Council of the European Union

Brussels, 4 April 2016
(OR. en)

5797/3/16
REV 3

LIMITE

CYBER 9
RELEX 78
JAIEX 12
TELECOM 12
COPS 35
POLMIL 31

NOTE

From:	Presidency
To:	Delegations
Subject:	Non-paper: Developing a joint EU diplomatic response against coercive cyber operations

Delegations will find in the Annex a revised version of the non-paper of the Presidency reflecting the discussion of the FOP on cyber issues of 1 March 2016 and the written comments received.

The Presidency would like to express its gratitude to Member States for their numerous and helpful contributions and offers as a reaction thereto the points below:

1. The Presidency acknowledges the practical difficulties surrounding the issue of attribution and has no intention of ignoring them while progressing with the work on this matter. However, it should be pointed out that several of the instruments presented in the paper as options are attribution- neutral: their application does not require directing accusations against other States as they are means of expressing concerns and signalling them in another way. For instance, regardless of the actual perpetrator, diplomacy can be used to encourage countries that serve as unwitting proxies for a coercive cyber operation to take action to mitigate the activity [1].

[1] For instance, the 2015 Report of the UN Group of Governmental Experts recommends that: *States should respond to appropriate requests to mitigate malicious ICT activity aimed at another State's critical infrastructure emanating from their territory*".

Furthermore, some of these instruments can be tailored to reflect the specific degree of attribution that can be established in a particular case whereas for the rest which require the establishment of a certain level of attribution, further discussions would be necessary and could be continued as part of the proposed Framework. The Presidency wishes to emphasize that it attaches a great value to them, especially in view of clarifying what is and what is not possible at EU level in that respect.

2. For purposes of clarity, a working definition of the term 'coercive cyber operation' has been introduced, which by no means should be regarded as a legal definition.

3. It should be further emphasized that the various proposed diplomatic response instruments represent a range of measures that fall under various competencies. These measures can either be employed by Member States solely in collaboration with other Member States, by Member States in cooperation with the EU institutions or by the EU institutions themselves. In most cases, the initiative for employing these measures lies with the Member States.

4. Several of the issues raised by Member States in their extensive comments such as the relationship between a possible diplomatic response toolbox and the NIS Directive implementation or the NATO cyber defence efforts go beyond the scope of the present revision of the paper. They in particular, but also other issues will require detailed further discussion by Member States in coordination with the EEAS as proposed in the Framework.

5. Next it should be underlined that these optional measures are complementary to, but not a replacement of, existing EU cyber diplomacy engagement. The non-paper assumes that current diplomatic efforts[2], such as supporting the wider ratification of the Budapest Convention and reaching common positions in international fora, will continue unabated. Yet those efforts are impacted by increasing global cyber security concern in general. Therefore the value of the suggested optional diplomatic measures lays in the fact that they are intended to respond to specific incidents threatening the security of the EU and its citizens and territory.

[2] Especially the diplomatic actions based inter alia on the EU Cyber Security Strategy of 25 June 2013, the EU Human Rights Guidelines on Freedom of Expression Online and Offline of 12 April 2014, the EU Cyber Defence Policy Framework of 18 November 2014, and the Council Conclusions on Cyber Diplomacy of 10 February 2015.

ANNEX

Non-paper: Developing a joint EU diplomatic response against coercive cyber operations

Introduction

In the context of the evolving and increasingly hybrid security threats facing the EU, the increased number and impact of coercive cyber operations is of a particular concern. A growing ability and willingness of States and non-state actors**, such as criminal- and terrorist groups,** to pursue their political objectives by undertaking disruptive or even destructive **coercive** cyber operations can be observed~~.~~[3]**. For the purposes of this non-paper, coercive cyber operations can be defined as cyber operations that constitute internationally** a **wrongful or ~~i~~illegal act intended to exert undue diplomatic, informational, military or economic pressure on a target State. Such coercive cyber operations**~~This~~ **might** pose~~s~~ a threat to ~~global norms and responsible State behaviour principles and values that has an impact on~~ the security of EU, its citizens and territory.

Such coercive cyber operations can occur across a wide spectrum of intensity, complexity and impact. Where coercive cyber ~~incidents~~ **operations** ~~potentially~~ reach the legal threshold of an armed attack, States may act in self- or collective defence**.** ~~, particularly through NATO.~~ However, the unique attributes of cyber operations make it possible to generate highly coercive effects through disruptive or even destructive cyber operations, whilst remaining below the legal thresholds of an armed attack.

Joint response: developing the diplomatic toolbox

Therefore, below the threshold of an armed attack, and ~~A~~**a**s a result of their specific attributes, ~~therefore,~~ coercive cyber operations **can under certain circumstances** require a broader response and a comprehensive use of a multitude of policy instruments across varying domains. This applies particularly **if coercive cyber operations are used** in ~~the context of~~ a hybrid conflict.

[3] **The disruption of parts of the Ukrainian electrical grid in December 2015 is one example, among many others, of an incident that has raised particular concern.**

The EU is already undertaking action to improve its defenses against hybrid threats through increased prevention, early warning, resilience and coordination. ~~Against the cyber component of hybrid threats, t~~**T**he EU Cyber Security Strategy, the EU Cyber Defense Policy Framework and the Network and Information Security (NIS) Directive provide a valuable basis **with regards to existing response mechanisms**. New mechanisms under discussion, such as the *Joint Framework with actionable proposals*[4] against hybrid threats ~~should~~ also focus on cyber threats. An immediate joint defensive response is also possible through the cooperation group and the Computer Security Incident Response Teams (CSIRTs) network created by the NIS Directive and in collaboration with other international CSIRTs.

However, the coercive and political character of cyber operations, especially State-sponsored ones, mandates the question of what could be done **in the area of foreign policy** to broaden the capability of EU and its Member States to respond to this increasing threat**.** ~~in the political domain as well as in the technical domain?~~

One such option would be to develop a comprehensive cyber diplomacy toolbox that is part of the EU Common Foreign and Security Policy ~~and the EU Common Security and Defence Policy~~. **Such a toolbox could identify the possible foreign policy instruments at disposal of the EU and / or its Member States according with the Treaties.**

Th**e creation of such a toolbox**~~is~~ would ensure that the EU and its Member States can adequately respond to coercive cyber operations **beyond the established mechanisms** ~~not just at a technical level, but~~ **aware of the** ~~can also employ the~~ foreign and security policy tools **at their disposal** to exert the political, diplomatic, criminal justice and economic influence that the EU and its Member States have at the world stage. In this regard, the EU and NATO would be able to complement each other **with a view to their respective strengths.** ~~and could coordinate their activities in this field (e.g. sharing each other's situational reports). For instance, a Technical Agreement between CERT EU – NCIRC has now been reached to enhance this action.~~

[4] The EU Foreign Affairs Council in May 2015 invited the Vice President/High Representative to present ~~by the end of 2015~~ a *Joint framework with actionable proposals* to help countering hybrid threats and foster the resilience of the EU and its Member States as well as partners, in close co-operation with Commission services, EEAS and the European Defence Agency, and in consultation with the Member States.

The role of cyber diplomacy

In the Council Conclusions on Cyber Diplomacy[5] of 11 February 2015 the Member States concluded 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".

It is assumed that coercive cyber operations, especially state-sponsored ones, are undertaken by perpetrators on the basis of rational cost/benefit analyses. The aim of conducting cyber diplomacy is to influence these analyses by increasing the economic, legal, moral and political costs of coercive cyber operations. By imposing such costs for undertaking coercive cyber operations, cyber diplomacy can both enhance the immediate response to a coercive cyber operation and help to establish a deterrent effect in the long term.

Many individual Member States could perceive it as difficult to diplomatically respond to the ~~most likely~~ perpetrators, especially of state-sponsored coercive cyber operations, on their own. Where appropriate, a joint response at EU level could be much more effective to ensure that a diplomatic response has the desired effect. This underscores the continued need for adequate coordination and cohesion in developing effective responses.

Situational awareness, attribution and proportionality

Before any collaborative diplomatic response could be considered in the aftermath of a coercive cyber operation, establishing a sufficient degree of shared situational awareness will be the first priority for the EU and its Member States.

[5] 6122/15.

Given the well-known problems with confidently attributing coercive cyber operations to a certain actor, it should be clear that the instruments mentioned below should be employed with careful consideration.

In this regard, it should be noted that attribution can be established with various degrees of certainty. The ~~proportionality~~ **decision to use** ~~of~~ each of ~~these~~ **the proposed** instruments could be tied to the level of certainty of attribution which can be achieved.

After a sufficient degree of attribution of a coercive cyber operation to a concrete country is established or where the perpetrator is identified, the proportionality of the possible use of diplomatic instruments should be decided on the basis of the damage caused by the cyber operation. If attribution is difficult to establish, possible diplomatic measures should remain very general; otherwise they risk becoming counter-productive. The proportionality of a response also depends in part on the scale, scope, duration and intensity with which each **diplomatic** instrument is used. The fact that such calculations remain difficult given the lack of **a** state practice in diplomatic responses to coercive cyber operations underlines the need for caution, but also emphasizes the importance of discussing these issues **at expert level, including in** FoP on Cyber Issues.

The importance of establishing situational awareness and~~, when possible,~~ attribution underlines the importance of adequate incident reporting and information sharing. The Europol/EC3, the Coordination group and CSIRT network established by the NIS Directive, CERT-EU**,** EU IntCen**,** ~~and~~ the type of EU Fusion Cell currently being considered to counter hybrid threats **and the Technical Arrangement between CERT-EU and NATO NCIRC** could all play valuable role in this regard. The Member States and EU Institutions will need to further explore how the information streams of these various **existing** mechanisms could be coordinated and combined in order to establish and enhance shared situational awareness.

Toolbox

An enhanced cyber diplomacy toolbox could include instruments that are suitable both for immediate response to incidents as well as elements that can be used ~~to~~**as an instrument to influence the behaviour of perpetrators** ~~punish or~~ **and** deter coercive cyber operations in the longer term. It should be highlighted that these instruments should be used with caution. They **are** presented only as options for consideration**, where appropriate,** and would not preclude action by any individual Member State.

Short-term diplomatic response:

- Statements by the Council and High Representative for Foreign Policy:
    - Issuing a statement condemning or expressing concern about a certain coercive cyber operations could play a signaling function, as well as serve as a form of strategic communication and deterrence against future coercive cyber operations.
    - Even without attribution to a particular State, expressing concern about a coercive cyber operation could send a strong message to the perpetrator that such practices constitute internationally **a** wrongful **or illegal** act~~s that are unacceptable and irresponsible behavior~~. **For instance, in those cases it could be useful to point towards the responsibility of States to ensure that their territory is not used for internationally wrongful or illegal acts, and to mitigate such activity.**
    - A challenge in this regard is the fact that it can take up to several weeks, if possible at all, to sufficiently ascertain the impact and the likely perpetrator of a coercive cyber operation to warrant a public statement, after which the sense of urgency may have abated. However, in such cases, a high degree of care**, situational awareness** and confidence might in fact strengthen the impact of a statement.
    - **For instance, longstanding international legal principles, t**he recommendations **on voluntary non-binding norms of responsible State behavior** put forward by the UN Groups of Governmental Experts **and** ~~,~~ the confidence building measures established in the OSCE **and ARF** ~~and longstanding international legal principles~~ could be used as a basis for such statements.

- Formal diplomatic requests for assistance by the EU and/or its Member States:
  - The primary channel for requesting technical assistance is usually through operational CSIRT contact networks.
  - However, in certain cases where multiple Member States and/or the EU Institutions themselves are affected at the same time, it could be beneficial for them to jointly contact other States at the diplomatic level to formally request assistance to stop harmful cyber activity originating from the territory of that State or to assist with the apprehension of or legal action against the perpetrators[6].
  - Signaling concern by requesting assistance can be particularly valuable in the case of coercive cyber operations undertaken by non-state actors, or if State involvement cannot be attributed with confidence.

- Using the EEAS network of delegations and Member States embassies:
  - To further illustrate the seriousness with which the EU and its Member States view a particular coercive cyber operation, the EEAS network of delegations could, together with Member State embassies, carry out demarches.
  - Either to ask for political or technical support in mitigating a certain coercive cyber operation or to condemn a certain cyber operation when attribution is sufficiently confident. This could be a valuable instrument both in suspected perpetrator states and third countries.
  - Other forms of exerting diplomatic pressure, escalating to measures such as recalling diplomats, could also be considered.

[6] Though there is not always a legal obligation for States to provide assistance to each other, paragraph 13H of the report of the 2014-2015 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174) establishes the voluntary, non-binding norm that "States should respond to appropriate requests for assistance".

- Active measures:
    - Under certain circumstances, international law permits a state to undertake measures to stop the harm resulting from ~~an internationally wrongful act or imminent threat~~**a coercive cyber operation**. Examples range from the expulsion of foreign diplomats to **stronger** ~~more forcible~~ measures, but these possibilities are predominantly employed by individual states. However, it should be underlined that there are various ways that Member States can assist each other when undertaking such **active**~~forcible~~ measures.

Long term diplomatic response:

- Signaling through EU bilateral and multilateral diplomatic engagement
    - The bilateral EU-led political dialogues, particularly the Cyber Dialogues ~~with China, India, Brazil, US, Japan and the Republic of Korea~~**led by the EEAS** could be used to raise concerns about certain coercive cyber operations and point out their presumed international wrongfulness **or illegality.** ~~.~~
    - Concern could be expressed both about the suspected coercive cyber operations of third countries or those of the dialogue partner itself (directly or indirectly).
    - In this regard, it could also be useful to underline the importance of the application of international law and norms of responsible State behavior, for instance in bilateral EU agreements with partners (e.g. EU Framework Agreements).
    - Concern could also be expressed in multilateral fora such as the UN and the OSCE.

- Assessing the viability of imposing EU sanctions
    - Imposing sanctions against certain "natural or legal persons, entities or bodies"-[7] could be a way to raise the costs of undertaking coercive cyber operations and serve as a deterrent to conduct such actions. Though there are clear challenges **with establishing evidence** when it comes to ~~attribution~~**imposing restrictive measures in response to cyber operations**, the EU has prior experience in implementing sanctions packages that could help envisage their application in the cyber context as well. The EU could investigate options to design appropriate sanctions as a possible response.
- Preparing law enforcement investigations and prosecution:
    - In addition to formulating a diplomatic response it ~~is~~ **could be** beneficial ~~also~~ to investigate and prosecute coercive cyber operations **more actively**. In this regard, **only Member States can initiate an investigation, but** cooperation and coordination through Europol and Eurojust would be valuable. Whilst it is clear that prosecuting complex coercive cyber operations is highly challenging, particularly when a clear State-sponsored link is present, this can yield valuable diplomatic leverage over a suspected perpetrator.
- Leveraging EU regulatory and economic power:
    - In addition to a foreign and security policy response toolbox, the EU also has significant regulatory and economic instruments at its disposal as the largest single market in the world. The ability of the EU to pursue cases in **bilateral and** multilateral trade settings is one example. Whether, and under which conditions, such instruments could be used in response to coercive or severe cyber operations could be discussed.

[7] **For instance, the Council can impose restrictive measures within the framework of the CFSP such as the freezing of assets, establishing economic sanctions and restricting admission to the Union. See for instance the Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy (11205/12). The Council can also adopt a CFSP decision under Article 29 TEU.The measures foreseen in that Council Decision are either implemented at EU or at national level.**

Decision making procedures

Given the specific attributes of coercive cyber operations and the many bodies, organizations and institutions that would be involved, **proper attention has to be given to the legal bases of each possible measure and the procedures to be followed accordingly.** ~~t~~**T**he question is how EU and its Member States could decide to undertake joint diplomatic action to counter coercive cyber operations. One possible way could be to have FoP draw up a proposal for possible diplomatic response measures and present them to PSC, or where appropriate, to the Council for approval. Where appropriate, FoP could do so, in cooperation with appropriate regional Council working groups, the Coordination group and CSIRT network established by the NIS Directive. After approval by PSC or the Council, such a proposal could be executed, for example by drawing up a joint statement, or delegated to RELEX for technical implementation where necessary. In addition, it could be discussed if and to what extent the Solidarity Clause (222 TEU) and the Mutual Defence Clause (42(7) TEU) could be relevant for deciding upon and coordinating a diplomatic response to a particular coercive cyber operation.

Strategic messaging

Formulating a joint response to coercive cyber operations constituting internationally wrongful **or illegal** acts in cyber would present the EU with a number of political and legal challenges, especially in the implementation phase. In view of recent developments, however, the likelihood of such events taking place is increasing at a concerning rate. It is therefore preferable to discuss these dilemma~~'~~s sooner rather than later. Additionally, communicating the willingness of the EU and its Member States and the availability of a diplomatic toolbox to respond jointly to coercive cyber operations could already send a strong signal to potential perpetrators that there will be costs to such ~~attacks~~ **coercive cyber operations**.

Follow-up

- Further discussion about the development of a joint diplomatic toolbox at EU level would be held at the cyber attaches meeting of 8 April 2016.
- After that a revised version of the non-paper will be sent to Political Security Committee, and if possible to the Political-Military Group for further discussion.
- FoP would continue the discussions in view of that input in its upcoming meetings on 20 and 27 May and would present the outcome of those discussions and the respective issues for political guidance to the (Foreign Affairs) Council in June. EEAS would be expected to take an active role in this process and lead the development, in collaboration with Member States and EU Institutions and EU Agencies, such as ENISA, of a Framework which will serve as basis for the development of the future joint diplomatic toolbox against coercive cyber operations.
- This Framework would focus on four areas:
    - Further mapping of the shared situational awareness and information exchange mechanisms that are available or would be beneficial in order for a joint diplomatic response to be undertaken, as well as of the most appropriate mechanisms and procedures for decision-making in the possible scenarios, including which EU institutions, agencies and preparatory bodies should be involved.
    - Further analyzing and clarifying the legal bases and competences of the Member States and EU institutions with regards to the various instruments proposed in the paper to be included in the toolbox.
    - Further analyzing the possible impact and respective benefits of the various diplomatic instruments proposed in the paper to be included in the toolbox.
    - In collaboration with COM, task an (EU) research institute to conduct a limited, exploratory assessment of the viability and requirements for designing possible EU sanctions instruments (with possible informal follow-up discussion to be taken up only in 2017).
- In the long term, on the basis of the outcome of the discussion in the (Foreign Affairs) Council in June and later on, if necessary in COREPER and/or Council, the adoption of Council Conclusions on a diplomatic response toolbox against coercive cyber operations could be considered as a further step.