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.