Council of the European Union
General Secretariat

Brussels, 07 June 2018

WK 6758/2018 REV 2

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (09.09.2021)

LIMITE

CYBER
COPEN
COPS
COSI
DATAPROTECT
JAI
JAIEX
POLMIL
TELECOM
DAPIX

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:	Draft Council Conclusions on EU Coordinated response to Large Scale Cybersecurity Incidents and Crises - Comments from Member States (CZ, DE, ES, FR, LV, LT, NL and SE)

Delegations will find in Annex Member States comments on the draft Council Conclusions on EU Coordinated response to Large Scale Cybersecurity Incidents and Crises. The REV 2 version of this document contains the comments of Latvia.

TABLE OF CONTENT

Pages

CZECH REPUBLIC 2

GERMANY 3

SPAIN 8

FRANCE 9

LATVIA 14

LITHUANIA 15

NETHERLANDS 20

SWEDEN 24

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

GERMANY

Draft Council conclusions on EU coordinated response to large scale cybersecurity incidents and crises

The Council of the European Union,

1. RECOGNISING the need for an efficient EU level response to large scale cyber incidents and crises as stressed in the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU of 20 November 2017[1].

2. RECALLING the Council conclusions of 19 June 2017[2] on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox") and the corresponding implementing guidelines of 11 October 2017 as well as the Council conclusions on the Integrated Political Crisis Response arrangements[3].

3. TAKING INTO CONSIDERATION the Commission Recommendation of 13 September 2017[4] on a Coordinated Response to Large-scale Cybersecurity Incidents and Crises and the core objectives and guiding principles set out therein.

4. RECOGNISING the competences of the Member States **in the field of IT crisis management** and their responsibility for national security in the domain of cybersecurity.

5. WELCOMING the adoption of the CSIRTs Network Standard Operating Procedures (SOPs) ~~and the on-going work within the Cooperation Group on a common taxonomy for cybersecurity incidents~~.

Commented [A1]: In this context it is important to emphasize that IT crisis management is a part of the MS responsibility for national security in the domain of cybersecurity

Commented [A2]: In general, we share the view that the operational information exchange should be developed further and made easier Nonetheless, it also should to be stated that the aim of creating a common taxonomy still deserves a thorough discussion It is in this regard important to preserve the necessary flexibility Individual taxonomies should not be prevented a priori as they may be used to meet situation-specific requirements

[1] 14435/17

[2] 9916/17

[3] 10708/13

[4] C(2017) 6100 final

6. RECOGNISING the on-going work on the Law Enforcement Emergency Response Protocol, that describes a mechanism for early detection and identification of cyber incidents and crises, eventually leading to an investigation under the normal applicable operating procedures, complementing and aligning a response by the law enforcement community with existing EU crisis response mechanisms.

7. BUILDING on the discussions at the Cybersecurity Challenges Conference in Sofia on 26 March 2018.

Commented [A3]: We suggest specification of the results of the discussions

8. ~~WELCOMING~~ **TAKING INTO CONSIDERATION** the Memorandum of Understanding to establish a framework for cooperation signed by ENISA, EC3, CERT-EU and the EDA which will further strengthen their cooperation within their respective mandates~~, in particular on matters of information exchange, cyber exercises as well as technical cooperation~~.

9. UNDERLINING the need to make use of the existing crisis management mechanisms, processes and procedures **on national and EU level**.

Commented [A4]: In this context it is important to emphasize that there are already existing crisis management mechanisms, processes and procedures on national as well as on European level

10. RECALLING the importance of an effective implementation of the Directive on Security of Network and Information systems[5] and the development of capabilities of national CSIRTs and competent authorities as regards responding to and handling of cybersecurity incidents.

11. RECALLING that activities ~~at Member States and~~ EU level~~, as well as cross-border cooperation,~~ with regard to cyber incidents and crisis take place following the principles of subsidiarity and proportionality.

Commented [A5]: Member States and cross-border cooperation underlies different rules than the EU regarding the principle of subsidiarity and proportionality in accordance with Art 5 of the EU Treaty

12. ~~RECOGNISING the importance of shared situational awareness, coordinated public communication and effective response during large-scale cybersecurity incidents and crises.~~

Commented [A6]: 1) "*Shared situational awareness*": A joint understanding (common situational awareness) can only be reached on the basis of national conclusions and evaluations The present text does not state that clear enough

2) "*Coordinated public communication*": Crisis communication in case of a cyber incident follows the same rules as any crisis communication Guidance and responsibilities have already been established These established rules on communication in crisis situations provide ways to reach a joint understanding within the EU on the basis of national assessments They also apply to large-scale crises and cyber incidents

[5] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19 7 2016, p 1)

Fostering the preparedness and crisis prevention

13. ~~RECALLING the need to prevent cyber incidents and crises by continuing to bolster EU capabilities to address cyber threats.~~

14. CALLS upon the Member States to ensure that their national crisis management mechanisms adequately address cyber incidents and crisis as well as provide necessary procedures for cooperation at EU level at the technical~~,~~ **and** operational ~~and political~~ level.

Increasing the situational awareness

15. CALLS upon the EU institutions, agencies and bodies and its Member States to cooperate and contribute to EU level situational awareness both before and during cyber incidents and crises through regular EU Cybersecurity Technical Situation Reports~~ and EU Cybersecurity Operational Situation Reports~~.

Ensuring the effective response

16. ~~RECOGNISING that crises response can take many forms and requires a coordinated approach at EU level, ranging from identifying technical measures to operational measures as well as political measures, depending on the type of incident or crises.~~

17. ~~CALLS upon the Member States to identify, develop and implement further means of operational cooperation, including in the CSIRTs Network SOPs, in relation to early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents~~.

18. CALLS upon the Member States to identify and put in place a corresponding cooperation protocol and SOPs recognising that cyber incidents have the potential of leading to a cross-sectorial crisis, i.e. impacting simultaneously the functioning of different sectors, infrastructures or services, stressing the need to establish appropriate procedures and concrete measures for timely information sharing and situational awareness at operational level amongst competent authorities, such as the national Single Point of Contacts under the NIS Directive.

Commented [A7]: The main purpose of the blueprint is the enhancement of cooperation related to preparedness for a large-scale cyber incident This should be reflected also in the Council Conclusions which focus too much on response and crisis communication

Commented [A8]: This mono-causal statement would imply that the prevention of cyber incidents and crises mainly lies within the competences of the EU It is however essential to state that cybersecurity and incident and crises prevention mainly lies within the competences of the Member States

Commented [A9]: The Blueprint partially aims at establishing a political decision making structure specifically for cyber incidents However this is already in detail regulated in the IPCR and its SOP We should avoid to establish a second parallel structure At least the political level should be taken out of the Blueprint Therefore we ask for deletion of the highlighted text

Commented [A10]: EU labelled reports would only be the end product of the individual "Cybersecurity Technical Situation Reports" which shall be provided by the "EU institutions, agencies and bodies and its Member States" Hence the prefix "EU" is misleading and suggests that the EU has the monopoly to compile unified "Technical Situation Reports" That wrong impression has to be avoided

Commented [A11]: The NIS Directive primarily promotes the necessity of operational cooperation between the Member States Therefore, it should not be stated that a "coordinated approach at EU level" is primarily "required"

Commented [A12]: Mandate and tasks of the CSIRTs Network already include these goals Therefore it seems neither necessary nor helpful to prescribe certain aspects of closer cooperation within the framework of these Council Conclusions
Only if this passage should not be deleted, we would then ask for the following concretization: "CALLS UPON the Cooperation Group"

Commented [A13]: Does this mean that there must always be EU cooperation/information, even if an MS decides to act alone against an attack?

Implications not clear Legislation assignments (if this is meant) are not to be made within the context of Council conclusions

Commented [A14]: It is not clear which "corresponding cooperation protocol and SOPs " are meant here If it refers to 17) then the CSIRT Networks SOPs should explicitly be mentioned

Commented [A15]: Is this an obligation to inform the other EU states/institutions in any case?

19. ~~CALLS upon the Commission to bring forward a legislative proposal for a Cybersecurity Emergency Response Fund.~~

Commented [A16]: What is the aim of the Cybersecurity Emergency Response Fund? Legal basis? If that is not clear, the point should be deleted

20. Streamlining the public communication

Commented [A17]: As stated above: Crisis communication in case of a cyber incident follows the same rules as any crisis communication Guidance and responsibilities have already been established These established rules on communication in crisis situations provide ways to reach a joint understanding within the EU on the basis of national assessments They also apply to large-scale crises and cyber incidents

21. RECOGNISING that public communication could refer to communication about an incident to the public as a whole, communication of more technical or operational information with critical sectors and/or those who have been affected, as well as could serve as a clear signal of likely consequences of a diplomatic response to influence the behaviour of potential aggressors.

22. CALLS upon the EU institutions~~ and Member States~~ to ensure effective~~ and, where necessary, coordinated~~ communication towards the public~~, keeping in mind that aligning the public communication to mitigate negative effects of cybersecurity incidents and crises and the public communication to influence a potential aggressor is essential for a diplomatic response to be effective~~.

Building on the lessons learned and post incident analysis

23. CALLS upon the EU institutions and Member States to ~~promote and share the analysis of operational and strategic aspects of lessons~~**continue building trust and confidence with regard to the operational cooperation**~~ of large cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved~~.

Commented [A18]: Who are "relevant actors involved"?

Developing a European Cybersecurity Crisis Cooperation Framework

24. CALLS upon the Member States and the EU institutions, agencies and bodies to jointly work towards development of European Cybersecurity Crisis Cooperation Framework within the context of EU crisis management mechanisms, in particular the IPCR, taking into account their respective roles, mandates and competences, putting in place the practical operationalisation and documentation of all the relevant actors, mechanism, processes and procedures.

~~CALLS upon the relevant stakeholders to undertake necessary steps to remove any obstacles and/or fill in any gaps identified both in terms of information flows and in terms of interoperability of the procedures and mechanisms as well as to establish links among the mechanisms, processes and procedures where necessary.~~

Commented [A19]: The whole of that passage remains highly unclear and cannot be supported Therefore we ask for deletion

SPAIN

COMMENTS to the Draft Council Conclusions on EU Coordinated response to Large Scale Cybersecurity Incidents and Crises (doc 9240/18 - 29th May 2018)

10. RECALLING the importance of an effective implementation of the Directive on Security of Network and Information systems and the development of capabilities of national CSIRTs, competent authorities and Single Points of Contact as regards responding to and handling of cybersecurity incidents.

Fostering the preparedness and crisis prevention

13. UNDERLINING the need to make use of the existing cyber exercises, in particular the Cyber Europe organized by ENISA, to test crisis management mechanisms, processes and procedures at technical, operational and strategic/political level.

Increasing the situational awareness

15. CALLS upon the EU institutions, agencies and bodies and its Member States to cooperate and contribute to EU level situational awareness at all levels (technical, operational, strategic) both before and during cyber incidents and crises through regular EU Cybersecurity Technical Situation Reports and EU Cybersecurity Operational Situation Reports.

Ensuring the effective response

17. CALLS upon the Member States to identify, develop and implement further means of operational cooperation among the Single Points of Contact, including in the CSIRTs Network SOPs , in relation to early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents.

FRANCE

Les autorités françaises remercient la Présidence pour la transmission de sa proposition de conclusions du Conseil sur une réponse coordonnée aux incidents et crises transfrontières de cybersécurité (document 9240/18) transmis le 29 mai 2018 aux États membres, sur lequel elles tiennent à lui faire part des commentaires suivants.

De manière générale, les autorités françaises souhaitent, au travers de leurs commentaires, réaffirmer :

- la responsabilité de chaque Etat membre de l'Union dans le renforcement de ses propres capacités de prévention et de réponse aux incidents de cybersécurité ;
- les principes directeurs de proportionnalité, de subsidiarité et de complémentarité sur lesquels repose le Plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cyber sécurité majeurs.

Les autorités françaises estiment par ailleurs nécessaire que les Etats membres puissent affiner les modalités de leur coopération au niveau opérationnel pour répondre efficacement aux incidents de cybersécurité de grande ampleur. Dans cette perspective, les autorités françaises considèrent que le Groupe de coopération établi par la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union est une enceinte pertinente au sein de laquelle les travaux de déclinaison du plan d'action pourraient être poursuivis. Il est suggéré notamment que le Groupe de coopération puisse soumettre les premiers résultats de ces travaux au Groupe horizontal du Conseil sur les questions cyber (GHQC) d'ici à la fin de l'année 2018. Il appartiendra ensuite aux Etats Membres de l'Union européenne de se prononcer sur l'adoption du « *Blueprint* » tel qu'affiné au niveau du Groupe de coopération et du GHQC sur la base de la proposition de la Commission.

Les autorités françaises se réservent la possibilité de compléter, de préciser ou d'amender leur position, ainsi que les commentaires exprimés ci-dessus.

Draft Council conclusions on EU coordinated response to large scale cybersecurity incidents and crises

The Council of the European Union,

1. RECOGNISING the need for an efficient EU level response to large scale cyber incidents and crises as stressed in the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU of 20 November 2017[6].

2. RECALLING the Council conclusions of 19 June 2017[7] on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox") and the corresponding implementing guidelines of 11 October 2017 as well as the Council conclusions on the Integrated Political Crisis Response arrangements[8].

3. TAKING INTO CONSIDERATION the Commission Recommendation of 13 September 2017[9] on a Coordinated Response to Large-scale Cybersecurity Incidents and Crises- and the core objectives and guiding principles set out therein.

4. RECOGNISING the competences of the Member States and their responsibility for national security in the domain of cybersecurity.

5. WELCOMING the adoption of the CSIRTs Network Standard Operating Procedures (SOPs) and the on-going work within the Cooperation Group on a common taxonomy for cybersecurity incidents.

6. RECOGNISING the on-going work on the Law Enforcement Emergency Response Protocol, that describes a mechanism for early detection and identification of cyber incidents and crises, eventually leading to an investigation under the normal applicable operating procedures, complementing and aligning a response by the law enforcement community with existing EU crisis response mechanisms.

7. ~~BUILDING on~~TAKING NOTE of the discussions at the Cybersecurity Challenges Conference in Sofia on 26 March 2018.

[6] 14435/17

[7] 9916/17

[8] 10708/13

[9] C(2017) 6100 final

8. ~~WELCOMING~~ TAKING INTO CONSIDERATION the Memorandum of Understanding to establish a framework for cooperation signed by ENISA, EC3, CERT-EU and the EDA which will further strengthen their cooperation within their respective mandates, in particular on matters of information exchange, cyber exercises as well as technical cooperation.

9. UNDERLINING the need to make use of the existing crisis management mechanisms, processes and procedures on national and European level.

10. RECALLING the importance of an effective implementation of the Directive on Security of Network and Information systems[10] and the development of capabilities of national CSIRTs and competent authorities as regards responding to and handling of cybersecurity incidents.

11. RECALLING that activities at Member States and EU level, as well as cross-border cooperation, with regard to cyber incidents and crisis take place following the principles of subsidiarity and proportionality.

12. RECOGNISING the importance of shared situational awareness, coordinated public communication and effective response during large scale cybersecurity incidents and crises.

Fostering the preparedness and crisis prevention

13. RECALLING the need to prevent cyber incidents and crises by continuing to bolster EU Member States' capabilities to address cyber threats.

14. CALLS upon the Member States to ensure that their national crisis management mechanisms adequately address cyber incidents and crisis as well as provide necessary procedures for cooperation at EU level at the technical, operational and political level.

Increasing the situational awareness

15. CALLS upon the EU institutions, agencies and bodies and ~~its~~ Member States to cooperate and contribute to EU level situational awareness both before and during large-scale cyber incidents and crises through regular EU Cybersecurity Technical Situation Reports and EU Cybersecurity Operational Situation Reports.

[10] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19 7 2016, p 1)

Ensuring the effective response

16. RECOGNISING that crises response can take many forms and may require~~s~~ a coordinated approach at EU level, ranging from identifying technical measures to operational measures as well as political measures, depending on the type of incident or crises.

17. CALLS upon the ~~Member States~~ Cooperation Group to identify, develop and implement further means of ~~operational~~ cooperation at the operational level, including in relation with the CSIRTs Network SOPs, in relation to early warnings, mutual assistance and principles and modalities for coordination ~~when Member States respond~~ of response to cross-border risks and incidents and to report on progress to the Horizontal Working Party on Cyber issues no later than December 2018.

18. CALLS upon the Member States to identify and put in place a corresponding cooperation protocol and SOPs at national level, recognising that cyber incidents have the potential of leading to a cross-sectorial crisis, i.e. impacting simultaneously the functioning of different sectors, infrastructures or services, stressing the need to establish appropriate procedures and concrete measures for timely information sharing and situational awareness at operational level amongst competent authorities, ~~such as~~including the national Single Point of Contacts under the NIS Directive.

~~19. CALLS upon the Commission to bring forward a legislative proposal for a Cybersecurity Emergency Response Fund.~~

Streamlining the public communication

20. RECOGNISING that public communication could refer to communication about an incident to the public as a whole, communication of more technical or operational information with critical sectors and/or those who have been affected, as well as could serve as a clear signal of likely consequences of a diplomatic response to influence the behaviour of potential aggressors.

21. CALLS upon the EU institutions and Member States to ensure effective and, where necessary, coordinated communication towards the public, ~~keeping in mind that aligning the public communication~~as a mean -to mitigate negative effects of cybersecurity incidents and crises and ~~the public communication~~ to influence ~~a~~ potential aggressor, which is essential for a diplomatic response to be effective.

Formatted: English (United Kingdom), Strikethrough

Commented [ALT20]: Council already stated in Nov 2017 that it "NOTE[D] the possibility to examine, should the Commission present a proposal for the establishment of a Cybersecurity Emergency Response Fund…"

Formatted: Default Paragraph Font, English (United Kingdom), Strikethrough

Formatted: English (United Kingdom), Strikethrough

Building on the lessons learned and post incident analysis

22. CALLS upon the EU institutions and Member States to promote and share the analysis of operational and strategic aspects of lessons of large-scale cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved.

Developing a European Cybersecurity Crisis Cooperation Framework

23. CALLS upon the Member States and the EU institutions, agencies and bodies to jointly work towards development of European Cybersecurity Crisis Cooperation Framework within the context of EU crisis management mechanisms, in particular the IPCR, taking into account their respective roles, mandates and competences, putting in place the practical operationalisation and documentation of all the relevant actors, mechanism, processes and procedures.

24. CALLS upon the relevant stakeholders to undertake necessary steps to remove any obstacles and/or fill in any gaps identified both in terms of information flows and in terms of interoperability of the procedures and mechanisms as well as to establish links among the mechanisms, processes and procedures where necessary.

[redacted]

[redacted]

- [redacted]
- [redacted]

  [redacted]
- [redacted]

  [redacted]

LITHUANIA

Draft Council conclusions on EU coordinated response to large scale cybersecurity incidents and crises

The Council of the European Union,

1. RECOGNISING the need for an efficient EU level response to large scale cyber incidents and crises as stressed in the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU of 20 November 2017[11].
2. RECALLING the Council conclusions of 19 June 2017[12] on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox") and the corresponding implementing guidelines of 11 October 2017 as well as the Council conclusions on the Integrated Political Crisis Response arrangements[13].
3. TAKING INTO CONSIDERATION the Commission Recommendation of 13 September 2017[14] on a Coordinated Response to Large-scale Cybersecurity Incidents and Crises and the core objectives and guiding principles set out therein.
4. RECOGNISING the competences of the Member States and their responsibility for national security in the domain of cybersecurity.
5. WELCOMING the adoption of the CSIRTs Network Standard Operating Procedures (SOPs) and the on-going work within the Cooperation Group on a common taxonomy for cybersecurity incidents.

[11] 14435/17

[12] 9916/17

[13] 10708/13

[14] C(2017) 6100 final

6. RECOGNISING the on-going work on the Law Enforcement Emergency Response Protocol, that describes a mechanism for early detection and identification of cyber incidents and crises, eventually leading to an investigation under the normal applicable operating procedures, complementing and aligning a response by the law enforcement community with existing EU crisis response mechanisms.

7. BUILDING on the discussions at the Cybersecurity Challenges Conference in Sofia on 26 March 2018.

8. WELCOMING the Memorandum of Understanding to establish a framework for cooperation signed by ENISA, EC3, CERT-EU and the EDA which will further strengthen their cooperation within their respective mandates, in particular on matters of information exchange, cyber exercises as well as technical cooperation.

9. UNDERLINING the need to make use of the existing crisis management mechanisms, processes and procedures.

10. RECALLING the importance of an effective implementation of the Directive on Security of Network and Information systems[15] and the development of capabilities of national CSIRTs and competent authorities as regards responding to and handling of cybersecurity incidents.

11. RECALLING that activities at Member States and EU level, as well as cross-border cooperation, with regard to cyber incidents and crisis take place following the principles of subsidiarity and proportionality.

12. RECOGNISING the importance of shared situational awareness, coordinated public communication and effective response during large scale cybersecurity incidents and crises.

[15] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19 7 2016, p 1)

Fostering the preparedness and crisis prevention

13. RECALLING the need to prevent cyber incidents and crises by continuing to bolster EU capabilities to address cyber threats.

14. CALLS upon the Member States to ensure that their national crisis management mechanisms adequately address cyber incidents and crisis as well as provide necessary procedures for cooperation at EU level at the technical, operational and political level.

Increasing the situational awareness

15. CALLS upon the EU institutions, agencies and bodies and its Member States to cooperate and contribute to EU level situational awareness both before and during cyber incidents and crises through regular EU Cybersecurity Technical Situation Reports and EU Cybersecurity Operational Situation Reports.

Ensuring the effective response

16. RECOGNISING that crises response can take many forms and requires a coordinated approach at EU level, ranging from identifying technical measures to operational measures as well as political measures, depending on the type of incident or crises.

17. CALLS upon the Member States to identify, develop and implement further means of operational cooperation, including in the CSIRTs Network SOPs, in relation to early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents. In this context it welcomes group of Member States initiative to create Cyber Rapid Response Teams and to deepen voluntary cooperation in cyber field through mutual assistance in response to major cyber incidents.

18. CALLS upon the Member States to identify and put in place a corresponding cooperation protocol and SOPs recognising that cyber incidents have the potential of leading to a cross-sectorial crisis, i.e. impacting simultaneously the functioning of different sectors, infrastructures or services, stressing the need to establish appropriate procedures and concrete measures for timely information sharing and situational awareness at operational level amongst competent authorities, such as the national Single Point of Contacts under the NIS Directive.

19. CALLS upon the Commission to bring forward a legislative proposal for a Cybersecurity Emergency Response Fund.

Streamlining the public communication

20. RECOGNISING that public communication could refer to communication about an incident to the public as a whole, communication of more technical or operational information with critical sectors and/or those who have been affected, as well as could serve as a clear signal of likely consequences of a diplomatic response to influence the behaviour of potential aggressors.

21. CALLS upon the EU institutions and Member States to ensure effective and, where necessary, coordinated communication towards the public, keeping in mind that aligning the public communication to mitigate negative effects of cybersecurity incidents and crises and the public communication to influence a potential aggressor is essential for a diplomatic response to be effective.

Building on the lessons learned and post incident analysis

22. CALLS upon the EU institutions and Member States to promote and share the analysis of operational and strategic aspects of lessons of large cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved.

Developing a European Cybersecurity Crisis Cooperation Framework

23. CALLS upon the Member States and the EU institutions, agencies and bodies to jointly work towards development of European Cybersecurity Crisis Cooperation Framework within the context of EU crisis management mechanisms, in particular the IPCR, taking into account their respective roles, mandates and competences, putting in place the practical operationalisation and documentation of all the relevant actors, mechanism, processes and procedures.

24. CALLS upon the relevant stakeholders to undertake necessary steps to remove any obstacles and/or fill in any gaps identified both in terms of information flows and in terms of interoperability of the procedures and mechanisms as well as to establish links among the mechanisms, processes and procedures where necessary.

CALLS EU Institutions and Member States to regularly test their response to large scale cyber incidents at European and national level.

NETHERLANDS

Draft Council conclusions on EU coordinated response to large scale cybersecurity incidents and crises

The Council of the European Union,

1. RECOGNISING the need for an efficient EU level response to large scale cyber incidents and crises as stressed in the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU of 20 November 2017[16].
2. RECALLING the Council conclusions of 19 June 2017[17] on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox") and the corresponding implementing guidelines of 11 October 2017 as well as the Council conclusions on the Integrated Political Crisis Response arrangements[18].
3. TAKING INTO CONSIDERATION the Commission Recommendation of 13 September 2017[19] on a Coordinated Response to Large-scale Cybersecurity Incidents and Crises and the core objectives and guiding principles set out therein.
4. RECOGNISING the competences of the Member States and their responsibility for national security in the domain of cybersecurity.
5. WELCOMING the adoption of the CSIRTs Network Standard Operating Procedures (SOPs) and the on-going work within the Cooperation Group on a common taxonomy for cybersecurity incidents.

[16] 14435/17
[17] 9916/17
[18] 10708/13
[19] C(2017) 6100 final

6. RECOGNISING the on-going work on the Law Enforcement Emergency Response Protocol, that describes a mechanism for early detection and identification of cyber incidents and crises, eventually leading to an investigation under the normal applicable operating procedures, complementing and aligning a response by the law enforcement community with existing EU crisis response mechanisms.

7. BUILDING on the discussions at the Cybersecurity Challenges Conference in Sofia on 26 March 2018.

8. WELCOMING the Memorandum of Understanding to establish a framework for cooperation signed by ENISA, EC3, CERT-EU and the EDA which will further strengthen their cooperation within their respective mandates, in particular on matters of information exchange, cyber exercises as well as technical cooperation.

9. UNDERLINING the need to make use of the existing crisis management mechanisms, processes and procedures.

10. RECALLING the importance of an effective implementation of the Directive on Security of Network and Information systems[20] and the development of capabilities of national CSIRTs and competent authorities as regards responding to and handling of cybersecurity incidents.

11. RECALLING that activities at Member States and EU level, as well as cross-border cooperation, with regard to cyber incidents and crisis take place following the principles of subsidiarity and proportionality.

12. RECOGNISING the importance of shared situational awareness, coordinated public communication and effective response during large scale cybersecurity incidents and crises.

13. RECOGNISING that large scale crises response can take many forms and may require a coordinated approach at EU level, ranging from identifying technical measures to operational measures as well as political measures, depending on the type of incident or crises.

Commented [T21]: Added to reflect that the blueprint explicitly focuses on large scale incidents and crises, not any incident

Commented [T22]: Not every incident automatically needs a coordinated approach at the EU level, but at national or regional level only

Commented [T23]: This would fit better as a preamble

[20] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19 7 2016, p 1)

Fostering the preparedness and crisis prevention

~~13.~~14. RECALLING the need to prevent cyber incidents and crises by continuing to bolster EU capabilities to address cyber threats.

~~14.~~15. CALLS upon the Member States to ensure that their national crisis management mechanisms adequately address cyber incidents and crisis for response at the national level as well as provide necessary procedures for cooperation at EU level at the technical, operational and political level.

Increasing the situational awareness

~~15.~~16. ~~C~~ALLS upon the EU institutions, agencies and bodies and its Member States to cooperate and contribute to EU level situational awareness both before and during large scale cyber incidents and crises ~~through regular EU Cybersecurity Technical Situation Reports and EU Cybersecurity Operational Situation Reports~~, and to share national threat reports.

Commented [T24]: Added to reflect that the blueprint explicitly focuses on large scale incidents and crises, not any incident

Commented [T25]: Does this reference procedures in place at the CSIRT's Network? Or are these new ideas?

If they are new ideas, they might be too prescriptive for this document

Ensuring the effective response

~~16. RECOGNISING that crises response can take many forms and requires a coordinated approach at EU level, ranging from identifying technical measures to operational measures as well as political measures, depending on the type of incident or crises.~~

Commented [T26]: This would fit better as a preamble

17. CALLS upon the Member States to identify, develop and implement further means of operational cooperation, including in the CSIRTs Network SOPs, in relation to early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents.

18. CALLS upon the Member States to identify and put in place a corresponding cooperation protocol and SOPs recognising that cyber incidents have the potential of leading to a cross-sectorial crisis, i.e. impacting simultaneously the functioning of different sectors, infrastructures or services, stressing the need to establish appropriate procedures and concrete measures for timely information sharing and situational awareness at operational level amongst competent authorities, such as the national Single Point of Contacts under the NIS Directive.

19. ~~CALLS upon the Commission to bring forward a legislative proposal for a Cybersecurity Emergency Response Fund.~~

Commented [T27]: This goes beyond the phrasing in the Council Conclusions agreed upon from November 2017

Para 36 of those conclusion notes only that the Council might examine a Commission proposal As these Council Conclusions are the first to be referenced in this document, NL does not see the need for this particular paragraph

Streamlining the public communication

20. RECOGNISING that public communication could refer to communication about an incident to the public as a whole, communication of more technical or operational information with critical sectors and/or those who have been affected, as well as could serve as a clear signal of likely consequences of a diplomatic response to influence the behaviour of potential aggressors

Commented [T28]: Would work better as a preamble

21. CALLS upon the EU institutions and Member States to ensure effective and, where necessary and possible, coordinated communication towards the public, keeping in mind that aligning the public communication to mitigate negative effects of large scale cybersecurity incidents and crises and ~~the~~ that ~~public~~ communication to influence a potential aggressor is essential for a diplomatic response to be effective.

Commented [T29]: Depending on the sort of crises/incident it may not be possible to wait for coordinated communication to be agreed upon

Crisis communication in any case is a national competence

Commented [T30]: Would this inherently need to be public? A reaction in bilaterale context might also be considered, depending on the specifics of each case

Commented [T31]: This part might work better as a separate clause This now covers two separate topics in one sentence One is public communication towards the EU audience, the other about attribution and communication to possible aggressors

Building on the lessons learned and post incident analysis

22. CALLS upon the EU institutions and Member States to promote and share the analysis of operational and strategic aspects of lessons of large cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved.

Developing a European Cybersecurity Crisis Cooperation Framework

23. CALLS upon the Member States and the EU institutions, agencies and bodies to jointly work towards development of European Cybersecurity Crisis Cooperation Framework within the context of EU crisis management mechanisms, in particular the IPCR, taking into account their respective roles, mandates and competences, putting in place the practical operationalisation and documentation of all the relevant actors, mechanism, processes and procedures.

24. CALLS upon the relevant stakeholders to undertake necessary steps to remove any obstacles and/or fill in any gaps identified both in terms of information flows and in terms of interoperability of the procedures and mechanisms as well as to establish links among the mechanisms, processes and procedures where necessary.

SWEDEN

Draft Council conclusions on EU coordinated response to large scale cybersecurity incidents and crises

The Council of the European Union,

1. RECOGNISING the need for an efficient EU level response to large scale cyber incidents and crises as stressed in the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU of 20 November 2017[21].
2. RECALLING the Council conclusions of 19 June 2017[22] on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox") and the corresponding implementing guidelines of 11 October 2017 as well as the Council conclusions on the Integrated Political Crisis Response arrangements[23].
3. TAKING INTO CONSIDERATION the Commission Recommendation of 13 September 2017[24] on a Coordinated Response to Large-scale Cybersecurity Incidents and Crises and the core objectives and guiding principles set out therein.
4. RECOGNISING the competences of the Member States and their responsibility for national security in the domain of cybersecurity.
5. WELCOMING the adoption of the CSIRTs Network Standard Operating Procedures (SOPs) and the on-going work within the Cooperation Group on a common taxonomy for cybersecurity incidents.
6. RECOGNISING the on-going work on the Law Enforcement Emergency Response Protocol, that describes a mechanism for early detection and identification of cyber incidents and crises, eventually leading to an investigation under the normal applicable operating procedures, complementing and aligning a response by the law enforcement community with existing EU crisis response mechanisms.

[21] 14435/17
[22] 9916/17
[23] 10708/13
[24] C(2017) 6100 final

7. BUILDING on the discussions at the Cybersecurity Challenges Conference in Sofia on 26 March 2018.

Comment to nr 7: What are the official conclusions from the Cybersecurity Challenges Conference in Sofia and do all MS agree on this? If none, perhaps this paragraph should be deleted pr replaced with "RECOGNISING that a Conference on Cybersecurity Challenges was held in Sofia on 26 March 2018."

8. WELCOMING the Memorandum of Understanding to establish a framework for cooperation signed by ENISA, EC3, CERT-EU and the EDA which will further strengthen their cooperation within their respective mandates, in particular on matters of information exchange, cyber exercises as well as technical cooperation.

9. UNDERLINING the need to make use of the existing crisis management mechanisms, processes and procedures.

Comment to nr 9: Please specify which existing crisis management mechanisms, processes and procedures that are in mind.

10. RECALLING the importance of an effective implementation of the Directive on Security of Network and Information systems[25] and the development of capabilities of national CSIRTs and competent authorities as regards responding to and handling of cybersecurity incidents.

11. RECALLING that activities at Member States and EU level, as well as cross-border cooperation, with regard to cyber incidents and crisis take place following the principles of subsidiarity and proportionality.

12. RECOGNISING the importance of shared situational awareness, coordinated public communication and effective response during large scale cybersecurity incidents and crises.

Fostering the preparedness and crisis prevention

13. RECALLING the need to prevent cyber incidents and crises by continuing to bolster EU capabilities to address large scale cyber threats.

[25] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19 7 2016, p 1)

14. CALLS upon the Member States to ensure that their national crisis management mechanisms adequately address cyber incidents and crisis as well as provide necessary procedures for existing cooperation at EU level at the technical, operational and political level.

Comment to nr 14: Sweden believes that the wording isn't clear. What procedures for technical, operational and political level does the wording aim at?

Increasing the situational awareness

15. CALLS upon the EU institutions, agencies and bodies and its Member States to cooperate and contribute to EU level situational awareness both before and during cyber incidents and crises through regular EU Cybersecurity Technical Situation Reports and EU Cybersecurity Operational Situation Reports.

Comment to nr 15: What EU institutions, agencies and bodies and its Member States are in mind? Isn't the idea that this is essentially about CERT collaboration within the CSIRT network?

Ensuring the effective response

16. RECOGNISING that crises response can take many forms and may require~~s~~ a coordinated approach at EU level, ranging from identifying technical measures to operational measures as well as political measures, depending on the type of incident or crises.

17. CALLS upon the Member States to identify, develop and implement further means of existing operational cooperation, including in the CSIRTs Network SOPs, in relation to early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents.

Comment to nr 17: The development of work should focus on existing operational cooperation and to make that more effective. Nothing new is needed.

18. CALLS upon the Member States to identify and put in place a corresponding cooperation protocol and SOPs recognising that cyber incidents have the potential of leading to a large scale cross-sectorial crisis, i.e. impacting simultaneously the functioning of different sectors, infrastructures or services, stressing the need to establish appropriate procedures and concrete measures for timely information sharing and situational awareness at operational level amongst competent authorities, such as the national Single Point of Contacts under the NIS Directive.

19. ~~CALLS upon the Commission to bring forward a legislative proposal for a Cybersecurity Emergency Response Fund.~~

Comment to nr 19: There hasn't been any in depth discussions about proposing a new fund and Sweden therefore want this paragraph to be deleted. In relation to the ongoing negotiations of the EU budget, it isn't the right time to present this kind of proposal since the council conclusions may not anticipate the outcome.

Streamlining the public communication

20. RECOGNISING that public communication could refer to communication about a~~n~~ large scale incident to the public as a whole, communication of more technical or operational information with critical sectors and/or those who have been affected, as well as could serve as a clear signal of likely consequences of a diplomatic response to influence the behaviour of potential aggressors.

21. CALLS upon the EU institutions and Member States to ensure effective and, where necessary, coordinated communication towards the public, keeping in mind that aligning the public communication to mitigate negative effects of large scale cybersecurity incidents and crises and the public communication to influence a potential aggressor is essential for a diplomatic response to be effective.

Building on the lessons learned and post incident analysis

22. CALLS upon the EU institutions and Member States to promote and share the analysis of operational and strategic aspects of lessons of large cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved.

Developing a European Cybersecurity Crisis Cooperation Framework

23. CALLS upon the Member States and the EU institutions, agencies and bodies to jointly work towards development of European Cybersecurity Crisis Cooperation Framework within the context of existing EU crisis management mechanisms, in particular the IPCR, taking into account their respective roles, mandates and competences, putting in place the practical operationalisation and documentation of all the relevant actors, mechanism, processes and procedures.

Comment to nr 23: Nothing new should be developed.

24. CALLS upon the relevant stakeholders to undertake necessary steps to try to remove ~~any~~ obstacles and/or fill in ~~any~~ gaps identified both in terms of information flows and in terms of interoperability of the existing procedures and mechanisms as well as to establish links among the mechanisms, processes and procedures where necessary.

Comment to nr 24: What is meant by the last part of the sentence, "as well as to establish links among the mechanisms, processes and procedures where necessary". This formulation is to vague to know what the intention is.