Conseil de
l'Union européenne

Bruxelles, le 15 décembre 2020
(OR. en)

14064/20

HYBRID 47	**EDUC 444**
DISINFO 48	**AUDIO 63**
AG 70	**DIGIT 153**
PE 106	**INF 223**
DATAPROTECT 152	**COSI 251**
JAI 1112	**CSDP/PSDC 643**
CYBER 279	**COPS 480**
JAIEX 120	**POLMIL 199**
FREMP 147	**IPCR 50**
RELEX 1010	**PROCIV 97**
CULT 89	**CSC 362**

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Nº doc. préc.:	13626/20
Objet:	Conclusions du Conseil sur le renforcement de la résilience et la lutte contre les menaces hybrides, y compris la désinformation, dans le contexte de la pandémie de COVID-19

Les délégations trouveront en annexe les conclusions du Conseil visées en objet, approuvées par le Conseil par voie de procédure écrite le 15 décembre 2020.

ANNEXE

Projet de conclusions du Conseil sur le renforcement de la résilience et la lutte contre les menaces hybrides, y compris la désinformation, dans le contexte de la pandémie de COVID-19

1. Le Conseil rappelle les conclusions pertinentes du Conseil européen[1] et du Conseil[2], et note que la pandémie de COVID-19 met en exergue la nécessité d'intensifier les efforts et les initiatives en cours pour protéger l'Union européenne, ses États membres et leurs sociétés, ainsi que les institutions de l'UE, contre les menaces hybrides et leurs effets néfastes. Sans préjudice de la responsabilité exclusive des États membres en matière de sécurité nationale, le Conseil note ce qui suit:
   - les menaces hybrides représentent un défi croissant pour la sécurité, la stabilité ainsi que les valeurs et principes communs de l'UE;
   - des acteurs étatiques et non étatiques hostiles ont pour objectif de déployer et d'utiliser des outils moins conventionnels afin de perturber, de saper ou de délégitimer les démocraties et les institutions démocratiques, d'interférer dans les processus électoraux, de diviser les populations ou, de manière générale, d'étendre leur influence clandestine;
   - les nouvelles technologies et les crises telles que la pandémie actuelle offrent à des acteurs hostiles l'occasion d'étendre leurs activités d'ingérence, ce qui constitue un défi supplémentaire pour les États membres et les institutions de l'UE, outre la crise elle-même.

2. Nous devons protéger nos sociétés et nos institutions démocratiques des [...] menaces hybrides qui sont le fait d'acteurs étatiques et non étatiques hostiles. Pour lutter contre ces menaces, y compris les actes de cybermalveillance, la désinformation et les menaces qui pèsent sur la sécurité économique, il est nécessaire d'adopter une approche globale assortie d'une coopération et d'une coordination efficaces.

---

[1] En particulier les conclusions du Conseil européen de juin 2019, mars 2019, décembre 2018, octobre 2018, juin 2018, mars 2018, juin 2015 et mars 2015.

[2] En particulier les documents ST 14972/19, ST 10048/19, ST 6573/1/19 REV 1, ST 10255/19, ST 12836/19 et ST 7928/16.

Au niveau de l'UE, il s'agirait de disposer d'une capacité d'analyse autonome et de capacités technologiques renforcées et de mettre l'accent en priorité sur les ressources financières et humaines et leur redistribution. Le Conseil mesure les progrès accomplis dans la mise en œuvre du cadre commun en matière de lutte contre les menaces hybrides et de la communication conjointe intitulée "Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides", ainsi qu'en ce qui concerne le plan d'action contre la désinformation, la communication conjointe consacrée à la désinformation concernant la COVID-19 et le train de mesures visant à garantir des élections européennes libres et équitables, conformément aux conclusions pertinentes du Conseil et du Conseil européen. Le Conseil invite toutes les parties prenantes concernées à redoubler d'efforts et à soutenir la réalisation des objectifs définis dans les documents susmentionnés.

3. Le Conseil constate que la pandémie de COVID-19 rend l'UE et ses États membres plus vulnérables aux menaces hybrides, notamment dans le cadre de l'intensification de la diffusion de la désinformation et des interventions manipulatrices. Les tentatives sont de plus en plus sophistiquées et de plus en plus nombreuses. Le Conseil note que l'approche adoptée par l'UE pour lutter contre la désinformation est multidisciplinaire et multipartite. Le Conseil invite la Commission et le haut représentant à:
   - renforcer encore les réponses apportées au niveau de l'UE, en tenant compte des dommages économiques et sociétaux, ainsi que de l'éventuel préjudice pour la santé publique, causés par la désinformation et l'utilisation malveillante des technologies émergentes, y compris, sans s'y limiter, l'intelligence artificielle;
   - mettre au point une approche globale, systématique et proactive pour lutter contre ces phénomènes, en particulier en prenant acte du fait que, dans le contexte des menaces hybrides, les ingérences étrangères représentent un défi transsectoriel, dont il convient de tenir compte dans les efforts déployés par l'UE et les États pour s'y attaquer, qu'il s'agisse de mesures préventives, de la détection, de la qualification et de l'identification des sources ou de réactions politiques appropriées et efficaces susceptibles d'imposer des coûts aux acteurs étrangers étatiques et non étatiques hostiles en renforçant la résilience des sociétés, en protégeant l'intégrité du débat public et par d'autres moyens.

À cette fin, le Conseil souligne qu'il importe d'allouer des ressources suffisantes aux institutions compétentes de l'UE et demande instamment à la Commission et au haut représentant, conjointement avec les États membres, de continuer à renforcer les task forces de la division Communication stratégique du SEAE et à développer le système d'alerte rapide en vue de mettre en place une plateforme globale pour les États membres et les institutions de l'UE. En outre et conformément à ses conclusions de décembre 2019, le Conseil invite le haut représentant à évaluer les besoins et les possibilités pour ce qui est du renforcement de ses activités de communication stratégique dans toutes les autres zones géographiques, d'une manière équilibrée, et à tenir compte des acteurs hybrides émergents, qui exercent des activités visant à menacer la sécurité de l'UE et/ou de ses États membres, tout en conservant les capacités nécessaires pour mener à bien les tâches de communication stratégique existantes.

4. Le Conseil salue l'évaluation de la mise en œuvre et de l'efficacité du code de bonnes pratiques contre la désinformation[3]. Il prend acte des progrès accomplis et souligne qu'il importe de remédier aux lacunes du code de bonnes pratiques que cette évaluation a mises en lumière. Il estime que la voie à suivre en matière de lutte contre la désinformation aux niveaux national et de l'UE pourrait englober une série d'approches, dont la possibilité de disposer d'un cadre de régulation ou de corégulation et des moyens nécessaires à un contrôle indépendant, effectué à la fois par des organismes de régulation et par la société civile, notamment en ce qui concerne l'accès aux données. Sur cette base, le Conseil invite la Commission à élaborer et, à terme, à mettre en œuvre de nouvelles exigences en matière de transparence applicables aux plateformes en ligne. Ces exigences viseraient à promouvoir une sphère publique numérique opérationnelle, une responsabilisation renforcée et une transparence accrue dans la lutte contre la désinformation. Ces mesures devraient s'appuyer sur la primauté des droits fondamentaux, notamment la liberté d'expression, ainsi que sur un débat public démocratique. Le Conseil se félicite du lancement, en juin 2020, de l'Observatoire européen des médias numériques et insiste sur la nécessité de prendre de nouvelles mesures à l'appui de l'éducation aux médias et de l'habileté numérique pour toutes les classes d'âge, ainsi que sur la nécessité du pluralisme des médias, de l'indépendance des médias et de la vérification des faits, l'objectif étant de donner à nos sociétés les moyens de lutter contre la désinformation et d'autres risques créés et amplifiés par les nouvelles technologies.

---

[3] Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement (Évaluation du code de bonnes pratiques contre la désinformation - Résultats obtenus et domaines dans lesquels des améliorations sont possibles), 10 septembre 2020.

5. Le Conseil prend acte du plan d'action pour la démocratie européenne de la Commission, procédera à un examen approfondi de son contenu et reviendra sur cette question dans les mois à venir.

6. La lutte contre les menaces hybrides requiert une appréciation approfondie de la situation (notamment la capacité à détecter, identifier et analyser ces menaces, y compris leur source), le renforcement de la résilience ainsi que des mesures visant à combattre ces menaces. Cela nécessitera des actions aux niveaux national, européen et international, en coopération avec les partenaires, notamment le secteur privé et les propriétaires et opérateurs d'infrastructures et de services critiques.
   Le Conseil prend note des travaux menés par la Commission, conjointement avec le centre d'excellence européen pour la lutte contre les menaces hybrides, sur le thème suivant: "Tour d'horizon des menaces hybrides: modèle conceptuel"[4]. Il estime que la conceptualisation des menaces hybrides et de la terminologie correspondante est importante pour identifier ces menaces en vue d'améliorer la cohérence entre les mesures européennes et nationales de manière à renforcer la résilience et à lutter contre les menaces hybrides de manière plus efficace et rationnelle. Le Conseil invite la Commission et le haut représentant à poursuivre leurs travaux et à mettre au point le modèle conceptuel, en s'appuyant sur les orientations stratégiques et conformément à la mise à jour de l'action n° 1 du cadre commun de 2016, afin d'en faire un cadre de réponses, de mesures de résilience et d'indicateurs de résilience connexes, fondé sur des études de cas.
   Par ailleurs, ce modèle pourrait servir d'instrument d'orientation en vue de l'élaboration d'initiatives futures concernant les menaces hybrides au niveau européen, et les États membres pourraient en tenir compte lorsqu'ils mettent au point leurs structures et initiatives nationales. Ces travaux pourraient également contribuer à l'analyse de réponses globales et coordonnées aux actions hybrides, selon le cas, aux niveaux national et de l'UE, compte tenu de tout l'éventail d'instruments disponibles.

[4] Giannopoulos, G., Smith, H., Theocharidou, M., "The Landscape of Hybrid Threats: A conceptual model" (Tour d'horizon des menaces hybrides: modèle conceptuel), Commission européenne, Ispra, 2020, PUBSY n° 117280.

7. Le Conseil prend note de la stratégie de l'UE sur l'union de la sécurité présentée par la Commission en 2020, qui prévoit le développement d'une approche nouvelle et plus proactive de la lutte contre les menaces hybrides. Il observe les efforts actuellement déployés en ce qui concerne la création d'une plateforme en ligne restreinte sur laquelle les États membres indiqueront les outils et mesures de lutte utilisés contre les menaces hybrides à l'échelle de l'UE. Il approuve l'accent mis sur l'intégration des considérations hybrides dans l'élaboration des politiques, soulignant en outre la nécessité de suivre des approches qui soient globales et pangouvernementales au niveau national et de l'UE. Dans ce contexte, il invite la Commission et le haut représentant à jouer un rôle actif pour remédier aux défaillances paneuropéennes, y compris en ce qui concerne la sécurité et la résilience des chaînes d'approvisionnement dans le cadre de la sécurité économique, et à présenter des initiatives visant à renforcer la résilience et à améliorer les réponses, s'il y a lieu, en tenant dûment compte des technologies émergentes.

8. Le Conseil rappelle que, s'appuyant sur l'analyse des menaces et d'autres éventuelles contributions thématiques, les orientations stratégiques définiront des lignes directrices ainsi que des buts et des objectifs spécifiques dans le domaine de la sécurité et de la défense, y compris en ce qui concerne le renforcement de la résilience et la lutte contre les menaces hybrides.

9. Le Conseil prend note du fait que la stratégie de l'UE sur l'union de la sécurité reconnaît la cellule de fusion contre les menaces hybrides du Centre de situation et du renseignement de l'UE (INTCEN) comme point focal pour l'évaluation des menaces hybrides. Il invite le haut représentant, conjointement avec la Commission, à élaborer des initiatives sur la manière dont la cellule de fusion contre les menaces hybrides pourrait contribuer, dans le cadre de son mandat, à intégrer les flux d'informations, à renforcer la capacité d'analyse autonome de l'UE et à améliorer l'appréciation de la situation dans tous les domaines liés aux menaces hybrides. Cela concerne notamment les contributions volontaires des États membres et celles des institutions, organes et organismes de l'UE couvrant les menaces hybrides. Le Conseil réaffirme sa position[5] visant à renforcer encore les travaux de la cellule de fusion contre les menaces hybrides et demande que celle-ci soit dotée de ressources humaines et de financements supplémentaires, sans préjudice des besoins dans d'autres domaines d'action de l'INTCEN.

---

[5] Conclusions du Conseil sur les efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides (document ST 14972/19).

De plus, il appelle au développement d'une capacité d'analyse des tendances hybrides tournée vers l'avenir afin d'analyser les menaces hybrides, en mettant fortement l'accent sur les menaces existantes, tout en tenant compte des acteurs hybrides émergents et de leurs activités malveillantes, y compris lorsqu'ils ciblent des infrastructures critiques et utilisent les nouvelles technologies.

10. Chacune des crises actuelles souligne la nécessité de disposer d'infrastructures d'information sûres et résilientes entre les institutions, organes et organismes européens et en leur sein, y compris en matière de communication sécurisée pour les États membres au sein du Conseil et d'échange électronique rapide d'informations classifiées. Le Conseil invite les institutions, organes et organismes de l'UE à renforcer encore leur sécurité et leur résilience. Dans le droit fil de précédentes conclusions du Conseil et conformément au mandat confié par le Conseil européen de juin 2019, il les encourage vivement à œuvrer ensemble, avec le soutien des États membres, à la poursuite du renforcement de leur culture de sécurité et de la protection du personnel, des réseaux d'information et de communication et des processus décisionnels de l'UE.

11. En complément du renforcement de la résilience, qui demeure l'une des tâches les plus importantes et est au cœur des efforts européens de lutte contre les menaces hybrides, l'engagement et les mesures diplomatiques constituent un autre outil européen efficace. Le Conseil étudiera plus en détail, au cours des mois à venir, des réponses possibles dans le domaine des menaces hybrides, qui pourraient couvrir des mesures de prévention et l'imposition de coûts à des acteurs étatiques et non étatiques hostiles.

12. Le Conseil note que les actes de cybermalveillance constituent souvent un élément essentiel des menaces hybrides et prend acte de la poursuite de la mise en œuvre de la boîte à outils cyberdiplomatique de l'UE, y voyant une étape importante pour prévenir, empêcher et décourager ces actes et y réagir, y compris en ce qui concerne ceux qui relèvent d'une campagne hybride.

13. Le Conseil insiste sur la nécessité d'aider le voisinage de l'UE et les Balkans occidentaux[6] à renforcer leur résilience à l'égard de la désinformation et des ingérences étrangères.

14. Le Conseil met l'accent sur la nécessité de coopérer, s'il y a lieu, avec des partenaires partageant les mêmes valeurs et principes européens afin de continuer à élaborer des mesures efficaces pour lutter contre les ingérences étrangères et la désinformation.

15. Le Conseil souligne également l'importance que revêt la mise en œuvre effective des deux déclarations communes sur la coopération UE-OTAN et de l'ensemble commun de propositions, dans le plein respect des principes de transparence, de réciprocité, d'inclusion et d'autonomie décisionnelle des deux organisations ainsi que de leurs procédures décisionnelles, et réaffirme, dans ce cadre, la nécessité d'une coopération renforcée, synergique et bénéfique, y compris pour lutter contre les menaces hybrides et la désinformation. Il appelle à une approbation et à une mise en œuvre rapides du plan PACE pour 2022-2023 et, dans ce contexte, réaffirme la nécessité d'une approche plus ambitieuse afin de renforcer la résilience et d'approfondir les synergies entre les deux organisations, nouvelle étape sur la voie d'une interaction plus étroite entre elles dans des situations de crise réelle. Il salue également la précieuse contribution apportée par le centre d'excellence européen pour la lutte contre les menaces hybrides, situé à Helsinki, et l'encourage à coopérer avec les centres d'excellence compétents de l'OTAN.

16. Le Conseil met également en avant l'importance de la contribution constante qu'apportent les missions et opérations de la PSDC, conformément à leurs mandats, en matière de lutte contre les menaces hybrides, y compris la désinformation, et insiste sur l'utilité de poursuivre la réflexion sur la manière dont ces missions et opérations pourraient répondre aux menaces hybrides, notamment en renforçant leur propre résilience, ainsi qu'en accordant un soutien aux États d'accueil dans ce domaine, s'il y a lieu.

---

[6] Déclaration de Zagreb du 6 mai 2020: https://www.consilium.europa.eu/media/43780/zagreb-declaration-fr-06052020.pdf.