Council of the European Union

NOTE

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

Delegations will find in Annex a revised version of the non-paper of the Presidency reflecting the discussion of the cyber attaches of 15 February 2016 and the written comments received.

The recent, claimed to be a state-sponsored hack of the Ukrainian electrical grid has underlined the urgency of developing a joint EU diplomatic response against coercive cyber operations.

We view this incident as part of a worrying trend of increasing numbers operations, especially apparently State sponsored ones.

We hope that you will be able to share your comments during the upcoming cyber capitals meeting 1 March 2016. We would like to discuss the paper on the basis of the following questions:

1.   Many threat analyses emphasize the increasing ability and willingness of states, rather than criminal or other non-state actors, to use cyber operations. Would your Member State share this perception?

2.   Do these developments in your view merit a discussion and what diplomatic measures the EU and its Member States can undertake jointly to respond to this threat?

3.   How do you evaluate on a general level the measures proposed in the paper? What others could be considered as part of a such diplomatic toolbox?

4.   Would you support eventual Council Conclusions in this regard in order establish the commitment of the EU and its Member States to properly respond to coercive cyber operations in particular state-sponsored ones?

5.   Is the connection with EU efforts to counter hybrid threats a helpful component of a discussion on a diplomatic toolbox for countering cyber threats?

6.   Would you support the follow-up process proposed at the end of the non-paper?

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 to pursue their political objectives by undertaking disruptive or even destructive cyber operations can be observed. This poses a threat to global norms and responsible State behaviour principles and values that has an impact on the security of EU citizens and territory.

Such coercive cyber operations can occur across a wide spectrum of intensity, complexity and impact. Where coercive cyber incidents 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

As a result of their specific attributes, therefore, coercive cyber operations require a broader response and a comprehensive use of a multitude of policy instruments across varying domains. This applies particularly in the context of a hybrid conflict.

In this regard, 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, the EU Cyber Security Strategy, the EU Cyber Defense Policy Framework and the Network and Information Security (NIS) Directive provide a valuable basis. New mechanisms under discussion, such as the *Joint Framework with actionable proposals*[1] 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 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 <u>comprehensive cyber diplomacy toolbox</u> that is part of the EU Common Foreign and Security Policy and the EU Common Security and Defence Policy. This would ensure that the EU and its Member States can adequately respond to coercive cyber operations not just at a technical level, but can also employ the foreign and security policy tools 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 and could coordinate their activities in this field (e.g. sharing each others situational reports). For instance, a Technical Agreement between CERT EU – NCIRC has now been reached to enhance this action.

---

[1] 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 Defense Agency, and in consultation with the EU Member States.

The role of cyber diplomacy

In the Council Conclusions on Cyber Diplomacy[2] 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 EU 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.

---

[2] 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 of each of these instruments could be tied to the level of certainty of attribution which can be achieved.

The proportionality of a response also depends in part on the scale, scope, duration and intensity with which each instrument is used. The fact that such calculations remain difficult given the lack of state practice in diplomatic responses to coercive cyber operations underlines the need for caution, but also emphasizes the importance of discussing these issues in the 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 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 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 punish or deter coercive cyber operations in the longer term. It should be highlighted that these instruments should be used with caution. They presented only as options for consideration and would not preclude action by any individual Member State.

Short-term diplomatic response:

- Statements by the Council and High Representative for Foreign Policy:
    - o 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.
    - o 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 wrongful acts that are unacceptable and irresponsible behavior.
    - o 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 and confidence might in fact strengthen the impact of a statement.
    - o The recommendations put forward by the UN Groups of Governmental Experts, the confidence building measures established in the OSCE 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[3].
    - 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.

---

[3]   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:
    - o Under certain circumstances, international law permits a state to undertake measures to stop the harm resulting from an internationally wrongful act or imminent threat. Examples range from the expulsion of foreign diplomats to 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 forcible measures.

Long term diplomatic response:

- Signaling through EU bilateral and multilateral diplomatic engagement
    - o The bilateral EU-led political dialogues, particularly the Cyber Dialogues with China, India, Brazil, US, Japan and the Republic of Korea could be used to raise concerns about certain coercive cyber operations and point out their presumed international wrongfulness.
    - o Concern could be expressed both about the suspected coercive cyber operations of third countries or those of the dialogue partner itself (directly or indirectly).
    - o 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).
    - o Concern could also be expressed in multilateral fora such as the UN and the OSCE.

- Assessing the viability of imposing EU sanctions
    - o Imposing sanctions against certain "natural or legal persons, entities or bodies" 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 when it comes to attribution, 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:

- o In addition to formulating a diplomatic response it is beneficial also to investigate and prosecute coercive cyber operations. In this regard, 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:
  - o 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 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.

Decision making procedures

Given the specific attributes of coercive cyber operations and the many bodies, organizations and institutions that would be involved, the 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 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.

Follow-up

- A discussion about formulating a joint diplomatic toolbox at EU level could be held at the FoP capital-level meeting.
- A discussion in the Political Security Committee on this topic could be a preliminary step towards which the Commission, EEAS and Member States could work.
- For information purposes, the topic could also be discussed in Relex and PMG Working groups.
- With the approval of PSC, the FoP could prepare short Council Conclusions tasking the EEAS to develop, in collaboration with Member States and the Commission and appropriate EU bodies such as ENISA, a short Action Plan to further develop the diplomatic toolbox against coercive cyber operations and submit it to the Council for approval.
- This Action Plan could 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.
    - Further mapping of the most appropriate mechanism and procedures for decision making in several possible scenarios, including which EU institutions, bodies and working groups should be involved.

- o Where appropriate, develop the various diplomatic instruments in the toolbox further, including by outlining their potential costs and benefits.
- o 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)

- These short Council Conclusions tasking the EEAS could be adopted by a Foreign Affairs Council or JHA Council within the current Presidency period.
- In the long term, a discussion in COREPER aimed at the adoption of broader Council Conclusions on a diplomatic response toolbox against coercive cyber operations could be a goal.

———————————