Council of the
European Union

Brussels, 18 April 2017
(OR. en)

8146/17

LIMITE

CYBER 53
RELEX 308
POLMIL 33
CFSP/PESC 327

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7923/17
Subject:	Joint Diplomatic Response to Cyber Operations (Cyber Toolbox) - Member States' comments

Delegations will find in Annex Member States' comments on the Joint Diplomatic Response to Cyber Operations ("Cyber Toolbox") as set out in doc. 7923/17.

GERMANY

First comments by Germany

1. WHY A CYBER TOOLBOX?

In the recent period, we have observed a growing ability and willingness of State and non-state actors, including criminal and terrorist groups, to pursue their objectives by undertaking disruptive or even destructive cyber operations. NATO has declared cyberspace as a domain of operations, "the ~~fourth~~ fifth one". Disinformation using cyber means, cyber-espionage, intellectual property theft, cyber-attacks on infrastructures, cybercrime or cyber conflict, may call for responses going beyond our current communication and cybersecurity policies. Cyber has to be seen also in the context of hybrid threats.

The EU is already taking action on cyber through increased prevention, early warning, resilience and coordination. The Global Strategy for the European Union's Foreign and Security Policy, the 2013 EU Cyber Security Strategy, the EU Cyber Defence Policy Framework, the Network and Information Security (NIS) Directive and the creation of the European Network and Information Security Agency ENISA, the establishment of the CERT- EU and of a European Cyber Crime Centre at Europol address these issues. The joint framework on countering hybrid threats (JOIN(2016)18 final) may be used also.

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 signaling the likely consequences of a cyber-attack would dissuade potential attackers. It would require putting in place solid preparatory practices and communication procedures.

The current Issues paper responds to the PSC tasking of 23 June 2016 on the basis of the Netherlands Presidency non-paper. It presents a toolbox, which could be used by the EU and its Member States to respond to cyber operations.

This should be seen as complementary to, but not a replacement for, existing EU cyber diplomacy engagement. Current diplomatic efforts and operational actions, such as supporting wider compliance with the existing international law such as the Budapest Convention on Cybercrime and reaching common positions in international fora, will continue unabated. But there is a growing need for the EU to protect its long term strategic, security and economic interests and to develop strategic guidelines to do so.

2. WHAT TO INCLUDE INTO THE TOOLBOX?

The cyber toolbox will include instruments that are suitable both for an immediate response to incidents as well as elements that can be used to influence behaviour and deter adverse cyber operations in the longer term. These instruments are presented as options for consideration, where appropriate, and would not preclude action by any individual Member State.

A non-exhaustive list of instruments below is presented in order of presumed impact (from lower to higher impact). The overall proportionality of a response depends on the scale, effect, scope, duration and intensity with which each instrument is used.

Statements by the Council and High Representative for Foreign Policy

Issuing a statement expressing concern or condemning general cyber trends or certain cyber operations could play a signaling function, as well as serve as a form of strategic communication and deterrence against future cyber operations.

Formal Council Conclusions

Issuing general or specific formal Council Conclusions on cyber operations could play a signaling function, underlining awareness and determination on cyber issues and dissuade potential attempts of dividing EU Member States positions by cyber operations.

Formal joint requests for technical assistance through diplomatic channels

Following the Network and Information Security Directive, the primary channel for requesting technical assistance is usually through the Computer Emergency Response Team Contact Networks (designated as CSIRT's contact networks – computer security incident response team). When multiple Member States and/or the EU institutions are affected, it would be beneficial to jointly contact third States using diplomatic levers to formally request technical assistance.

Diplomatic Demarches

EU delegations could, together with Member State embassies, carry out demarches to a number of different ends. For instance, demarches could ask for support in mitigating a particular cyber operation, condemning such an operation or clarifying the circumstances around a cyber-attack with links to its territory.

Signaling through EU bilateral and multilateral topical or political dialogues

Bilateral EU-led political dialogues, particularly cyber dialogues, could also be used to follow-up on statements and raise concerns about certain cyber operations. Concern could be expressed about the suspected cyber operations of third state or non-state actors. Concern could also be expressed in multilateral bodies such as the UN, OSCE, NATO and WTO, and in bilateral dialogues with the secretariats of multilateral bodies, and in particular with the UN Secretariat.

Restrictive measures

The Union may impose restrictive measures 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. 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.

Other instruments

Among other lawful responses, a State that is the victim of an internationally wrongful act may, under certain conditions, resort to proportionate countermeasures against the State which is responsible for the internationally wrongful act in order to induce that State to comply with its international obligations. ~~Other~~ Certain forms of diplomatic pressure, such as recalling diplomats or establishing investigating teams could also be considered if deemed necessary. ~~For example the Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0, the most comprehensive analysis of how existing international law applies to cyberspace, provides a more comprehensive list of possible counter-measures for States that have been subject to an internationally wrongful act in the Cyber domain.~~

3. HOW TO USE THE TOOLBOX

The above-mentioned tools should be implemented as far as possible through the use of existing mechanisms. These tools should be used in a coherent and consistent manner: this requires *inter alia* a more developed understanding of the full scope of 'coercive cyber operations' (see Council document 5797/6/16).

Preparing a decision

Before any collaborative diplomatic response (or position) could be considered, sharing a sufficient degree of information will be of key importance for the EU and its Member States. Making best use of current information-sharing mechanisms will be key.

The Europol Cybercrime Centre (EC3), the NIS Directive established EU Coordination group and EU CSIRT network including CERT-EU, the EEAS' Intcen, including the Hybrid Fusion Cell, all play a valuable role in this regard by sharing analyses, early warning and information related to risks and incidents within their respective constituencies, in accordance with their mandate and the confidentiality of the information.

At a policy level, in order to enhance internal coordination and to help develop a comprehensive and coherent EU approach on cyber issues, a Horizontal Working Party on Cyber issues, chaired by the rotating Presidency, as a formal Council preparatory body, has been established. The Working Party ensures the strategic and horizontal coordination of cyber issues in the Council and can be involved in both legislative and non-legislative activities. On the basis of the relevant information streams, and in accordance with their responsibilities, the Working Party and PSC should act as preparatory bodies for use of the toolbox. The Working Party has a signaling role in this regard.

Preparing decision would also most often require discussing further the issues of the attribution and of the necessity and proportionality of the decision.

Making a decision

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 competence and initiative for employing these measures lies with the Member States. The respective legal basis, procedure and fora depend on which instrument will be used to respond to a cyber operation, though the Council is the central actor in the decision-making process when the European Union in its quality pursuant to Article 47 TEU as legal person under international law is affected, and could be a key implementer of the decision, next to the Member States involved and to the High Representative of the Union for Foreign Affairs and Security Policy and / or the Commission.

Appropriate coordination with like-minded countries and allies should be envisaged, particularly in the context of EU-NATO cooperation.

Following a decision

After the decision to impose a measure has been taken, it should be actively and systematically communicated by the EU and its Member States inside and outside of the EU. Therefore it is important that the reasons for which measures are taken are made known and the relevant audience targeted. EEAS StratCom capabilities should be fully used.

A specific communication approach both towards third countries could also be developed as part of the imposition of a measure in cooperation with Member States and the Commission. Specific communication could also be necessary to the country being at the origin of the wrong-doing, also in order to prevent continuation of the wrong-doing.

Proper attention should be given to the follow-up of a decision and its possible repeal.

4. THE ISSUE OF ATTRIBUTION

A common position based on a sufficient degree of shared situational awareness between

Member States is key in order to trigger a response.

First, it should be pointed out that most of the instruments presented in this Issues paper do not always require attribution or directing accusations against a given state or non-state actor: they are a means of expressing concerns and signaling them in another way. For instance, regardless of the actual perpetrator, diplomacy can be used to encourage countries that serve as unwitting proxies or transit points for an illegal cyber operation to take action to mitigate the activity. Furthermore, some of these instruments can be tailored to reflect the specific degree of attribution that can be established in a particular case.

The customary international law of State responsibility supplies the standards for attributing acts, including cyber acts, to States. The law of State responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution. In this context, it follows from the principle of sovereignty that a State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. Absolute certainty is not required. Instead, international law generally requires that States act reasonably under the circumstances when they gather information and draw conclusions based on that information. There is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate responsive action, although it is recognized for the purposes of this Cyber Toolbox that States may choose to reveal such evidence, for instance in order to convince other States to join them in condemnation of the malicious cyber activity. ~~Given the well-known problems with confidently attributing cyber operations to a certain actor, it should be clear that in other cases the instruments mentioned should be employed with careful consideration. Evidence used to attribute responsibility should be able to pass the scrutiny of Member States.~~

The considerations above notwithstanding, a State who decides to take measures, based on its own assessment and attribution of a given operation to another State, has to be mindful that in case the attribution turns out to be erroneous its measures may themselves be an internationally wrongful act against which the affected State in turn may take its own measures. As anywhere else, there is a risk of being wrong. In any case the State accused of having carried out a malicious cyber operation can be expected to refute that claim as long as possible by challenging the attribution. Therefore, regardless of the validity of the claim or counterclaim and the level of "proof" required, the State that takes action will have to have to be ready to engage in an extended, politically charged public argument about the case.

Regarding attribution a third point needs to be taken into account. While it is legally correct that States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies, a State—as a rule—cannot be held accountable for acts perpetrated by private third parties acting entirely on their own. To establish the international wrongfulness of a malicious cyber operation carried out by a private individual and the responsibility of a State, a double attribution is needed: First of the technical operation to an individual perpetrator, and secondly the link between that individual and the State who has sponsored, ordered, remunerated or knowingly tolerated that activities to an extent that legally the State itself can be regarded as the author of the respective operation

Restrictive measures should be able to pass judicial scrutiny. ~~Through cross-domain intelligence and political assessments on the possible interests of the attacker, attribution could be established with varying degrees of certainty.~~

The United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security recommends following a number of cyber norms and stresses that international law applies to cyber relations among States as much as it applies to all other types of international relations ~~in cyberspace. Other principles of customary international law, voluntary norms and confidence building measures relevant to cyberspace include due diligence and state responsibility. They should be used fully to support the attribution process. The limited state practice here underlines the need for careful consideration, but also emphasizes the importance of discussing further these issues at expert level.~~

5. ~~NECESSITY AND PROPORTIONALITY~~ THE ROLE OF THE CYBER TOOLBOX IN THE CONTEXT OF CYBER OPERATIONS AMOUNTING TO THE USE OF FORCE OR AN ARMED ATTACK

Under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the Charter of the United Nations and customary international law. States may 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, in response to an armed attack through cyberspace. ~~The Working Party could address how the various elements of the toolbox could or should be used in order to produce the desired effect, building inter alia on the concepts of necessity and proportionality~~. Where a cyber operation is to be considered as [an act of aggression] [use of force or as an armed attack], the toolbox can still be used to support or complement appropriate responses.

Further considerations by Germany:

- Germany supports the general approach of developing options for a joint EU diplomatic response to cyber operations, and welcomes that the Joint EEAS–Commission Services Issues Paper on a Joint EU Diplomatic Response to Cyber Operations takes our work on the "cyber diplomacy toolbox" forward.
- Germany conceives the reply to the question whether or not the findings of the Issues Paper should be endorsed as Council Conclusions is a function of the substance which Member States will be able to agree. If justified by the contents of such a document, Germany will support its endorsement as Council Conclusions. However, at this juncture the "cyber diplomacy toolbox" still requires amendments; it is at present not ripe for an immediate endorsement.
- At this stage Germany should like to reiterate her first set of proposals for amendment, in particular on certain aspects of international law, as distributed in hardcopy during the meeting of March 22, 2017 and, consecutively, as email message dated March 23, 2017. These proposals — which are attached to this message for reasons of convenience — address, inter alia, the issues of the international law of nonforcible countermeasures and

of attribution, which, in our view, require a more precise language if the document is to contain a "cyber diplomacy toolbox."

- In addition, it should be discussed in how far the EEAS's Hybrid Fusion Cell can be used as focal point for voluntary information and intelligence sharing on cyber operations that require an EU diplomatic response. The Hybrid Fusion Cell may be the appropriate venue to coordinate information sharing also on cyber operations, as cyber operations are particularly useful tools in hybrid conflicts.
- Germany expects that document 7923/17 CYBER 48 RELEX 289 POLMIL 31 CFSP/PESC 309, still to be issued for examination at the next meeting on April 19, 2017, will take account of these proposals for amendment.

HUNGARY

Hungary's position on the „Joint EEAS-Commission Services Issues Paper on a Joint EU Diplomatic Response to Cyber Operations ('Cyber Toolbox')" (WK 2569/2017)

The Presidency asked the Member States to submit written comments on the above document. Please find below the Hungarian contribution.

We would like to thank the Netherlands for putting this issue on the agenda and the EEAS and the Commission for preparing the issues paper. Before giving concrete comments on the document we would like to express some general observations.

We are supportive of the process and agree that a formalized output as for example in the form of council conclusions is a good way ahead, however we think that there is a need for further discussions on the topic before we can reach a common understanding. The Issues Paper states in chapter 2 that a non-exhaustive list of instruments is listed. Although we understand that it is probably impossible to list all the possible actions, we believe that the principles for how further instruments can be introduced should be set out. We also think that the process of initiating a joint response and the responsibilities of the different actors (MS, EU institutions) should be defined more clearly.

As we have stated during the Horizontal Working Party on Cyber Issues of 22 March, we think that the work done in the OSCE on cyber Confidence Building Measures should feature more prominently in the document. Every EU Member State is also a participating State in the OSCE. The OSCE has adopted 16 confidence building measures, some of which could also be referenced in the cyber toolbox. The OSCE Informal Working Group dealing with cyber issues will concentrate in 2017 on the implementation and operationalization of these Confidence Building Measures, which could eventually be also useful in the context of the diplomatic toolbox, like for example the consultation mechanism under CBM3.

On Page 1 in Chapter 1 it is stated, that „NATO has declared cyberspace as a domain of operations", after this the rest of the sentence should be deleted. There is no need to "number" whether it is 4th or 5th domain of operations.

We strongly support the last paragraph of the 1st chapter about existing cyber diplomacy engagement.

In the 2nd chapter under title "Formal joint requests for technical assistance through diplomatic channels" we think that the CSIRT Network has been tasked under the NIS directive, and no further task should be given via the cyber toolbox. The CSIRT Network is solely tasked with EU-internal coordination, and thus should not be mentioned in the diplomatic toolbox. EU Member States can decide based on concrete cases to jointly contact third States but this should be a sovereign right of the respective Member State(s).

In the 3rd chapter there is a vague reference in the document that the term "coercive cyber operations" must be better understood, but there are no suggestions on any mechanism/process to this end.

We agree that attribution poses a great challenge, and further detailed discussions are necessary on this topic.

Under title "Making a decision" the measures which can be "employed by MS in cooperation with the EU institutions or by the EU institutions themselves" must be clearly defined, so that competences based on the EU acquis are respected.

In the last paragraph of the 4th Chapter confidence building measures are mentioned. Since the OSCE has already adopted decisions on cyber CBMs and further work is foreseen on how to put these into practice, a concrete reference to OSCE should be made.

LATVIA

Latvian comments on the Cyber Diplomacy toolbox

05.04.2017

At the last HWGCI, the MT PRES requested input on the vehicle for delivering the message on the toolbox, what should and shouldn't be included in the toolbox.

We support brief council conclusions addressing the need for a common EU approach on a joint diplomatic response to cyber operations. A high level message on the threat faced by the EU is an appropriate first step in addressing an initial diplomatic response. More detailed and challenging issues addressed in document WK 2569/2017 INIT that can be further elaborated in a document in the future or even within the context of an EU Cyber Security Strategy review.

The conclusions should include the following elements:

- **a.** Cooperation with NATO in the context of the EU-NATO Cooperation Framework on responding to cyber operations.
- **b.** The political will to address the attribution of cyber-attacks and consider restrictive measures on a case by case basis.
- **c.** Support the use of all technical and operational level mechanisms offered by the NIS directive groups, ENISA and other EU institutional sources to provide support for common situational awareness.
- **d.** Stress the necessity to address cyber-attacks in the context of current and future EU work on hybrid threats and resilience.

Written comments by April 3 (Not the last time). : on the vehicle, items should or shouldn't be there, and specific text that needs to be changed.

1) Appreciate EU-NATO angle
2) Attribution-
    a. We will not solve all attribution issues here. Either have all issues here or split a simplified toolbox and invest in a longer paper on international law and attribution separately.
    b. Attribution will also be case by case always. Cannot be codified here.
3) The CSIRT network has a role to play as it works hands on on cyberincidents. (Not just a CSDP issue, can be an economic issue, as in NIS dir).
4) What is the timeline on resilience, and can we wait. What will be in the initiatives that should be taken into consideration.

NETHERLANDS

NL comments on JOINT EEAS-COMMISSION SERVICES ISSUES PAPER ON A JOINT EU DIPLOMATIC RESPONSE TO CYBER OPERATIONS ('CYBER TOOLBOX')

Toolbox – Council Conclusions

NL welcomes and highly appreciates the document prepared by the EEAS.

As suggested during the HWP Capitals, dd. 22 March, NL would be in favor of endorsement by the Foreign Affairs Council in June and supports Council Conclusions addressing the principal issues of the Toolbox, such as ensuring a firm basis within international law. Such Council Conclusions should be considered part of the broader ongoing cooperation within the EU foreign security policy framework.

NL is in favor of moving forward with the Council Conclusions as soon as possible in order to provide a political signal to (potential) malicious actors. However, several instruments will require further study and elaboration, as well as the decision making procedures for utilizing these and issues such as attribution. Such specific interpretations and policy development could be further drawn up in the form of practical implementation guidelines.

An option for taking the implementation guidelines forward would be to include these as an action in the roadmap of the EU cyber security strategy as it is updated. This would be in line with the Dutch view on strongly featuring international engagement, diplomatic relations, political-strategic aspects and capacity building in the second EU cyber security strategy.

Particularly the requirements for imposing restrictive measures deserve further examination in order to ensure that the EU is able to use these in the cyber context. Restrictive measures are amongst the most powerful instruments the EU has at its disposal, so deserve due attention.

In Council Conclusions, NL would also like to see a call for exercises in the use of the toolbox.

Comments on the text:

- (throughout) Given the confusion resulting from the difference between the legal and practical connotations of the term 'attack', it is best to avoid this term. NL would recommend to use the term 'cyber operation'. For instance "cyber operations against critical infrastructure" or "cyber operations disrupting or sabotaging the functionality of critical infrastructure" or the "adverse cyber operations" that is used on page 2 instead of the "cyber-attack".
- Avoid the use of the term 'cyber' on its own. In most cases throughout the text, this could be replaced by the term 'cyber threats'.

Page 1:

- (first paragraph) NATO considers cyberspace to the fifth domain of operations, not the fourth.
- (second paragraph)CERT-EU is the CERT for the EU institutions and is therefore of a different character than ENISA and the European Cyber Crime Centre. It does not contribute to the resilience of the European Union as such. CERT-EU should therefore be removed from this list.

Page 2

- Both the terms "dissuasion" and "deterrence" are used in these paragraphs. With a view to consistency, it would be recommended to choose and stick to one.
- (last paragraph on 'formal joint requests'): NL has strong reservations against the final paragraph on page 2:
    - The CSIRT's Network is solely an instrument to strengthen cooperation amongst EU Member States' CSIRTs. Therefore it can only be used within the EU, and it cannot be deployed as a tool to contact parties outside of the EU, as now seems to be suggested in the final paragraph. For the purpose of contacting parties outside the EU, bilateral CSIRT channels or contacts with regional CSIRT organisations like AP-CERT or OIC-CERT can be used.

- Instead of Computer Emergency Incident Response Team it should read “Computer Security Incident Response Team’s Networks.” That is what CSIRT stands for. It is used correctly in the next sentence.
- Also, the correct term is “CSIRT’s Network” instead of CSIRT’s contact networks.
- Lastly, this instrument is now described incompletely. In the context of the toolbox, the purpose of this instrument is not merely to request assistance if CERT-to-CERT channels are insufficient. The purpose of this instrument is to exert political pressure on the state that is likely responsible for the hostile cyber operation. Requesting assistance on the basis of the UN GGE 2015 norm 13H or on the basis of the international legal due diligence obligation, is intended as a way to signal to the opponent that the origins of the activity are known, that these are considered as violations of international norms and rules and provide the opponent with a decision point on whether to escalate or scale down his activity. The benefit of such signaling through a request for assistance is that it can be done without requiring firm attribution. This notion should also be captured in the description, to differentiate this instrument from normal CERT-to-CERT practice.

Page 3:

- (first paragraph on ‘demarches’):
  - It would be useful to mention that this instrument could also be used by Member States in collaboration with each other, but that the EEAS delegation may play a useful coordinating role in such cases.

- (fourth paragraph, on ‘other instruments):
    - NL would suggest that this paragraph should not be narrowed to actions that are available in response to an internationally wrongful act (such as countermeasures under the law of state responsibility). This paragraph should be expanded to actions that can be undertaken in response to cyber operations that constitute an unfriendly act in general (such as expulsing foreign diplomats).
    - With regards to ‘investigating teams’, it is currently unclear whether this refers to initiating law enforcement investigations or to teams that have been sent abroad to investigate incidents. In the latter case, it is not immediately clear to NL whether such teams are actually used in practice.
    - The second edition of the Tallinn Manual revolves around Cyber Operations in general, not just to Cyber Warfare.
- (fifth paragraph, on 3. How to use the toolbox):
    - It could be clarified whether this paragraph refers to a more developed understanding of how the use of diplomatic instruments could be decided upon or to a more developed understanding of the workings and objectives of coercive cyber operations themselves?

Page 4:

- (top paragraph):
    - Instead of Coordination Group it should read Cooperation Group. That is the correct name of the group. Here it should also say “CSIRTs Network” instead of CSIRT network
    - This Network, however, does not have the EEAS Intcen as a member or observer, as it now suggests. This could be clarified in the text, for example by changing the order in which organisations are listed, and putting IntCen and the HFC before the Cooperation Group.

- (fourth paragraph on ‘making a decision’):
    - NL supports the comments made by Germany in this section.
- (sixth paragraph on ‘following a decision’):
    - It could be helpful to clarify whether such communication is required within the EU or also externally. Because there could be circumstances where it would be preferable to conduct diplomacy in silence, and not make the use of diplomatic instruments public.

Page 5:

- (Regarding Attribution)
    - NL considers it important to take the fact that attribution is primarily a sovereign national decision by Member States as the point of departure for these considerations.
    - Consequently, it might be useful to distinguish here between those cases where it will be a (combination of) Member State(s) who will undertake action, or where the EU institutions will take action. Both situations might require different approaches to attribution, and different types of information sharing and assessment.
    - In cases where Member States act, it might be useful to emphasize their responsibility for determining the level of information that they wish to share and the channels they choose to use, in order to convince other Member States of their attribution assessment.
    - NL supports the first German set of comments (in blue), but proposes to replace the second set of comments (in red) with the shorter:
        - "Attribution consists of two steps: technical attribution and legal attribution. Technical attribution consists of determining who perpetrated the cyber operation. Legal attribution consist of determining the link between the perpetrator and a state for the purpose of establishing whether the conduct can be regarded as that of the state."

- (Necessity and proportionality)
    - Whilst NL has no objections to the German comments and suggestions (in blue) per se, it could be that the purpose of this paragraph was to indicate that each instrument should be used as an when appropriate and in a proportionate manner as described on page 2 (listing scale, scope, duration and intensity). This might be a more useful function for the paragraph than focusing it on situation of an armed attack.

PORTUGAL

Portugal welcomes the document on joint diplomatic response to hostile cyber operations under the threshold of armed attack and would be in favor of its public endorsement by the Foreign Affairs Council if possible in June.

In its conclusions on the subject the Council should nevertheless give a clear mandate to EEAS to conceive, plan and coordinate joint cyber diplomacy exercises encompassing the cyber policy teams of the ministries of Foreign Affairs of MS.

Coercion by state sponsored cyber entities, often under cyber criminal disguise, has been moving swiftly from critical infrastructures of essencial service providers to defense, media and political institutions.

Cyber malicious activity has thus become the weapon of choice in strategic confrontation below the threshold of armed conflict.

Consequently, showing determination at the highest political level to use the whole range of EU and national diplomatic tools, to respond collectively to cyber attacks against MS, is crucial.

SWEDEN

The Cyber Toolbox – Preliminary Swedish comments

Process

SE would welcome Council Conclusions.

What should be included or excluded?

- Council Conclusions could stress the role of coercive cyber operations in relation to the general foreign and security policy concerns of the EU, and thus the need for the EU to develop its tools and policies. Conclusions could stress that the EU has a long term ambition to develop EU action and capacity to support MS, as well as to support partners of the EU.

- Conclusion could highlight the broad and long-term security interest of the EU to counter threats (including cyber operations) to free and global flows of information, for reasons of economic growth, innovation, competiveness, human rights and global development.

- Conclusions should emphasize that cyber operations are subject to international law including international human rights law and international humanitarian law.

- Conclusions should stress the need to make full use of existing mechanisms for joint situational awareness and exchange of information. Also including exchange of information between EU and NATO.

- Conclusions need to clarify the scope for possible initiatives and actions on the EU level

- Conclusions should highlight those possible joint and/or cooperative measures which do not require attribution. The role of voluntary norms for responsible state behaviour as well as confidence building measures should be underlined. Cooperation with other organisations, notably the OSCE, could be underlined.

- Conclusions should firmly stress that a decision to attribute is the sovereign responsibility of the individual Member State, on the basis of its individual political and legal assessment.

- Conclusions need to point out the (connected) areas where further, in depth, legal and political analysis will be needed:
  - the potential scope and process for joint action at the EU-level building on MS' individual attribution
  - the possible use of restrictive measures as a joint response to coercive cyber operations (building on MS' attribution)
  - the legal basis and the implementation of international law

- Conclusions should include a follow up and way forward clause, indicating the areas where further work and analysis will be needed.

UNITED KINGDOM

1. WHY A CYBER TOOLBOX?

In the recent period, we have observed a growing ability and willingness of State and non-state actors, including criminal and terrorist groups, to pursue their objectives by undertaking disruptive or even destructive cyber operations. NATO has declared cyberspace as a domain of operations, "the fourth one". Disinformation using cyber means, cyber-espionage, intellectual property theft, cyber-attacks on infrastructures, cybercrime or cyber conflict, may call for responses going beyond our current communication and cybersecurity policies. Cyber has to be seen also in the context of hybrid threats.

The EU is already taking action on cyber through increased prevention, early warning, resilience and coordination. The Global Strategy for the European Union's Foreign and Security Policy, the 2013 EU Cyber Security Strategy, the EU Cyber Defence Policy Framework, the Network and Information Security (NIS) Directive and the creation of the European Network and Information Security Agency ENISA, the establishment of the CERT- EU and of a European Cyber Crime Centre at Europol address these issues. The joint framework on countering hybrid threats (JOIN(2016)18 final) may be used also.

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 signaling the likely consequences of a cyber-attack would dissuade potential attackers. It would require putting in place solid preparatory practices and communication procedures.

The current Issues paper responds to the PSC tasking of 23 June 2016 on the basis of the Netherlands Presidency non-paper. It presents a toolbox, which could be used by the EU and its Member States to respond to cyber operations.

This should be seen as complementary to, but not a replacement for, existing EU cyber diplomacy engagement. Current diplomatic efforts and operational actions, such as supporting wider compliance with the existing international law such as the Budapest Convention on Cybercrime and reaching common positions in international fora, will continue unabated. But there is a growing need for the EU to protect its long term strategic, security and economic interests and to develop strategic guidelines to do so.

2. WHAT TO INCLUDE INTO THE TOOLBOX?

The cyber toolbox will include instruments that are suitable both for an immediate response to incidents as well as elements that can be used to influence behaviour and deter adverse cyber operations in the longer term. These instruments are presented as options for consideration, where appropriate, and would not preclude action by any individual Member State.

A non-exhaustive list of instruments below is presented in order of presumed impact (from lower to higher impact). The overall proportionality of a response depends on the scale, scope, effect, duration and intensity with which each instrument is used. [1]

[1] It is important to mention the effect, as this is relevant to the response.

Statements by the Council and High Representative for Foreign Policy

Issuing a statement expressing concern or condemning general cyber trends or certain cyber operations could play a signaling function, as well as serve as a form of strategic communication and deterrence against future cyber operations.

Formal Council Conclusions

Issuing general or specific formal Council Conclusions on cyber operations could play a signaling function, underlining awareness and determination on cyber issues and dissuade potential attempts of dividing EU Member States positions by cyber operations.

Formal joint requests for technical assistance through diplomatic channels

Following the Network and Information Security Directive, the primary channel for requesting technical assistance is usually through the Computer Emergency Response Team Contact Networks (designated as CSIRT's contact networks – computer security incident response team). When multiple Member States and/or the EU institutions are affected, it would be beneficial to jointly contact third States using diplomatic levers to formally request technical assistance.

Diplomatic Demarches

EU delegations could, together with Member State embassies, carry out demarches to a number of different ends. For instance, demarches could ask for support in mitigating a particular cyber operation, condemning such an operation or clarifying the circumstances around a cyber-attack with links to its territory.

Signaling through EU bilateral and multilateral topical or political dialogues

Bilateral EU-led political dialogues, particularly cyber dialogues, could also be used to follow-up on statements and raise concerns about certain cyber operations. Concern could be expressed about the suspected cyber operations of third state or non-state actors. Concern could also be expressed in multilateral bodies such as the UN, OSCE, NATO and WTO, and in bilateral dialogues with the secretariats of multilateral bodies, and in particular with the UN Secretariat.

Restrictive measures

The Union may impose restrictive measures 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. 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.

~~***Other instruments***~~

Existing Rights of Member States Under International Law[2] Other forms of diplomatic pressure, such as recalling diplomats or investigating teams could also be considered if deemed necessary.[3] ~~For example the Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0, the most comprehensive analysis of how existing international law applies to cyberspace, provides a more comprehensive list of possible counter-measures for States that have been subject to an internationally wrongful act in the Cyber domain.~~

[2] Clarifies better what is meant by this paragraph

[3] We would like the reference to Tallin 2.0 deleted. It is an academic manual, not an EU agreed text, and should not be referred to in such a way in this document.

3. HOW TO USE THE TOOLBOX

The above-mentioned tools should be implemented as far as possible through the use of existing mechanisms. These tools should be used in a coherent and consistent manner: this requires *inter alia* a more developed understanding of the full scope of 'coercive cyber operations' (see Council document 5797/6/16).

Preparing a decision

Before any collaborative diplomatic response (or position) could be considered, sharing a sufficient degree of information will be of key importance for the EU and its Member States. Making best use of current information-sharing mechanisms will be key.

The Europol Cybercrime Centre (EC3), the NIS Directive established EU Coordination group and EU CSIRT network including CERT-EU, the EEAS' Intcen, including the Hybrid Fusion Cell, all play a valuable role in this regard by sharing analyses, early warning and information related to risks and incidents within their respective constituencies, in accordance with their mandate and the confidentiality of the information.

At a policy level, in order to enhance internal coordination and to help develop a comprehensive and coherent EU approach on cyber issues, a Horizontal Working Party on Cyber issues, chaired by the rotating Presidency, as a formal Council preparatory body, has been established. The Working Party ensures the strategic and horizontal coordination of cyber issues in the Council and can be involved in both legislative and non-legislative activities. On the basis of the relevant information streams, and in accordance with their responsibilities, the Working Party and PSC should act as preparatory bodies for use of the toolbox. The Working Party has a signaling role in this regard.

Preparing decision would also most often require discussing further the issues of the attribution and of the necessity and proportionality of the decision.

Making a decision

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] The respective legal basis, procedure and fora depend on which instrument will be used to respond to a cyber operation, though the Council is the central actor in the decision-making process, and could be a key implementer of the decision, next to the High Representative of the Union for Foreign Affairs and Security Policy and / or the Commission.

Appropriate coordination with like-minded countries and allies should be envisaged, particularly in the context of EU-NATO cooperation.

[4] We agree with this statement, but would like some clarity on which measures fall under which competence, and where these would be MS only, mixed, and EU only. We would agree that these should largely fall to individual Member States, but where it is envisaged that the measures do not fall solely to a Member State, it is important to understand the circumstances. If authorization is deemed to be mixed or for the EU, would it limit an individual Member State's ability to act?

Following a decision

After the decision to impose a measure has been taken, it should be actively and systematically communicated by the EU and its Member States inside and outside of the EU. Therefore it is important that the reasons for which measures are taken are made known and the relevant audience targeted. EEAS StratCom capabilities should be fully used.

A specific communication approach both towards third countries could also be developed as part of the imposition of a measure in cooperation with Member States and the Commission.

Specific communication could also be necessary to the country being at the origin of the wrong-doing, also in order to prevent continuation of the wrong-doing.

Proper attention should be given to the follow-up of a decision and its possible repeal.

4. THE ISSUE OF ATTRIBUTION

A common position based on a sufficient degree of shared situational awareness between Member States is key in order to trigger a response. [5]

~~First, it should be pointed out that most of the instruments presented in this Issues paper do not always require attribution or directing accusations against a given state or non-state actor: they are a means of expressing concerns and signaling them in another way. For instance, regardless of the actual perpetrator, diplomacy can be used to encourage countries that serve as unwitting proxies or transit points for an illegal cyber operation to take action to mitigate the activity. Furthermore, some of these instruments can be tailored to reflect the specific degree of attribution that can be established in a particular case.~~ [6]

[5] As drafted, this suggests that a Member State may not trigger a response without establishing a common position – is this a correct reading of this sentence?

[6] We would suggest deleting this paragraph – as drafted it is confusing and does not add anything of value to the text.

~~Given the well-known problems with confidently attributing cyber operations to a certain actor, it should be clear that in other cases the instruments mentioned should be employed with careful consideration. Evidence used to attribute responsibility should be able to pass the scrutiny of Member States. Restrictive measures should be able to pass judicial scrutiny. Through cross-domain intelligence and political assessments on the possible interests of the attacker, attribution could be established with varying degrees of certainty.~~

The customary international law of State responsibility supplies the standards for attributing acts to states, which can be applicable to activities in cyberspace. In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When attributing an internationally wrongful act to another state, or when taking action in response, a State must act in accordance with international law. In this context, a State assessesthe facts and is free to make its own determination in accordance with international law with respect to attribution of a cyber act to another State.[7]

[8]The United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security recommends following a number of cyber norms and stresses that international law applies in cyberspace. Other principles of customary international law, voluntary norms and confidence building measures relevant to cyberspace include due diligence and state responsibility. They should be used fully to support the attribution process. The limited state practice here underlines the need for careful consideration, but also emphasizes the importance of discussing further these issues at expert level.

---

7 This is taken from the G7 (Lucca) Declaration on Responsible States Behaviour in Cyberspace. We prefer that this language be used for clarity. (The German text inserted here came from an early draft of the declaration and was not the final text.)

8 Much evidence is likely to have come from classified channels and will be subject to disclosure restrictions -it is unlikely that any MS would want to or be able to share all supporting evidence with all MS. And in many cases Member States would not wish to publish any supporting evidence for a particular attribution. We would therefore recommend deleting this paragraph and replacing it with the wording from the G7 Declaration.

5. NECESSITY AND PROPORTIONALITY

The Working Party could address how the various elements of the toolbox could or should be used in order to produce the desired effect, building inter alia on the concepts of necessity and proportionality. Where a cyber operation is considered as an act of aggression, the toolbox can still be used to support or complement appropriate responses.