Council of the European Union

Brussels, 9 February 2016
(OR. en)

5797/16

CYBER 9
RELEX 78
JAIEX 12
TELECOM 12
COPS 35

NOTE

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

Delegations will find in an Annex a non-paper of the Presidency.

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 of state-sponsored cyber operations. In that regard, we hope that the non-paper set out in the Annex could complement the recent NATO food for thought paper that NL, UK and France supported.

We hope that you will be able to share your comments during the upcoming cyber attachés meeting on 15 February 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 to make clear EU engagement in a process to define proper response to cyber attacks, in particular the 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?

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 EU norms, principles and values and the security of EU citizens and territory.

Such cyber operations can occur across a wide spectrum of intensity, complexity and impact. Where cyber incidents potentially reach the political and legal threshold of an armed attack, States may act in self- or collective defense, 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 and political thresholds of an armed attack.

Joint response: developing the diplomatic toolbox

As a result of their specific attributes, therefore, 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 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 collaboration of national Computer Security Incident Response Teams (CSIRTs).

However, the coercive and political character of cyber operations, especially State-sponsored ones, mandates the question of what more could be done in the political domain to strengthen the capability of EU and its Member States to respond to this increasing threat?

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. 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).

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".

---

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 initial results are currently expected to be presented in March.

2 6122/15

It is assumed that 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 cyber operations. By imposing such costs for undertaking 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 cyber operations, on their own. Where appropriate, a joint response at EU level could be much more effective to ensure the effectiveness of cyber diplomacy in such cases. This underscores the continued need for adequate coordination and cohesion in developing effective responses.

Attribution and proportionality

Given the well-known problems with confidently attributing 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 importance of establishing attribution underlines the importance of adequate incident reporting and information sharing. The work of Europol EC3, EU IntCen and the type of EU Fusion Cell currently being considered to counter hybrid threats could be particularly valuable.

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 cyber operations underlines the need for caution, but also emphasizes the importance of discussing these issues in the FoP on Cyber Issues.

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 are presented only as options for consideration and would not preclude action by any individual Member State.

Immediate response:

- Statements by the Council and High Representative for Foreign Policy:
    - Issuing a statement condemning or expressing concern about a certain cyber operations could play a signaling function, as well as serve as a form of strategic communication and deterrence against future cyber operations.
    - Even without attribution to a particular State, expressing concern about a cyber operation could send a strong message to the perpetrator that such practices constitute internationally wrongful acts that are unacceptable and irresponsible behavior.
    - A challenge in this regard is the fact that it can take up to several weeks to sufficiently ascertain the impact and the likely perpetrator of a 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.
    - The voluntary, non-binding, but internationally accepted norms put forward by the UN Group 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 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 case, it could be beneficial for several Member States, the EU itself or 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 cyber operations undertaken by non-state actors, or if State involvement cannot be attributed with confidence.
- Using the EEAS network of delegations:
    - To further illustrate the seriousness with which the EU and its Member States view a particular 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 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 EU Delegation diplomats, could also be considered.
- 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. 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.

[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".

Long term response:

- Signaling through bilateral EU Political and Cyber Dialogues:
    - The bilateral dialogues, particularly the Cyber Dialogues with China, India, Brazil, US, Japan and Korea could be used to raise concerns about certain coercive cyber operations and point out their presumed international wrongfulness.
    - Concern could be expressed both about the suspected 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).
- Preparing EU sanctions instrument:
    - Imposing sanctions against certain "natural or legal persons, entities or bodies" could be an effective method to raise the costs of undertaking coercive cyber operations. Though there are clear challenges when it comes to attribution, the EU has a lot of prior experience in implementing sanctions packages that could facilitate their application in the cyber context as well. The EU could investigate options to prepare the necessary legal framework and operating procedures to be able to use sanctions as a possible response.
- Preparing law enforcement investigations and prosecution:
    - 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 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 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 cyber operations, the EU and its Member States could explore which of the EU procedures of the CFSP, Integrated Political Crisis Response (IPCR), Union Civil Protection Mechanism (UCPM) and the 2014 Council Decision No 2014/415/EU on the Arrangements for the Implementation by the Union of the Solidarity Clause are most suitable for deciding and coordinating a diplomatic response to a particular cyber operation.

Strategic messaging

Formulating a joint response to 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, the willingness to enter into these discussions could already send a strong signal to potential perpetrators of State-sponsored cyber operations that the costs of such attacks is about to increase.

Follow-up

- A discussion about formulating a joint diplomatic toolbox at EU level could be held at the FoP capital-level of meeting.
- As a first milestone, 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.
- In the long term, a discussion in COREPER aimed at the adoption of Council Conclusions on a diplomatic response toolbox against coercive cyber operations could be a goal.
- In addition to FoP, aspects of a diplomatic response toolbox could be further discussed in the competent Council preparatory bodies, such as RELEX and in geographic, JHA and trade-related working groups.

Further analysis would be required to determine which EU bodies and institutions would need to be involved in the development of such a diplomatic toolbox, and what best practices are already available.