wider EU approach that aims to contribute to the mitigation of cyber threats, conflict prevention and greater stability in international relations.

Category One: Preventive Measures

EU-supported Confidence Building Measures

The EU underlines the importance of confidence-building measures (CBMs) as a means of preventing conflicts and holds that the adoption of this Framework in itself serves a confidence-building function, enhancing much-needed transparency, predictability and stability. CBMs such as those developed by the OSCE are important voluntary measures for the EU and for Member States international and regional dialogue and cooperation in preventing or responding to crises arising from incidents caused by malicious cyber activities.

Awareness raising on EU policies

In addition to ongoing communication actions, EU démarches and EU-led political and thematic dialogues, particularly cyber or security dialogues could be used to make other States aware of the EU's strategic orientation on cybersecurity with regard to cyber issues and inform them about the existence of this Framework. These dialogues could also be used to improve understanding of the national policies of other States with regard to international peace and security with a view to reducing risks of misperceptions or misunderstanding in the case of malicious cyber incidents which may be considered as originating in or transiting through their territory. These dialogues could also help to identify possible other preventive or cooperative measures.

EU cyber capacity building in third countries

EU-led or supported cyber capacity building efforts may contribute to the prevention of cyber incidents affecting the EU or its Member States and contribute to global peace and stability in cyberspace. Such capacity building efforts may for instance aim at further advancing capabilities to investigate and prosecute cyber criminals or increasing incident response capacities in third countries. The EU has several capacity building mechanisms that allow both for a rapid response to prevent and mitigate immediate threats, such as the short-term component of the Instrument contributing to Stability and Peace (IcSP), and provide cyber capacity building aimed at increasing cyber resilience and reducing cyber threats in the long term, whether through for instance the long-term component of IcSP, the European Neighbourhood Instrument (ENI) or any other relevant financing instrument.

Category Two: Cooperative Measures

Cooperation through EU-led political and thematic dialogues or through démarches by the EU Delegations

EU-led political and thematic dialogues or EU-diplomatic démarches could be used to signal the seriousness of the situation for the EU and its Member States, to facilitate the peaceful resolution of an ongoing incident, to ask for assistance or cooperation to mitigate the malicious activity or to ask a third country to join in the response to a malicious cyber activity. The Member States / the Council could invite the EEAS and the Commission to raise a point in the relevant dialogues or exchanges with third countries and international organisations. Démarches are carried out in accordance with the EEAS Guidelines for EU Political démarches.

EU-led political and thematic dialogues or démarches by EU delegations could be especially beneficial for a Member State(s) when there are difficulties in establishing bilateral channels of communication with a given third country but with which the EU or other Member States have a working diplomatic relationship.

Category Three: Stability Measures

Statements by the High Representative and on behalf of the Council of the EU

Issuing a statement expressing concern or condemning general cyber trends or certain cyber activities could have a signalling function and underline awareness, as well as serving as a form of strategic communication and influencing potential aggressors, by signalling the likely consequences of malicious cyber activity, to refrain from engaging in malicious cyber activities. The EEAS Guidelines on Statements and Declarations set out four types of statements at EU level, namely: declarations by the High Representative on behalf of the EU; High Representative statements; Spokesperson statements; and local EU statements. Statements can be requested by the Member States, the HRVP, the HRVP Cabinet or the Spokesperson's Team or proposed by an EU delegation. Declarations by the High Representative on behalf of the EU are consulted with Member States, usually by means of COREU silence procedure.

EU Council conclusions

Issuing general or specific Council conclusions on malicious cyber activities could have a signalling function, set out action and underline awareness and determination of the EU and its Member States to prevent and respond to potential attempts to weaken EU unity or positions of the EU and its Member States, through malicious cyber activities. The Council could use this instrument to express a political position, to invite another EU institution to take action, or to prepare a proposal for coordinated Member States' action on a specific issue.

Diplomatic démarches by the EU delegations

EU Delegations or Member States locally representing the EU could carry out EU démarches to a number of different ends. When one or more Member States are impacted by a malicious cyber activity, it could be beneficial to jointly contact States exercising jurisdiction over these territories that have been used for conducting the malicious activity. A démarche could be used to raise concerns about certain malicious activities, signal the seriousness of the situation for the EU and its Member States, to facilitate the peaceful resolution of an ongoing incident, to ask for assistance or cooperation to mitigate the malicious activity or to ask a third country to join in the response to a malicious cyber activity. A démarche could also be a way to signal the likely consequences of a malicious cyber activity or to signal that the origins of the activity are known and that these are considered as contrary to international voluntary non-binding norms of responsible State behaviour or to international law as the case may be. This activity could take place without prejudice to any ongoing or future operational actions conducted in order to mitigate the impact of the malicious cyber activities. The benefit of such signalling is that it can generally be done without requiring firm attribution. Démarches are carried out in accordance with the EEAS Guidelines for EU Political Démarches.

Signalling through EU-led political and thematic dialogues

EU-led political and thematic dialogues, particularly cyber or security dialogues, could be used to raise concerns about certain malicious cyber activities, to signal the seriousness of the situation for the EU and its Member States, to facilitate the peaceful resolution of an ongoing incident, to signal the likely consequences of a malicious cyber activity or to signal the origin of the activity when known and that these are considered as contrary to international voluntary non-binding norms of State behaviour or to international law, as the case may be. The Member States / the Council can invite the EEAS and the Commission to raise a point in the relevant dialogues or exchanges with third countries and international organisations and multilateral bodies such as the UN, OSCE, NATO, WTO and G20.

Category four: EU Restrictive measures

The EU may impose restrictive measures[7] against third countries, entities or individuals on the basis of a Council decision adopted under Article 29 TEU coupled with a Council regulation setting out the necessary measures for its operation, adopted under Article 215 TFEU. If necessary, the EU may impose restrictive measures, as adopted under the relevant provisions of the Treaties, in response to malicious cyber activities. The imposition of restrictive measures shall be done in accordance with the respective procedures agreed by Member States set out in the guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy. In general, restrictive measures aim to bring about a change in policy or activity by the target country, government, entity or individual concerned in line with the objectives set out in the Council decision. Such measures can include, *inter alia*, travel bans, arms embargos, freezing funds or economic resources.

Category five: Possible EU support to Member States' lawful responses

The measures within this Framework can also be used to support or complement lawful responses by Member States. The EU could, upon request of the concerned Member State(s), provide support to Member States that individually or collectively resort to responses in accordance with international law that are not available within the CFSP. Such responses by Member States can take the form of any lawful measure, ranging from diplomatic steps similar to those outlined above, to the use of stronger individual or cooperative responses.

A Member State that is the victim of malicious cyber activity that constitutes an internationally wrongful act may, under certain conditions, lawfully resort to non-forcible and proportionate countermeasures. These countermeasures constitute actions directed at another State that is responsible for the internationally wrongful act, which would otherwise violate an obligation owed to that State. Such non-forcible countermeasures are conducted to compel or convince the latter to cease the malicious cyber activity, in compliance with its international obligations.

[7] doc. ST 11205/12 + COR 2 - Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy.

In grave instances, malicious cyber activities could amount to a use of force or an armed attack within the meaning of the Charter of the United Nations. In this latter case, Member States may choose to exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the Charter of the United Nations and in accordance with international law, including international humanitarian law. A Member State may also choose to invoke article 42 (7) TEU to call on other Member States to provide aid and assistance.

3. PROCESS TO INVOKE THE MEASURES WITHIN THE FRAMEWORK

The measures part of this Framework will be implemented as far as possible through the use of existing mechanisms. These measures should be used in a coherent and consistent manner: this requires *inter alia* a comprehensive shared situational awareness of malicious cyber activities.
In case of a crisis for which the Integrated Political Crisis Response (IPCR) arrangements[8] have been activated, following the appropriate agreed procedures[9] to handle the crisis at EU level, measures within this Framework could be part of the EU response at the political level. In this case the decision-making process of IPCR will apply. The IPCR arrangements are designed to allow a timely policy coordination and response at the EU political level (COREPER/Council) in the event of major emergencies or crises. The IPCR is also used to coordinate, at the strategic/political level, the response to the invocation of the solidarity clause (Art. 222 TFEU) to ensure the coherence and complementarity of Union and Member State action. The arrangements for the implementation by the Union of the solidarity clause are defined by Council Decision 2014/415/EU[10].

In situations where the malicious cyber activity has not led to the activation of the IPCR, the following procedure to invoke the measures within the Framework applies:

---

8 doc. 1078/13.

9 The Commission has presented a recommendation for a Blueprint for coordinated response to large-scale cross border cybersecurity incidents and crises that describes how existing and established Crisis Management principles and mechanisms make full use of existing cybersecurity entities on EU level and cooperation mechanisms between the Member States.

10 OJ L192, p. 53 of 1.07.2014.

Preparing a decision

Before any measure can be considered, timely and continuous sharing of sufficient information will be of key importance for the EU and its Member States. Decisions about the measures within this Framework should follow the normal decision making processes for those measures and correspond to the needs of the concrete situation in view of avoiding imposing measures that could have escalatory effects based on misinterpretations. Shared situational awareness agreed among Member States, in particular with regard to restrictive measures or possible EU support for Member States' lawful responses, has the purpose of enabling the EU and Member States to take a collective decision whether or not to use one or several measures as part of this Framework. Member States are not obliged to provide information or analysis when it considers this as contrary to the essential interests of its national security.

Ongoing exchanges on the cyber threat landscape, with the support of the appropriate EU institutions, agencies or bodies and, where appropriate, complemented by international partners or international organisations, will enable Member States to develop and maintain a shared understanding on malicious cyber activities and how these affect the Member States and the EU.

The EU Intelligence and Situation Centre (Intcen), in close cooperation, when necessary, with the CSIRTs network chaired by the rotating Presidency, the EC3, ENISA or CERT-EU, when appropriate, will assume a leading role in aggregating all-source information and preparing an analysis and political assessment about a single, or across events. This will provide the shared situational awareness needed for the decision-making on the measures within this Framework. The regular EU Cybersecurity Technical Situation Report on incidents and threats as prepared by ENISA could also be helpful in this regard. Improved cooperation and regular

exercising of relevant processes between these entities could provide more coherence between the relevant information streams, including for the purpose of early warning, as also referred to in the relevant Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[11]. The Horizontal Working Party on Cyber Issues will play a central role in coordinating, preparing and evaluating the result of exercises based on the given implementing guidelines as well as preparing relevant political guidance for the conduct of EU-wide cybersecurity exercises, as appropriate.

At policy level, in order to enhance internal coordination and to help develop a comprehensive and coherent EU approach on cyber issues, the Horizontal Working Party on Cyber Issues, chaired by the rotating Presidency, and the Political and Security Committee (PSC) will play a central role in the preparation of and decision-making on the measures selected for implementation.

Following the analyses prepared by the EEAS, any Member State, the High Representative or EEAS may submit an initiative or proposal to the Council. Any Member State is free to launch an initiative or to make a proposal at any time. On the basis of this initiative or proposal, Member States can continue exchanging relevant information enhancing the shared situational awareness and deliberate on whether any action should be taken.

[11] JOIN(2017) 450 final

Attributing a Malicious Cyber Activity

The shared situational awareness may include elements on attribution and in that case requires particular attention, as attribution of a malicious cyber activity remains a sovereign political decision based on all-source intelligence, taken on a case-by-case basis. Every Member State is free to make its own determination with respect to attribution of a malicious cyber activity. Attribution could be established, based on an analysis of technical data and all-source intelligence, including on the possible interests of the aggressor. The norms agreed by UN as voluntary non-binding norms of State behaviour reflect the principle that States should not knowingly allow their territory to be used for internationally wrongful acts, and should respond to appropriate requests for assistance by another State. The common expectations set by these agreed norms can be used to support the attribution process. The EU Intelligence and Situation Centre (Intcen), in close cooperation, when necessary, with the CSIRTs network chaired by the rotating Presidency, the EC3, ENISA or CERT-EU, when appropriate, plays a valuable role in this regard by sharing its analyses and information related to the origin of the malicious cyber activity in accordance with their mandate.

Member States may employ different methods and procedures to attribute malicious cyber activities and different definitions and criteria to establish a degree of certainty on attributing a malicious cyber activity. This framework does not attempt to harmonise those methods, procedures, definitions and criteria as attribution is a sovereign process. However, in order for a joint EU diplomatic response to be effective, the mechanism in this Framework aims to facilitate the decision-making process, including the process for collectively assessing the information provided and designing and implementing a measure or a coherent approach including several measures based on a shared situational awareness and a shared understanding on the origin of the malicious cyber activity, when necessary.

Member States can ensure an effective joint EU diplomatic response to malicious cyber activities by sharing relevant information through the existing mechanisms within the relevant constituencies or by providing their assessment on the origin of the malicious cyber activity to the appropriate preparatory body. It must be noted that there is no international legal obligation to reveal evidence on which attribution is based prior to taking an appropriate response, although it is recognised for the purposes of this Framework that Member States may choose to share such evidence, for instance in order to give effect to a joint EU diplomatic response or convince other Member States to join them in a response to the malicious cyber activity.

Not all of the measures presented in this Framework will require attribution: they are a means of preventing or resolving a cyber incident, expressing concerns and signalling them in another way. Furthermore, the use of the measures within the Framework can be tailored to the degree of certainty that can be established in any particular case.

Making a decision

The various diplomatic response measures fall under various competencies. These measures can be employed either by an individual Member State, collectively with other Member States, by Member States in cooperation with the EU institutions or by the EU institutions themselves. The measures could be used either independently, sequentially or in parallel as part of a coherent strategic approach on EU level designed and implemented to influence a specific actor.

In accordance with the scope of its competences and responsibility, the Horizontal Working Party on Cyber Issues, when necessary with political guidance from PSC, will act as a preparatory body for the purpose of invoking the measures within this Framework through which the initiative or proposal for a response could be discussed by Member States. Cooperation with relevant regional and thematic Council working groups could be sought where necessary. When the use of restrictive measures is concerned, the Foreign Relations (RELEX) Counsellors Working Party is in the lead on all legal, technical and horizontal aspects of the proposed restrictive measures. When Member States or an EU institution consider it appropriate, the PSC will deliberate on the initiative or proposal and provide political orientation to the respective working party, notably on the type of measure selected for further proceedings. The Chair of the Council preparatory body where the initiative or proposal originated from, where appropriate in cooperation with the Chair(s) of the other preparatory Council bodies involved, can organise meetings and when necessary, to discuss the parameters of the initiative or proposal. Experts from Legal Services, the EEAS and where necessary, the European Commission, should assist during the deliberations.
The decision to implement a measure within this Framework should be accompanied by the political and legal context of the measure, including technical details where appropriate. In addition to the relevant provisions of the TEU and TFEU and the procedures and guidelines for their attainment, this may include references to existing international law, voluntary non-binding norms of responsible State behaviour, OSCE confidence-building measures or any other applicable international agreement. Furthermore, the decision should set out the specific tasks with regard to the implementation of the measure.

The decision on implementing a measure should be taken at the appropriate level, to be defined on a case-by-case basis, by PSC, COREPER or the Council. Under the responsibility of the Council and of the High Representative, the PSC ensures the political control and strategic direction of crisis management operations referred to in Article 43 TEU, including conflict prevention tasks and may, within this Framework and when it is authorised to do so by the Council, take decisions in this area[12].

Appropriate coordination with like-minded partners and international organisations should be envisaged.

[12] Article 38 TEU.

Following a decision

After the decision has been taken about the measure within this Framework, it could, when appropriate, be actively and systematically communicated by the EU and its Member States inside and outside of the EU. The communication should correspond to the needs of the situation at hand and could vary in form, detail and timing and could have multiple objectives and effects. EEAS' StratCom, the HRVP Spokesperson and the Council Press Office could all play valuable roles as appropriate. Public communication could for instance be done via a formal and public Statement or Declaration on a political level, an off-the-record statement or a reactive line-to-take.
When communicating a decision, it is important that the reasons for which measures are taken are made known and the relevant audience targeted.

Proper attention by the appropriate bodies shall be given to the follow-up of a decision and its possible repeal.

DELETED FROM THIS POINT UNTIL PAGE 40

EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security

New York, 26/10/2018 - 20:26, UNIQUE ID: 181026_26

Statements on behalf of the EU

26 October 2018, New York – European Union Statement by Ms. Narcisa Vladulescu, Counsellor, European Union Delegation to the UN, at the 73rd Session of the United Nations General Assembly First Committee Thematic Discussion on Other Disarmament Measures and International Security

Mr. Chairman,

I have the honour to speak on behalf of the European Union. The Candidate Countries the former Yugoslav Republic of Macedonia*, Montenegro*, and Albania*, as well as the Republic of Moldova and Georgia, align themselves with this statement.

The EU reiterates its concerns raised by the increased ability and willingness of some States and non-State actors to pursue their objectives by undertaking malicious cyber activities that threaten international peace and security.

In that light, the EU is gravely concerned with the attempt by the Russian military intelligence service (GRU) to undermine the integrity of the Organization for the Prohibition of Chemical Weapons (OPCW), as reported by the Netherlands, which hosts the organisation. This aggressive cyber operation demonstrates grave contempt for the solemn purpose of the OPCW, which works to eradicate chemical weapons worldwide, notably under a UN mandate. The EU and its Member States deplore such hostile cyber operations which undermine international law and international institutions. We reaffirm our commitment to uphold the rules-based

international system, and defend international institutions from those that seek to do them harm, by improving and strengthening stability in cyber space, including through the UN.

Recognising the challenges posed by cyber threats, EU Member States have adopted a “Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities”. This Framework contributes to conflict prevention, cooperation and stability in cyberspace by detailing how measures within the EU’s Common Foreign and Security Policy, including restrictive measures, can be used to prevent and respond to malicious cyber activities. The measures within the Framework aim to protect the integrity and security of the EU, its Member States and their citizens, encourage cooperation, facilitate mitigation of threats and influence the behaviour of potential aggressors, both State and non-State actors, in the long term. By providing clarity on EU response to malicious cyber activities, the Framework contributes to international peace and security.

On 18 October 2018, the European Council called for measures to build strong cyber security in the European Union. EU leaders referred in particular to restrictive measures able to respond to and deter cyber-attacks.

Mr. Chairman,

The EU and its Members States promote the establishment of a strategic framework for conflict prevention, cooperation and stability in cyberspace that is based on the application of existing international law, and in particular of the UN Charter in its entirety, the development and implementation of universal norms of responsible state behaviour, and regional confidence building measures between States.

The EU recognises the role of the United Nations in further developing norms for responsible state behaviour in cyberspace. The EU emphasises that the consecutive UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, over the years, have reached consensus on a number of measures contributing to greater cyber stability, including on norms, rules and principles of responsible behaviour of States, the promotion of confidence building measures, capacity building and the application of international law in cyberspace. We should continue to build on this work.

Regarding the application of international law, the EU recalls that "International law and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."

The EU recalls that the 2013 and 2015 reports of the Group of Governmental Experts, which the General Assembly has repeatedly endorsed, contain important recommendations that States should fully implement and in particular 11 voluntary, non-binding norms, rules and principles of responsible behaviour of States that are listed in paragraph 13 of the 2015 GGE report, which include, among others, the following: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs", "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty", and "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions". The GGE also stressed that States should guarantee full respect of human rights, including the right to privacy and freedom of expression.

The EU also emphasises the following international principles deriving from the UN Charter which, *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 by 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; the inherent right to self-defense against an armed attack; respect for human rights and fundamental freedoms. We also believe that international humanitarian law applies to cyber operations in war time, including the principles of precaution, humanity, military necessity, proportionality and distinction.

The EU supports and encourages the development of regional confidence building measures, which are an essential element to increase cooperation and transparency and reduce the risk of conflict. Implementing cyber security confidence building

measures in the OSCE, ARF, OAS and other regional settings will increase predictability of State behaviour and further contribute to stabilising cyberspace.

In order to build trust and strengthen cooperation among States, as well as to implement the cyber norms, the EU acknowledges the role of capacity building, and stands ready to continue assistance to third countries in responding to cyber threats and increasing law enforcement capabilities to investigate and prosecute cybercrime. The EU considers it essential to advance cybersecurity capacity building through the development of appropriate domestic policies and legislation, protection of infrastructure, provision of training as well as upholding the rule of law in cyberspace.

Furthermore, the EU recognises that the interconnected and complex nature of cyberspace requires joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced, and calls on these stakeholders to recognise and take their specific responsibilities to maintain an open, free, secure, stable, accessible and peaceful cyberspace.

Mr. Chairman,

The EU and its Member States reaffirm their commitment to improving and strengthening stability in cyberspace. We should all recognise the achievements of the previous UN GGEs which provide the basis to continue work. We call on the UN Secretary General to continue to study and implement the measures to promote stability and security in cyberspace, and convene a new Group of Governmental Experts in 2019 with a view to providing a consensus report to the General Assembly.

To be successful, the GGE should remain effective and dynamic, and be able to deliver detailed results**.** Its mandate should be focused and guided by cumulative conclusions agreed in previous GGE reports, including the applicability of existing international law in cyberspace and the 11 norms of responsible State behaviour listed in paragraph 13(a)-(k) of the 2015 GGE report.

The EU believes that UN Member States, and in particular future GGE members, should submit national contributions on the subject of how international law applies to the use of ICTs by States as it builds on the consensus view that international law applies to cyberspace and advances the global understanding on national

approaches which is fundamental to maintaining long-term peace and security and reducing the risk of conflict in cyberspace. Such contributions could be annexed to the GGE's report.

Furthermore, the EU considers the aspect of consulting the UN membership as well as other stakeholders an important element of the mandate. The GGE shall hold regular, open-ended, inter-sessional consultations with the wider UN membership and interested stakeholders.

In conclusion, the EU will prioritise a resolution that reaffirms the consensus views articulated in previous Groups of Governmental Experts reports, including norms, rules and principles of responsible behaviour of states, confidence building measures, international law and capacity building and the importance of respect for human rights and fundamental freedoms in cyberspace. We note that draft Resolution L.37, co-sponsored by all EU Member States, is based on the previous First Committee resolutions that usually enjoy consensus. We note with regret that the traditional sponsor of the ICT Resolution, the Russian Federation, has chosen to pursue a different course of action this year. In particular, we would like to point to operational paragraph 1 of its current draft, which offers a selective list of recommendations of the previous UN GGE reports and norms established by a regional organization. Imposing this **o**n UN Member States through a UN General Assembly Resolution would set an unwelcome precedent for cyber security and all other areas of future work. It would undermine the consensual recommendations of the previous UN GGEs and prejudge the outcome of any consultative process which is neither inclusive nor open-ended.

Thank you, Mr. Chairman.

---

* *The former Yugoslav Republic of Macedonia, Montenegro and Albania continue to be part of the Stabilisation and Association Process.*

Council of the European Union

Brussels, 19 September 2018
(OR. en)

12187/18

CYBER 196
CFSP/PESC 829
COPS 322
RELEX 751
JAIEX 110
TELECOM 293
POLMIL 141

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	12094/18
Subject:	EU Lines to take on a draft resolution on "Developments in the field of information and telecommunications in the context of international security"

Delegations will find in annex the "EU Lines to take on a draft resolution on "Developments in the field of information and telecommunications in the context of international security" endorsed by the COREPER of 17 September 2018.

ANNEX

EU Lines to take on a draft resolution on "Developments in the field of information and telecommunications in the context of international security"

- The EU promotes the establishment of a strategic framework for conflict prevention, cooperation and stability in cyberspace that is based on the application of existing international law, and in particular of the UN Charter in its entirety, the development and implementation of universal norms of responsible state behaviour, and regional confidence building measures between States.

- The EU recognizes the role of the United Nations in further **developing norms for responsible state behaviour in cyberspace** and recalls that the outcomes of the United Nations Group of Governmental Experts discussions have articulated a consensual set of norms and recommendations, which the General Assembly has repeatedly endorsed, and which States should take as a basis for responsible state behaviour in cyberspace.

- The EU will prioritise **a consensus resolution that refers to the consensus views** articulated by several previous Groups of Governmental Experts, such as norms, rules and principles of responsible behaviour of states, confidence building measures, international law and capacity building, as a basis for further work. The resolution should also underline the importance of respect for human rights and fundamental freedoms in cyberspace.

- The EU has a clear preference for a short and precise resolution that calls for the creation of the new UN Group of Governmental Experts that builds on the discussions of the previous Groups of Governmental Experts and remains an effective and dynamic format. The mandate of the group should be focused, and guided by the previous GGE reports, including the applicability of international law in cyberspace and the 11 norms of responsible State behaviour listed in paragraph 13(a)-(k) of the UNGGE report 2015.

– The EU supports the UN GGE consensus view that **international law**, and in particular the Charter of the United Nations, is applicable also in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. In line with this position, "*the EU does not call for the creation of new international legal instruments for cyber issues"*[1].

– The EU believes that UN member states, and in particular future GGE members, should submit national contributions on the subject of how international law applies to the use of ICTs by States as it builds on the consensus view that international law applies to cyberspace and advances the global understanding on national approaches which is fundamental to maintaining long-term peace and security and reducing the risk of conflict in cyberspace. Such contributions could be annexed to the report.

– The EU **supports the continuation of the process** to discuss norms for responsible state behaviour, confidence building measures, and international law under the UN First Committee, and the establishment of a new GGE. The expert group should not exceed 20 or 25 experts in order to keep the dynamism and the ability to deliver detailed results within a year. It would help the process if the composition of the group would be chosen among the states with the most cyber expertise, and taking into account regional representation.

– The EU recognizes that the interconnected and complex nature of cyberspace require**s** joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced and calls on these stakeholders to recognize and take their specific responsibilities to maintain an open, free, secure and stable cyberspace. The EU considers the aspect of consulting the wider UN membership as well as other stakeholders as an important element in the mandate, and the group shall hold repeated, open-ended, inter-sessional consultations with the wider UN membership and interested stakeholders.

***

[1] *Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 11357/13, 2013.*

BACKGROUND

UN General Assembly 73 – First Committee

Four UN Groups of Governmental Experts on "Developments in the Field of Information and Telecommunications in the Context of International Security" gathered since 2009, and reported to the UNGA 1st Committee. Three reports have been issued during this period – in 2010, 2013 and 2015. The UNGGE 2016-2017 concluded its work without consensual report, and UNGA72 postponed substantial decisions to UNGA73.

The 1st Committee of the UN General Assembly this year could adopt a resolution to establish another UNGGE in order to continue the discussions on norms, rules and principles, of responsible behaviour of states, confidence building measures, international law and capacity building in the context of international security.

As stated in the 20 November 2017 Council Conclusions, the Council "*CALLS UPON the EU and its Member States to promote the establishment of a strategic framework for conflict prevention, cooperation and stability in cyberspace that is based on the application of existing international law, and in particular of the UN Charter in its entirety, the development and implementation of universal norms of responsible state behaviour, and regional confidence building measures between States;*

RECOGNISES the role of the United Nations in further developing norms for responsible state behaviour in cyberspace and recalls that the outcomes of the United Nations Group of Governmental Experts [UNGGE] *discussions over the years have articulated a consensual set of norms and recommendations, which the General Assembly has repeatedly endorsed, and which States should take as a basis for responsible state behaviour in cyberspace;*"

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 51)