Conseil de
l'Union européenne

Bruxelles, le 19 juin 2017
(OR. en)

10474/17

CYBER 98
RELEX 554
POLMIL 77
CFSP/PESC 557

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	19 juin 2017
Destinataire:	délégations
Nº doc. préc.:	9916/17
Objet:	Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique"), 19 juin 2017

Les délégations trouveront en annexe les conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique"), adoptées par le Conseil des affaires étrangères lors de sa 3551e session tenue le 19 juin 2017.

ANNEXE

CONCLUSIONS DU CONSEIL RELATIVES À UN CADRE POUR UNE RÉPONSE DIPLOMATIQUE CONJOINTE DE L'UE FACE AUX ACTES DE CYBERMALVEILLANCE ("BOÎTE À OUTILS CYBERDIPLOMATIQUE")

Le Conseil de l'Union européenne a adopté les conclusions suivantes:

1. L'UE est consciente que le cyberespace offre des possibilités considérables, mais qu'il présente aussi des défis en constante évolution pour les politiques externes de l'UE, notamment la politique étrangère et de sécurité commune, et souligne qu'il est de plus en plus nécessaire de protéger l'intégrité et la sécurité de l'UE, de ses États membres et de leurs citoyens contre les menaces informatiques et les actes de cybermalveillance.

L'UE rappelle ses conclusions concernant la stratégie de cybersécurité de l'Union européenne[1], en particulier sa détermination à maintenir un cyberespace ouvert, libre, stable et sûr, où les droits fondamentaux et l'État de droit s'appliquent pleinement. Elle rappelle également ses conclusions sur la cyberdiplomatie[2], notamment le fait qu'une approche commune et globale de l'UE en matière de cyberdiplomatie est susceptible de contribuer à la prévention des conflits, à la réduction des menaces qui pèsent sur la cybersécurité et à une stabilité accrue des relations internationales.

L'UE et ses États membres soulignent l'importance dun rôle actuel de l'UE en matière de cyberdiplomatie et de la nécessité d'assurer la cohérence entre ses différentes initiatives dans le domaine du cyberespace, afin de renforcer efficacement la cyber-résilience; ils sont encouragés à intensifier davantage leurs efforts en ce qui concerne les cyberdialogues dans le cadre d'une coordination politique effective et soulignent l'importance du renforcement des cybercapacités dans les pays tiers.

2. L'UE est préoccupée par la capacité et la volonté accrues d'acteurs étatiques et non étatiques à poursuivre leurs objectifs en menant des activités cybermalveillantes, dont la portée, l'échelle, la durée, l'intensité, la complexité, la sophistication et l'incidence sont variables.

---

1 Doc. 12109/13.
2 Doc. 6122/15.

L'UE souligne que les activités cybermalveillantes sont susceptibles de constituer des actes illicites au regard du droit international et rappelle que les États ne devraient pas mener ou soutenir sciemment des activités informatiques contraires aux obligations qu'ils leur incombent en vertu du droit international, et qu'ils ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications, comme indiqué dans le rapport de 2015 du groupe d'experts gouvernementaux des Nations unies.

3. L'UE rappelle ses efforts ainsi que ceux de ses États membres visant à améliorer la cyber-résilience, notamment grâce à la mise en œuvre de la directive SRI et aux mécanismes de coopération opérationnelle qu'elle prévoit, et rappelle que les activités cybermalveillantes dirigées contre des systèmesd'information, tels qu'ils sont définis par le droit de l'Union, constituent une infraction pénale et que la réalisation d'enquêtes et l'engagement de poursuites effectives à l'égard de telles infractions restent un effort commun des États membres.

L'UE et ses États membres prennent note des travaux menés actuellement par le groupe d'experts gouvernementaux des Nations unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, sur la base des rapports[3] de 2010, 2013 et 2015, et sont encouragés à soutenir résolument le consensus selon lequel le droit international en vigueur s'applique au cyberespace. L'UE et ses États membres ont la ferme volonté de soutenir activement l'élaboration de normes volontaires et non contraignantes de comportement responsable des États dans le cyberespace, ainsi que les mesures de confiance régionales adoptées par l'OSCE[4] visant à réduire les risques de conflits découlant de l'utilisation des technologies de l'information et des communications.

L'UE réaffirme qu'elle est attachée au règlement des différends internationaux dans le cyberespace par des moyens pacifiques, et que l'ensemble des efforts diplomatiques déployés par l'UE devraient en priorité être axés sur la promotion de la sécurité et de la stabilité dans le cyberespace au moyen d'une coopération internationale renforcée, ainsi que sur la réduction du risque de perceptions erronées, d'escalade et de conflits qui peuvent découler d'incidents liés aux TIC. À cet égard, l'UE rappelle que l'Assemblée générale des Nations unies a invité les États membres de l'ONU à s'inspirer des recommandations figurant dans les rapports des groupes d'experts gouvernementaux des Nations unies en ce qui concerne l'utilisation qu'ils font des TIC.

---

[3] A/68/98 et A/70/174.

[4] PC.DEC/1106 du 3 décembre 2013 et PC.DEC/1202 du 10 mars 2016.

4. L'UE souligne que le fait de signaler clairement les conséquences possibles d'une réponse diplomatique conjointe de l'UE face à de telles activités cybermalveillantes influence le comportement des cyberagresseurs potentiels, renforçant ainsi la sécurité de l'UE et de ses États membres. L'UE rappelle que l'attribution d'un acte à un acteur étatique ou non étatique reste une décision politique souveraine basée sur des renseignements de toutes sources et qu'elle devrait être établie en conformité avec le droit international relatif à la responsabilité des États. À cet égard, l'UE souligne que toutes les mesures relatives à une réponse diplomatique conjointe de l'UE face à des activités cybermalveillantes ne nécessitent pas une attribution à un acteur étatique ou non étatique.

5. L'UE souligne que les mesures relevant de la politique étrangère et de sécurité commune, y compris, si nécessaire, les mesures restrictives, adoptées dans le cadre des dispositions pertinentes des traités, conviennent à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance et qu'elles devraient encourager la coopération, faciliter la réduction des menaces immédiates et à long terme, et influencer le comportement d'agresseurs potentiels à long terme. L'UE travaillera à l'élaboration d'un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance, en s'appuyant sur les grands principes suivants:

- servir à protéger l'intégrité et la sécurité de l'UE, de ses États membres et de leurs citoyens,
- tenir compte du contexte plus large des relations extérieures de l'Union avec l'État concerné,
- permettre la réalisation des objectifs de la PESC tels qu'ils sont énoncés dans le traité sur l'Union européenne (TUE) et les procédures respectives prévues pour leur réalisation,
- reposer sur une appréciation commune de la situation entre les États membres et correspondre aux besoins de la situation concrète en présence,
- être proportionné à la portée, l'échelle, la durée, l'intensité, la complexité, la sophistication et l'incidence de la cyberactivité,
- respecter le droit international applicable et ne pas violer les droits et libertés fondamentaux.

6. L'UE invite les États membres, le Service européen pour l'action extérieure (SEAE) et la Commission à donner pleinement effet à l'élaboration d'un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance et réaffirme à cet égard sa volonté de poursuivre les travaux relatifs à ce cadre, en coopération avec la Commission, le SEAE et d'autres parties intéressées, en mettant en place des lignes directrices relatives à la mise en œuvre, y compris les procédures préparatoires et de communication, et de les tester au moyen d'exercices appropriés.