Conseil de
l'Union européenne

Bruxelles, le 28 mars 2022
(OR. fr)

7502/22

LIMITE

CYBER 94
COPS 136
RELEX 407
JAIEX 27
TELECOM 124
COSI 76
JAI 409
IPCR 41

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents
Objet:	Conclusion de l'exercice de gestion de crise de grande ampleur d'origine Cyber (EU CyCLES)

1. INFORMATIONS GÉNÉRALES SUR L'EXERCICE CYBER

Afin de faire face à la multiplication des activités cyber-malveillantes, se situant essentiellement en dessous du seuil des attaques armées, mais susceptibles d'aller jusqu'à une situation correspondant à une agression armée telle que définie dans la Charte des Nations Unies, il est nécessaire de renforcer la préparation et la capacité de réaction de l'Union européenne aux cyber-incidents de grande envergure.

Par conséquent, la présidence, en coopération avec le Service européen pour l'action extérieure (SEAE) et avec le soutien de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), a organisé un exercice de grande envergure mobilisant un large éventail d'acteurs impliqués dans la réponse de l'Union européenne à de tels incidents.

L'objectif principal de l'exercice EU CyCLES[1] dans son ensemble est de sensibiliser l'échelon politique européen et de renforcer la coopération entre les niveaux technique, opérationnel et politique en cas de cyber-attaque de grande envergure. Dans la première phase de l'exercice, le scénario était axé sur les mécanismes de gestion des crises cyber de l'Union européenne (évaluation de la gravité de la crise, assistance) et sur la réponse politique que l'Union européenne peut apporter dans sa dimension interne.

La deuxième phase de l'exercice a débuté le 9 février 2022 lorsque des informations ont été connues sur l'origine de l'attaque. Elle s'est concentrée sur la dimension externe de la réponse de l'Union européenne, en particulier la réponse de l'Union européenne à l'attaquant. La dernière partie de l'exercice vise à mettre en pratique la réponse de l'Union européenne et de ses États membres à une cyberattaque de grande envergure ayant entraîné des effets cinétiques, des pertes humaines et des dommages matériels.

L'exercice « EU CyCLES » a été joué au COREPER (le 14 janvier et le 9 février), au groupe de travail horizontal sur les questions cyber (GHQC) (le 21 janvier, le 1er février et le 11 février) et au Comité politique et de sécurité (COPS) (le 15 février).

L'exercice devait se conclure lors du Conseil « Affaires étrangères » du 21 février 2022, mais n'a pu être finalisé en raison d'un changement de l'ordre du jour du Conseil lié à l'agression russe contre l'Ukraine.

Le Haut représentant a annoncé lors du Conseil Affaires étrangères du 21 mars que la dernière étape serait jouée au COREPER le 1er avril.

[1] EU Cyber Crisis Linking Exercise on Solidarity

2. PRINCIPAUX ÉLÉMENTS DU SCENARIO

L'exercice a débuté le vendredi 14 janvier 2022 avec la saisine du COREPER, dans le cadre d'un point divers, au sujet d'un cyber incident pouvant avoir des effets transfrontaliers. Par la suite, à la demande du COREPER II, le Groupe Horizontal sur les Questions Cyber a effectué un suivi et fourni une évaluation générale de la gravité et de l'impact de la crise dans l'ensemble de l'Union européenne, notamment par la mobilisation des acteurs concernés afin de fournir une connaissance partagée de la situation[2].

- La crise cyber a rapidement pris de l'ampleur, avec un nouvel État membre touché, des effets sur les secteurs de l'énergie et celui des services de santé ainsi que le risque d'effets transfrontaliers importants et d'une éventuelle saturation des capacités de réaction.
- En coordination avec les deux États membres les plus touchés, la présidence française du Conseil de l'Union européenne a décidé d'activer le mécanisme intégré de réponse aux crises politiques (IPCR) de l'Union européenne en mode 'échange d'informations'. La Commission et le Service européen pour l'action extérieure ont surveillé en permanence le paysage des menaces cyber et fourni des analyses par le biais du rapport intégré de connaissance et d'analyse de la situation (rapport ISAA) et de l'évaluation des renseignements stratégiques faite par le centre de situation et de renseignement de l'Union européenne (INTCEN).
- Sur la base de ces rapports de connaissance situationnelle, le Groupe Horizontal sur les Questions Cyber puis le COPS ont discuté (11 février et 15 février) des éléments d'une note d'options du Service européen pour l'action extérieure (SEAE) présentant les mesures diplomatiques possibles, dans le cadre de la boîte à outils cyber diplomatique, pour répondre à l'attaque et à l'Etat (fictif) dont elle émane.

[2] Le réseau des CSIRTs et le réseau de coopération opérationnelle en cas de crise cyber (CyCLONe).

- La cyber-attaque s'est intensifiée et a entraîné des pertes humaines et matérielles. Ces conséquences ont amené un État membre ciblé à invoquer l'article 42.7 du TUE le 16 février 2022.
- La Présidence a activé l'IPCR en mode plein. Une réunion extraordinaire des ministres de l'intérieur a été convoquée par la présidence pour faire face aux conséquences en termes de gestion civile de la crise (simulée).
- Sur la base des derniers événements et de l'invocation de l'article 42.7 TUE, le Haut représentant a convoqué une réunion extraordinaire des ministres des Affaires étrangères (simulée le 21 février 2022) pour traiter de la dimension extérieure de la cyber-attaque.
- Au cours de cette réunion, la Finlande a présenté dans les grandes lignes sa demande d'assistance au titre de l'article 42.7 TUE. Le Haut représentant a souligné l'obligation pour les États membres de fournir une assistance par tous les moyens nécessaires et a indiqué, à la suite de la demande de la Finlande, la disponibilité du Service européen pour l'action extérieure de soutenir l'État membre victime. Les États membres ont approuvé une déclaration attribuant la cyber-attaque à l'État du Blueland.
- Les ministres ont ensuite chargé le COREPER de faire le suivi de la réunion.

3. **DÉROULÉ DE LA DISCUSSION AU COREPER**

La discussion au COREPER est supposée se tenir immédiatement après la réunion des Affaires étrangères du 21 février.

La Présidence introduira la discussion et rappellera brièvement le déroulement de l'exercice, sur la base du scénario.

La Finlande, l'Etat membre attaqué, rappellera sa lettre du 16 février 2022 au Haut Représentant dans laquelle elle invoquait l'article 42(7) TUE et la demande d'aide et d'assistance bilatérale faite aux Etats membres lors de la réunion des ministres du 21 février.

Le Service européen pour l'action extérieure rappellera la déclaration du Haut Représentant au nom de l'Union européenne attribuant la cyberattaque à l'État du Blueland. Il présentera les options de mesures diplomatiques supplémentaires, dans le cadre de la boîte à outils cyber diplomatique. Il exprimera la disponibilité du Service européen pour l'action extérieure, sur la base d'une demande explicite de l'État membre attaqué, àoffrir son assistance, en tant que centre d'échange pour la coordination du soutien de l'UE à la Finlande.

La Commission interviendra sur la mobilisation de ses outils et proposera sa contribution.

La Présidence invitera les Etats membres à explorer toute la gamme des mesures en réponse à la cyber-attaque attribuée au Blueland, sur la base des questions d'orientation (voir ci-dessous).

Les interventions des États membres sont censées se concentrer sur les mesures prises par les États membres pour soutenir l'État membre victime dans le contexte de l'activation de l'article 42.7 TUE (« en réponse à l'invocation de l'article 42.7 TUE, nous pourrions offrir (...) afin de soutenir l'État membre attaqué »).

À la suite de cet exercice, la présidence française, le SEAE et l'ENISA prépareront un « rapport après action » présentant les enseignements tirés de l'exercice depuis son commencement.

4. QUESTIONS POUR GUIDER LA DISCUSSION

1. Suite à l'invocation par la Finlande de l'article 42(7) du TUE, quelles mesures spécifiques d'aide et d'assistance votre pays serait-il en mesure d'offrir ?

2. Suite à l'attribution publique de l'attaque à l'État du Blueland, quelles mesures diplomatiques supplémentaires et quels autres instruments de l'Union européenne, par exemple ceux de la Commission, pourraient être mobilisés en parallèle, selon leurs procédures respectives ?