Council of the European Union

Brussels, 18 March 2019
(OR. en)

6852/1/19
REV 1

LIMITE

CYBER 57
CFSP/PESC 156
COPS 56
RELEX 188
JAIEX 25
TELECOM 91
POLMIL 18
HYBRID 7

NOTE

From:	EEAS
To:	Delegations
Subject:	Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities - Attribution of malicious cyber activities - discussion of a revised text

Delegations will find in Annex a revised version of the non-paper on attribution of malicious cyber activities in the context of the Framework for a joint EU diplomatic response to malicious cyber activities prepared on the basis of the discussions in the Horizontal Working Party on Cyber Issues held on 5 March 2019 and the written comments sent by Member States.

The above mentioned document will be presented for discussion at the meeting of the Horizontal Working Party on Cyber Issues on 20 March 2019. Following that discussion, the EEAS intends to organise, as requested by Member States, a scenario-based discussion that would allow to test the process as set out in the paper, with a view to submitting it for endorsement by PSC and adding it as annex to the implementing guidelines after that.

New changes in comparison to the previous version are indicated in **bold** and **underlined** and deleted text is marked with ~~strike through~~.

ANNEX

NON-PAPER ON ATTRIBUTION OF MALICIOUS CYBER ACTIVITIES IN THE CONTEXT OF THE FRAMEWORK FOR A JOINT EU DIPLOMATIC RESPONSE TO MALICIOUS CYBER ACTIVITIES

INTRODUCTION

The EU has stepped up its response to malicious cyber activities by adopting a Framework for a joint EU diplomatic response to malicious cyber activities (the "cyber diplomacy toolbox"[1]). The Framework offers the full use of measures within the Common Foreign and Security Policy (CFSP), including, if necessary, restrictive measures.

Generally, attribution can be defined as a practice of assigning responsibility for a malicious cyber activity to a specific actor. After responsibility has been assigned, that attribution may be accompanied by a diplomatic response and / or communicated to third countries, the responsible actor, or made public. However these further steps may not necessarily take place. Attribution is a sovereign political decision taken on a case-by-case basis.

Not all diplomatic measures require attribution, for example diplomatic measures may be involved in preventing or resolving a cyber incident, expressing concerns and signalling them in another way. Some measures, however, may benefit from attribution.

In order for the EU to implement a diplomatic response that requires attribution, **all EU Member States need to agree on this attribution.** ~~attribution decisions by EU Member States should be coordinated. Such~~ **A** coordinated attribution **at EU level** requires consensus amongst all Member States.

This non-paper aims to facilitate the process of coming to such coordinated attribution at an EU level, and therefore suggests a process for this, as well as the elements and questions that could be taken into account during such discussion.

---

1 9916/17.

This paper should be seen as an annex to the Framework for a joint EU diplomatic response to malicious cyber activities ("cyber diplomacy toolbox"), and in particular its implementing guidelines[2], and could be useful in cases where coordinated attribution is desirable in order to effectively implement a joint EU diplomatic response.

ATTRIBUTION

For the purpose of this Framework ~~Generally~~, attribution ~~can be~~ **is** defined as a practice of assigning responsibility for a malicious cyber activity to a specific actor. Attribution is a sovereign political decision 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.

The sovereign decision by an EU Member State to attribute can lead to different strategies and posture, including ~~by~~ the possibility to communicate the attribution to third countries, the responsible actor, or the public, as well as by coordinating the attribution at EU level and / or through a joint effort by using the Framework for a joint EU diplomatic response to malicious cyber activity.

It should be noted that attribution is not a measure, an end, or a strategy in itself. Attribution is the result of a process that determines responsibility for a malicious cyber activity, and could be a means to contribute to the implementation of a measure that would require such judgement.

Attribution is a decision following a process consisting of several stages. The process to come to a political decision to attribute a malicious activity to an actor could include more technocratic stages such technical (cyber-forensic analysis) and all-source information (analysis and assessment) as well as stages that include legal and political assessments.

[2] 13007/17.

COORDINATED ATTRIBUTION AT EU LEVEL

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 paper does not attempt to harmonise those national methods, procedures, definitions and criteria.

It should however be noted that a better understanding of how **the process of** attribution is conducted at the national level has the potential to improve the process of coming to coordinated attribution at EU level. Enhanced capacity at EU level to swiftly and effectively coordinate national decisions on attribution could in many instances be assumed to sustain the ability by the EU and its Member States to jointly impose measures on those who violate international law, and / or do not abide by the framework for cyber stability that has been agreed upon in the UN.

As well, coordinated attribution by EU Member States, when communicated to others, either privately or publicly, could have the potential to strengthen the ability to influence the behaviour of potential malicious actors in cyberspace as compared to attribution by just one or a group of Member States. The prospect that coordinated attribution could signal strong EU Member States' capabilities to establish with certainty that an actor holds responsibility for a malicious cyber activity could be also taken into account, as it can diminish an actor's willingness and ability to carry out further malicious activities.

ELEMENTS TO EXCHANGE ON ATTRIBUTION IN THE COUNCIL

As stated in the implementing guidelines to the Framework, before a measure can be considered, timely and continuous sharing of information is of key importance for the EU and its Member States. It applies particularly in the context of coordinated attribution. However, it must be noted that there is no international legal obligation to reveal ~~evidence~~ **information** on which attribution is based. Attribution is a sovereign political decision.

While Member States recognize that information sharing could contribute to for instance convincing other Member States to join them in attributing a malicious cyber activity or give effect to a joint EU diplomatic response, a possible decision to reveal such information will be taken on a case-by-case basis without recognition of precedence.

During a discussion on a particular cyber threat or trend, Member States could exchange relevant information in order to build shared situational awareness. Furthermore, Member States could deliberate on whether any diplomatic response should be taken, and whether it is necessary and possible to coordinate attribution. **Member States may also wish to develop a shared understanding on the degrees of certainty on the basis of the assessments put forward by Member States.**

To support the situational awareness, the EU Intelligence and Situation Centre (INTCEN) ~~assumes, in accordance with the implementing guidelines to the Framework, a role in aggregating all-source information and preparing an analysis about a single, or across events.~~ **could share its assessment with Member States in accordance with their mandate. The mandate of the INTCEN primarily consists of providing EU decision makers with intelligence-based assessments, based on voluntary contributions from Member States. This role does not change when dealing with malicious cyber activities. INTCEN should reflect the state of the art of intelligence, including the nuances and potential differences between the contributions from Member States. This assessment will therefore at EU level** ~~It should however be noted that national assessment of Member States attained through their respective national processes will be used to determine each Member State's decision and that the assessment produced by INTCEN will be~~ **only be** introductory, complementary or accessory. **It should be noted that an assessment by INTCEN does not substitute Member States analyses and cannot be considered in itself as a shared understanding of the threat**.

Law enforcement, judiciary, intelligence or diplomatic channels might be used to **further exchange information between Member States, or** request more information from ~~Member States,~~ third countries or other relevant bodies such as international partners and organisations **by Member States and / or the EEAS.** In this regard, appropriate attention should be given to the classification of information, intelligence, the overall assessment as well as the interests of all parties involved.

~~In order for the EU to be able to swiftly and effectively coordinate on attribution, Member States may develop a shared understanding on the degrees of certainty on the basis of the assessments put forward by Member States, to which INTCEN might contribute with its aggregated analyses from voluntary contributions from Member States as well as from within the EU system. An assessment by INTCEN should refer to details regarding typologies of the open source information and intelligence adopted for the analysis and an indication of the number of Member States who provided information on a voluntary basis. In order to support the awareness INTCEN's assessment should be accompanied by degrees of certainty ranging from remote chance (less than 5%) up to almost certain (more than 95%)[3].~~

The norms agreed by the UN as voluntary non-binding norms of State behaviour include, inter alia, that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, and should respond to appropriate requests for assistance by another State. The common expectations set by these agreed norms could also be used to support the attribution process.

Based on the coordination within the HWPCI, to be shared and, when necessary, discussed with relevant Council preparatory bodies when appropriate (e.g. regional or thematic Council WG[4]) and with political guidance from the Political and Security Committee (PSC) when appropriate, the Council may decide at the appropriate level, to be defined on a case-by-case basis, by PSC, COREPER or the Council, whether or not to coordinate on attribution.

PROCESS TO DECIDE ON COORDINATED ATTRIBUTION BY THE COUNCIL

In case of an initiative or proposal by one or several Member States to coordinate attribution, including by those affected Member States who detected malicious cyber activities and request to assess the possibility of attribution further with the support from other Member States, it would be useful for the Council to consider the following:

~~[3] An assessment by INTCEN can be established with degrees of certainty ranging from remote chance (less than 5%) up to almost certain (more than 95%). Uncertainty yardstick in Annex.~~

[4] As enlisted in the document 10925/18.

1. The Council may agree on whether coordinated attribution is needed for the joint EU response to be effective, specifying the purpose and assessing the effect. **It should be noted that not all diplomatic measures require attribution, for example diplomatic measures may be involved in preventing or resolving a cyber incident, expressing concerns and signalling them in another way. Some measures, however, may benefit from attribution.**

2. Member States may continue to share information on the malicious activity, as well as, for the purpose of coordinated attribution, the perceived actor and, when applicable, its sponsor.

   Based on this, the Council may take a decision about whether the situational awareness is sufficient to take a decision on coordinate**d** attribution or whether more information is needed to improve the accuracy.

3. Based on sovereign considerations as well as the situational awareness on EU level, the Council may **decide** to coordinate attribution, and secondly, whether the attribution should be made public or not, and to what detail, if any. When discussing the appropriateness of coordinating attribution, and while deciding whether to communicate the coordinated attribution to others, either privately or publicly, it could be useful for the Council to consider the following:

   - the contribution to the protection of the integrity and security of the EU, its Member States and their citizens;

   - the contribution to the advancement of responsible state behaviour, including compliance with international law and respect for voluntary norms;

   - the impact on the ongoing work of services such as law enforcement or intelligence services;

   - the likelihood of a counter-response by ~~the~~ **any** actor (risk of escalation);

   - the consequences for existing EU external relations, at the international, regional and bilateral levels;

- the reputation and credibility of the EU (risk of the bystander effect, risk of manipulation, risk to the EU's strategic autonomy);
- the precedence of a malicious cyber activity;
- the second-order effects;
- the predictability and coherence of joint EU responses in previous and/or future cases.

4. To accompany the coordinated attribution, the Council may decide whether and if yes, which diplomatic measure to take in response, who will implement this measure and how the implementation will be coordinated, in accordance with the implementing guidelines.

   Who will implement the diplomatic measure and how the implementation will be coordinated also depends on the nature of the response measure and the respective procedures for its attainment.

   In line with the implementing guidelines, the use of the measures within the Framework could be tailored to the degree of certainty that Member States have.

5. Following a decision on coordinated attribution and / or decision to take a joint EU diplomatic response, the Council may explore whether the EU can and should work together with third countries and / or international or regional organisations to respond to the malicious cyber activity, where necessary, appropriate and possible including coordination on attribution.

REQUESTING OR PROVIDING SUPPORT

In case of a third country requesting the EU to support the response to a malicious cyber activity through a joint EU diplomatic response, or the EU requesting support of third countries to respond to a malicious cyber activity, sharing of information by the third country and / or Member States in a timely manner is vital for the described decision-making process to be effective and efficient. The options for information exchange with certain third countries[5] should be explored in the context of the Framework, with appropriate attention given to the **origin and** classification of information, intelligence and the overall assessment.

---

[5] Parties to be validated by the relevant Council body.

~~**ANNEX I**~~

~~**Qualitative Term**~~	~~**Associated Probability Range**~~
~~Remote chance~~	~~> 0% - 5%~~
~~Highly unlikely~~	~~10% - 20%~~
~~Unlikely~~	~~25% - 35%~~
~~Realistic probability~~	~~40% - 50%~~
~~Probable or likely~~	~~55% - 75%~~
~~Highly likely~~	~~80% - 90%~~
~~Almost certain~~	~~95% - <100%~~