Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 26 February 2021

WK 2690/2021 ADD 1

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 - Comments by FR, DE, EL and PL delegations on Articles 5 to 11

Delegations will find in Annex comments by FR, DE, EL and PL delegations on Articles 5-11.

TABLE OF CONTENT

France

Commentaires portant sur les articles 5 à 11

Dans la perspective de la réunion du groupe horizontal sur les questions cyber du 2 mars 2021, les autorités françaises souhaitent partager avec la Présidence de premiers éléments d'analyse sur la proposition de directive en objet. Les autorités françaises tiennent cependant à souligner que l'analyse du document à l'échelle nationale se poursuit et que ces éléments pourraient être appelés à évoluer au cours des négociations.

Sur l'**article 5**, les autorités françaises accueillent positivement les propositions de la Commission européenne, qui doivent permettre aux États de renforcer leurs capacités. Plus spécifiquement, les autorités :

- souhaitent interroger la Commission sur la finalité recherchée à travers le libellé du paragraphe (1c), dont le périmètre et l'objectif doivent être précisés. Les autorités françaises tiennent à souligner la difficulté - voir l'impossibilité - de mettre en œuvre une analyse de risque unique à l'échelle nationale, en prenant en compte l'ensemble des spécificités sectorielles et des administrations publiques. Si une méthodologie d'analyse du risque a du sens à l'échelle d'une organisation, transposer une telle méthode à l'échelle nationale ne semble pas réaliste ;
- soutiennent l'approche relative à la sécurisation des chaines d'approvisionnement et la divulgation coordonnée des vulnérabilités. Un débat sera nécessaire sur les libellés et périmètres de la proposition mais l'objectif poursuivi est bénéfique au regard de l'état de la menace. Sur le sujet précis de la divulgation coordonnée des vulnérabilités (CVD), la France attachera un intérêt particulier à la protection des chercheurs et des lanceurs d'alerte en la matière ;
- s'interrogent sur la finalité des indicateurs de performance clé (KPI) et l'utilisation qui pourra en être faite à l'échelle de l'Union Européenne.

Sur l'**article 6**, les autorités françaises accueillent positivement la proposition de la Commission. Le passage à l'échelle en matière de CVD doit *in fine* contribuer à la mise en œuvre de la sécurité du marché unique numérique. Les autorités françaises pourront toutefois souligner que ce mécanisme devra respecter la souveraineté de chaque État membre dans le traitement des vulnérabilités remontées. Plus précisément, les autorités françaises :

- rappellent leurs précédents commentaires sur la définition de vulnérabilité retenue à l'article 4 (8) qui devrait largement reposer sur les travaux menés à l'Organisation de coopération et de développement économiques (OCDE) ou par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ;
- soulignent que ce nouveau mécanisme européen devra s'inscrire en cohérence avec le règlement sur la cybersécurité (*Cybersecurity Act*) et les dispositions prévues en la matière dans les schémas de certification;

- regrettent que le rôle attribué aux équipes de réponse aux incidents de sécurité informatique (CSIRTs) dans le mécanisme de CVD ne soit pas reflété dans l'article idoine (article 10);
- affirment la nécessité de clarifier la finalité du registre telle qu'abordée dans les considérants 30 et 31. En effet, il est important de distinguer les besoins de partage d'informations (i) entre les CSIRTs des États membres dans le cadre de la coordination du traitement d'une vulnérabilité impliquant plusieurs éditeurs ou fournisseurs de service au sein de l'Europe et (ii) pour communiquer envers les utilisateurs des produits et services. L'article 6 alinéa 2 devrait de la même manière définir l'usage du registre et identifier les personnes susceptibles d'y accéder (i) si le registre est utilisé pour coordonner le traitement d'une vulnérabilité ou (ii) s'il sert à publier des informations sur les vulnérabilités;
- soulignent enfin que, la gestion par l'ENISA d'un tel registre pose en filigrane la question de sa capacité à gérer des informations sensibles. Si l'ENISA venait à assumer ce type de missions, une sécurisation de ses réseaux de communication sera incontournable.

Sur l'**article 7**, les autorités françaises accueillent favorablement les propositions de la Commission, qui font écho à la structuration du cadre européen de gestion de crise. Plus spécifiquement, les autorités françaises:

- indiquent à ce titre qu'un lien devrait être effectué avec le réseau EU-CyCLONe institué à l'article 14, les autorités étant désignées au titre du paragraphe 1 ayant vocation à participer au réseau;
- s'interrogent sur la différence d'objectifs poursuivis entre les paragraphes 2 et 3: les autorités françaises considèrent que le paragraphe 2 devrait éventuellement s'inscrire comme une composante du plan national;
- rappellent que tout plan national de gestion de crise cyber doit s'inscrire dans une stratégie nationale plus large, les incidents d'origine cyber provoquant toujours des conséquences sectorielles;
- soulignent qu'il serait opportun que les plans nationaux prévoient également un exercice de retour d'expérience suite à un exercice ou un incident (i.e. "*post-mortem analysis*").

Sur l'article 9, les autorités françaises soulignent que l'animation de la communauté au niveau national par le CSIRT doit relever d'une obligation de moyens et non de résultats.

Sur l'**article 10**, les autorités françaises:

- rappellent que l'assistance mutuelle doit s'inscrire dans le respect des prérogatives souveraines des États membres. Aborder cette question à l'échelle de l'UE est extrêmement pertinent, mais la mise à disposition de capacités devrait s'effectuer sur une base volontaire;
- s'interrogent sur la pertinence de maintenir la lettre (b) du paragraphe 4 dans cet article: cette mission pourrait échoir plus naturellement aux autorités compétentes désignées au titre du paragraphe 1 de l'article 7 (qui participeront également au réseau CyCLONe).

Sur l'**article 11**, les autorités françaises:

- soulignent qu'il serait pertinent, afin d'assurer la cohérence des procédures et de la coopération, de prévoir également une notification des autorités de gestion de crise cyber désignées au titre de l'article 7;
- rappellent les interrogations de la France sur la notion de "*near misses*", qui ne trouve pas de définition à l'article 4.

Les autorités françaises se tiennent à la disposition de la Présidence portugaise pour toute précision utile.

GERMANY

Please note: The following list of comments and questions regarding Art. 5 – 11 NIS2 is non-exhaustive and may be expanded in future discussions. Comments and questions are sorted by order of the Articles.

1. Question regarding Art. 5 in general – In case of Germany, the jurisdiction for some policies stated in Art. 5 lies with the federal states. Please advise if it is the Commission's view that in such cases, Member States may refrain from including these policies in their national cybersecurity strategy, seen that this is adopted by the federal government.

2. Question regarding Art. 5 para. 1 lit. c – The term "assets" could be interpreted to have two different meanings: (i) assets in the sense of those at the disposal of the Member State to counter the risks or (ii) those assets within a Member State that are facing cybersecurity risks. Kindly explain the intention behind the term and clarify the term's meaning.

3. Question regarding Art. 5 para. 2 lit. d – What is the Commission's understanding of the term „public core of the open internet" and why does the Commission only address availability and integrity, while confidentiality is not included?

4. Question regarding Art. 5 para. 1 lit. f – Kindly elaborate the Commissions view what "a policy frame-work for enhanced coordination" would have to include (at a minimum).

5. Question regarding Art. 5 para. 2 – Why has the Commission opted to include regulatory prescriptions like policies and guidelines in the areas of public procurement or supply chains into national security strategies and not have them separately?

6. Question and Comment regarding Art. 5 para. 2 lit. a – Kindly elaborate on the exact objective of including supply chains here. It appears that the aim is to create a concept for improving the existing supply chains of ICT currently used in important entities. In light of the diversified system landscape and, in particular, complex, globally branched supply chains with focus areas in China and the United States, this is only possible to a limited extent and the possibility to achieve effects appears doubtful. Rather, concepts for improving cybersecurity should be created through the use of corresponding products with secure supply chains or the establishment of secure supply chains.

7. Comment regarding Art. 6 – Germany also sees the need to implement a national Vulnerability Equities Process (VEP) in parallel to the CVD to ensure a coordinated approach how to classify vulnerabilities for disclosure and concurrent use for security agencies. A national way forward is currently under discussion. In order to prevent erosion of trust in the CVD process, it is also important that vulnerabilities, which have been shared via the CSIRT network, may not be misused by other member states. Germany supports the initiative for ENISA to host a common vulnerability database.

8. Question regarding Art. 6 para. 2 – How should the relationship between Art. 6 para. 2 and Art. 10 para. 2 lit. b be understood? Both provisions concern the disclosure of information on vulnerabilities to entities. However, in one case this is done by ENISA and once by the respective CSIRTs. How is it ensured that the information does not contradict each other in individual cases (i.e. communication)?

9. Comment regarding Art. 7 – Art. 7 does apparently not draw a clear distinction between crises in cyberspace and conventional crises. Thus, para. 1 mentions incidents and crises in general or the authorities responsible for them, while para. 3 in turn specifically addresses cybersecurity incidents and crises. This should be clarified.

10. Question regarding Art. 7 para. 4 – According to this provision, the member states shall notify the Commission of their national plans for responding to cybersecurity incidents and crises, with reference to para. 3, with extensive details of the crisis management procedure and the appropriate channels for information exchange, etc. Would the Commission agree, that this would pose a dangerous bundling of information in a central location, which in the wrong hands could pose an enormous threat to cybersecurity in Europe?

11. Question regarding Art. 9 para. 1 – This provision requires "incident handling in accordance with a well-defined process". Does this provision contain an implicit requirement for the creation of process descriptions?

12. Question regarding Art. 10 para. 2 lit. e and f – We note that both these provisions are new and a substantive extension of tasks. Could the Commission kindly explain the meaning of “mutual assistance” as depending thereon, it would be subject to different requirements.

GREECE

Comments on Articles 5-11 of the NIS 2.0 proposal (COM(2020) 823 final)

Art. 5

We consider that the inclusion of an explicit reference to measures/policies for the promotion of cybersecurity with privacy would also be highly beneficial as part of national cybersecurity strategies, in line with ENISA's recommendations and good practice guides.

Art. 7 par. 4

We propose the deletion of the word "strictly".

Art. 9 par. 5

> This paragraph needs to be discussed in combination with art. 16 of the proposal. In any case, participation of national CSIRTs in peer reviews should be performed on a voluntary basis.

POLAND

Poland has a scrutiny reservation on art. 5 to 11 NIS2 as they are currently under examination.

Art. 5

1) Art. 5.1.a - The strategy should include the objectives and priorities not the definition of the objectives and priorities.
2) Art. 5.1.b - Could the EC elaborate why in NIS2 this point mentions "public bodies and entities" when in the NISD it is "government bodies".
3) Ar. 5.1.c – The phrase "an assessment to identify relevant assets and cybersecurity risks" is not clear. Shouldn't we rather speak of identification of assets and risks, and assessment of risks?
4) Art. 5.1.d – Why the preparedness, response and recovery is limited to incidents, shouldn't for example threats also be considered?
5) Art. 5.1.e – This para refers to "various authorities and actors", when para b) to "public bodies and entities as well as relevant actors". Shouldn't these two provisions be aligned?
6) Art. 5.1 – There is a need to add also additional para on the sources of financing for the implementation of the Strategy
7) There is a need to thoroughly analyse para 2 and clarify its provisions.
8) Art.5.2.d – What does is mean "the general availability and integrity"? Why there was a need to add adjective "general"? Could the EC elaborate on the meaning of the phrase "the public core of the open internet"? Shouldn't the wording regarding the internet be aligned with the one used for example in the CC on Cybersecurity Strategy?
9) Art. 5.2.e – Why was the education omitted in this para? There is a need to rephrase this para to be more clear.
10) Art. 5.2.f – Could the EC elaborate why "the policy to develop cybersecurity tools and secure network infrastructure" was limited only to academic and research institutions?
11) Art. 5.2 – There should a provision clarifying what will happen with the Strategies notified under the NISD.
12) Art. 5.3 - This para relates to "key performance indicators" whereas in previous para there was no mentioning that these indicators should be established.
13) Art. 5.4 – The last sentence should be a separate para.
14) Every Strategy should also entail a detailed action plan with the timeline. We propose to add provision on that.

Art. 6

1) Art. 6.1 – Could the EC explain what is "the reporting entity" mentioned in this para? Para 2 refers to "important and essential entities and their suppliers".
2) Coordinated Vulnerability Disclosure shall not be CSIRT responsibility only as it has broader aspects than just technical failures and cover as well manufacturer or provider responsibilities, which is out of the scope of CSIRTs and may require engagement by competent authorities/national cybersecurity authorities.
3) There is a need to clarify the provisions on the registry. The following questions arise:
    a. What kind of vulnerabilities will be registered?
    b. Who will sent the notifications to the registry?
    c. Will the entities sent the notifications directly to ENISA or via national authorities (preferred model) ?
    d. Will the information on the vulnerabilities be checked/verified before being put to the register?
    e. What the conditions of access to the registry will be?
    f. Will the register be public or only available to certain entities, if the latter what sort of entities?
4) There should be a deadline for ENISA to develop the registry.
5) MS should be involved in establishing the policies and procedures mentioned in para 2.
6) The tasks of the designated CSIRT should be in the article not in the recital (recital 29). There is a need for clarity when it comes to provisions on the designated CSIRT and its role.
7) The recital 30 states that entities which do not fall in the scope of the Directive may, on voluntary basis, disclose the vulnerabilities. This is not reflected in the art. 6.2.
8) Could the EC elaborate what are the "structured cooperation agreements" mentioned in recital 31, what is the difference between cooperation agreement and a structured one? What will these agreements encompass?

Art. 7

1) Implementation of these provisions requires stronger alignment of the cybersecurity and critical infrastructure frameworks. What are the plans of the EC in this respect, notably coordination between DG Home and DG Connect? We would much welcome an analyses how the NIS2 and the directive on resilience of critical entities is synchronized when it comes to cybersecurity crises, to avoid any duplication of tasks and overlapping competences.
2) The directive on resilience of critical entities foresees establishment of cooperation group. Could the EC elaborate why there is a need to designate competent authorities responsible for management of large – scale incidents and crises under NIS2 and no to use the structure of the cooperation group from the directive on resilience of critical entities?

3) There should be a possibility that the plans mentioned in para 3, could be part of plans on the protection of the critical infrastructure. It should not be necessary to always establish separate plans dedicated only to cybersecurity incident and crisis response.

Art. 8

Art. 8.4 - In comparison to the NISD provisions, the NIS2 omitted the SPOC's tasks to ensure cooperation with the NIS CG and the CSIRT Network. Could the EC elaborate on the reasoning to introduce these changes?

General comment to art. 8 and 9 – Regarding the articles on CSIRTs, it would be good to know the opinion on these provisions of the CSIRT Network, where the experts are gathered, notwithstanding the leading role of the HWP CI to negotiate the draft. What are the plans to include the CSIRT Network and NIS CG in the discussions? We believe there is a need to reflect on this issue.

Art. 9

1) To avoid incident reporting degradation there is a need to highlight that incident details shared by entities with CSIRTs shall not be used by competent authorities for penalization.
2) Art. 9.5 - What would be the role of CSIRTs in the peer reviews? Art. 16 states that peer reviews will be conducted by technical cybersecurity experts drawn from MS and does not foresee any role for the CSIRTs.

Art. 10

1) Art. 10.1 introduces the term "constituency". This term is only used once in the draft. Therefore there might be a need for clarification.
2) Art. 10.4 - The adoption of common taxonomies would entail alignment of many legal frameworks, notably critical infrastructure, the NISD, as well as legislation specific for CSIRTs exercising their powers in defense and national security. This constitutes a mayor challenge both at national and European level. Therefore there is a need to introduce in the Directive provisions/recitals facilitating the achievement of the synergies at the European and national level. Current proposal seems to be insufficient.

Art. 11

1) Art. 11.2 - This para states that MS shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and **near misses** submitted pursuant to this Directive. There is no obligation to notify near misses, only a possibility on a voluntary basis in accordance with art. 27. Therefore it is not possible to receive the notifications when there is no obligation to submit them.

2) Art. 11.3 - The same comment regarding near missed as in para 2.

3) Art. 11.4 - The obligation to cooperate between different authorities should be designed in a more general, future proof way. There might be different sectorial legislations like DORA in future.

4) Art. 11.5 - The information to be transmitted encompasses cybersecurity risks, cyber threats and incidents. Could the EC elaborate why in this provision the term risk remained, while for example in art. 10.2.b risks are not listed, instead the provision relates to cyber threats.