Conseil de
l'Union européenne

Bruxelles, le 10 décembre 2019
(OR. en)

14972/19

HYBRID 56	**EDUC 478**
DISINFO 18	**AUDIO 118**
AG 68	**DIGIT 179**
PE 257	**INF 332**
DATAPROTECT 300	**COSI 252**
JAI 1307	**CSDP/PSDC 575**
CYBER 328	**COPS 360**
JAIEX 177	**POLMIL 129**
FREMP 176	**IPCR 23**
RELEX 1147	**PROCIV 100**
CULT 141	**CSC 294**

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Objet:	Efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides - Conclusions du Conseil (10 décembre 2019)

Les délégations trouveront ci-joint les conclusions du Conseil sur les efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides, adoptées lors de la 3739e session du Conseil le 10 décembre 2019.

ANNEXE

Conclusions du Conseil sur les efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides

1. Le Conseil rappelle les conclusions pertinentes du Conseil européen[1] et du Conseil[2] et affirme qu'il reste déterminé à renforcer la résilience de l'Union et de ses États membres à l'égard des menaces hybrides à caractère multiforme et évolutif et à intensifier la coopération mise en œuvre pour les détecter, les prévenir et les combattre.

2. Le Conseil mesure les progrès accomplis dans la mise en œuvre du cadre commun en matière de lutte contre les menaces hybrides (2016) et de la communication conjointe intitulée "Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides" (2018), ainsi que du plan d'action contre la désinformation (2018), conformément aux conclusions pertinentes du Conseil.

3. La responsabilité de la lutte contre les menaces hybrides incombe au premier chef aux États membres. Les efforts déployés au niveau de l'UE sont complémentaires par nature et n'affectent en rien la responsabilité exclusive qui incombe aux États membres à l'égard des questions de sécurité nationale. Pour répondre aux menaces hybrides, il est nécessaire d'adopter une approche de la sécurité qui soit globale et pangouvernementale et qui associe l'ensemble de la société, en travaillant de manière plus stratégique, coordonnée et cohérente dans l'ensemble des domaines d'action pertinents. Il est important qu'une approche pangouvernementale soit également suivie et appliquée au niveau de l'UE.

4. Dans les présentes conclusions, le Conseil fixe des priorités concernant la protection de nos sociétés, de nos citoyens, de nos libertés et de la sécurité de notre Union contre les menaces hybrides dans le contexte de la mise en œuvre du nouveau programme stratégique pour 2019-2024, en favorisant une approche globale de la sécurité fondée sur davantage de coordination, de ressources et de capacités technologiques, sur la base du travail considérable déjà réalisé dans différents domaines d'action, y compris dans le cadre de la coopération en matière de sécurité et de défense au niveau de l'UE.

---

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 10048/19, ST 6573/1/19 REV 1, ST 10255/19, ST 12836/19 et ST 7928/16.

5. Les efforts visant à protéger nos institutions démocratiques contre les menaces hybrides doivent toujours respecter les droits fondamentaux, y compris la protection des données à caractère personnel, la liberté d'expression et d'information et la liberté d'association, tels qu'ils sont inscrits dans la Charte des droits fondamentaux.

6. L'UE et ses États membres devraient continuer à développer, perfectionner et exercer leurs capacités à détecter les activités hybrides, à en analyser les sources et à y répondre, et appuyer le renforcement de la résilience des États membres et des institutions, organes et agences de l'UE à l'égard des menaces hybrides en agissant à long terme, en tirant pleinement parti des instruments existants qui sont adaptés à cet objectif. Le Conseil insiste sur la nécessité de mettre à jour le protocole opérationnel de l'UE de lutte contre les menaces hybrides, sur la base des enseignements tirés des exercices précédents.

7. Le Conseil souligne qu'il demeure nécessaire de coopérer avec des organisations internationales telles que l'ONU, l'OSCE et le Conseil de l'Europe et des configurations telles que le G7 afin de défendre l'ordre mondial fondé sur des règles, notamment dans le contexte de la lutte contre les menaces hybrides, y compris par des mesures de confiance et d'autres mesures pertinentes.

8. En matière de renforcement de la résilience et de la lutte contre les menaces hybrides, le Conseil souligne la détermination de l'UE à poursuivre une coopération étroite et mutuellement profitable avec tous les pays partenaires concernés, en particulier ceux du voisinage de l'UE, et à poursuivre son soutien à ces pays.

9. Le Conseil demande que des efforts constants et soutenus soient déployés pour faire encore progresser la mise en œuvre de toutes les actions liées à la lutte contre les menaces hybrides dans le cadre de l'ensemble commun de propositions pour la mise en œuvre des déclarations conjointes sur la coopération entre l'UE et l'OTAN, notamment en ce qui concerne l'appréciation de la situation, la communication stratégique, la prévention et la gestion des crises, ainsi que le renforcement de la résilience. Dans ce contexte, il réaffirme la nécessité d'intensifier le dialogue politique sur la lutte contre les menaces hybrides et de mener régulièrement des exercices parallèles et coordonnés (PACE), avec la participation de l'ensemble des États membres de l'UE et des Alliés de l'OTAN, et il demande que le nouveau plan PACE soit rapidement finalisé. Le Conseil met l'accent sur la nécessité de prendre en compte les enseignements tirés et souligne l'importance que revêt un échange d'informations sans entraves, inclusif et non discriminatoire.

Le Conseil souligne 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. Il se félicite en outre des échanges interservices réguliers et structurés, y compris de la coopération entre la Cellule de fusion de l'UE contre les menaces hybrides du Centre de situation et du renseignement de l'UE (INTCEN) et la Branche "Analyse des menaces hybrides" de l'OTAN.

10. Le Conseil prend acte des efforts déployés par les États membres, en coopération avec la Commission et le Service européen pour l'action extérieure (SEAE), pour mener l'étude sur les risques hybrides prévue dans l'action n° 1 du cadre commun en matière de lutte contre les menaces hybrides (2016) et préconise la poursuite des travaux et l'éventuelle révision de l'étude sur les risques hybrides en vue de mieux remédier aux défaillances.

Travailler de manière cohérente pour renforcer la résilience et lutter contre les menaces hybrides

11. Lors du développement et de l'utilisation de technologies nouvelles et émergentes, y compris l'intelligence artificielle et les techniques de collecte de données, il convient de prendre dûment en considération les nouvelles possibilités en matière de renforcement de la résilience, ainsi que les vulnérabilités potentielles et les effets en cascade dans le contexte de la lutte contre les menaces hybrides, afin de réduire les risques globaux, y compris dans le cadre du processus de planification stratégique du programme-cadre pour la recherche et l'innovation.

12. Le Conseil note que les actes de cybermalveillance peuvent faire partie des menaces hybrides et, dans ce contexte, souligne la pertinence de la boîte à outils cyberdiplomatique de l'UE.

13. La relation entre menaces hybrides et sécurité économique est un élément pertinent qu'il convient de prendre en compte et qui continue de relever, en premier lieu, de la responsabilité des États membres.

14. De nouveaux instruments, tels que le mécanisme prévu par le règlement de l'UE sur le filtrage des investissements directs étrangers, devraient être utilisés de manière efficace pour renforcer la résilience et lutter contre les menaces hybrides en fournissant les moyens d'identifier et de traiter les investissements directs étrangers susceptibles de porter atteinte à la sécurité ou à l'ordre public.

15. Le Conseil invite la Commission à tenir compte de la résilience face aux menaces hybrides dans le processus d'analyse d'impact des futures propositions législatives pertinentes, y compris en ce qui concerne les futurs programmes-cadres pour la recherche et l'innovation.

16. Le Conseil souligne l'importance que revêt la tenue régulière d'exercices et de discussions fondées sur des scénarios en ce qui concerne la lutte contre les menaces hybrides au niveau ministériel et à d'autres niveaux, ainsi que l'incorporation d'éléments hybrides dans d'autres formations et exercice pertinents de l'UE à tous les niveaux, avec le soutien des États membres et des organes compétents, en particulier le centre d'excellence européen pour la lutte contre les menaces hybrides, le cas échéant.

17. Afin d'assurer la cohérence des prochaines étapes de la coopération menée au sein de l'UE en matière de renforcement de la résilience et de lutte contre les menaces hybrides, le Conseil invite la Commission et le haut représentant à établir une cartographie qui tiendrait compte des mesures prises jusqu'à présent et des documents pertinents adoptés de manière globale, en vue d'éventuelles initiatives nouvelles.

Interdépendance entre sécurité intérieure et sécurité extérieure

18. Les services répressifs, la protection civile et les autres autorités concernées devraient continuer à améliorer leur niveau de préparation en vue de prévenir les menaces hybrides et d'y faire face. La coopération entre les autorités nationales concernées, ainsi que les institutions, organes et organismes de l'UE, sur la base de leurs mandats respectifs, sur tous les aspects de l'interdépendance entre sécurité intérieure et sécurité extérieure, doit être constamment améliorée et intégrée dans les autres domaines d'action, tout en renforçant les synergies et en évitant les doubles emplois, y compris au moyen de méthodes de travail horizontales, d'échanges volontaires d'informations, de formations et d'exercices intersectoriels. À cette fin, il convient d'évaluer de manière plus approfondie le rôle de soutien et la contribution des mécanismes et agences concernés de l'UE, dans le cadre de leurs mandats respectifs et en accord avec les contraintes budgétaires existantes.

19. Le recours aux mécanismes et instruments pertinents de l'UE venant n appui aux réponses des États membres aux menaces intersectorielles et transfrontières devrait être davantage précisé par les institutions et organes de l'UE, en collaboration avec les États membres, notamment le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR), le mécanisme de protection civile de l'Union (MPCU) et son Centre de coordination de la réaction d'urgence (ERCC).

20. Le Conseil reconnaît la possibilité, pour les États membres , d'invoquer la clause de solidarité (article 222 du TFUE) pour faire face à une crise grave résultant d'activités hybrides.

Appréciation de la situation et analyse du renseignement

21. La coopération menée au sein de l'UE en matière de renforcement de la résilience et de lutte contre les menaces hybrides doit être guidée par une évaluation de la menace régulièrement actualisée et par une appréciation globale de la situation. Celles-ci doivent être mises au point par le Centre de situation et du renseignement de l'UE et sa cellule de fusion contre les menaces hybrides afin de renforcer les capacités de l'UE et de ses États membres à détecter, prévenir et perturber les activités hybrides, ainsi qu'à y réagir, dans le respect des compétences des États membres.
Le Conseil estime que les travaux de la cellule de fusion de l'UE contre les menaces hybrides devraient être encore renforcés, en prévoyant un niveau approprié de ressources, y compris en ce qui concerne l'expertise professionnelle.

22. Le Conseil rappelle ses conclusions du 19 avril 2016 sur la lutte contre les menaces hybrides, dans lesquelles il est demandé de mobiliser les instruments de l'UE afin de prévenir et de contrer les menaces hybrides qui pèsent sur l'UE, ses États membres et ses partenaires. Le Conseil insiste sur la nécessité de continuer à développer les fonctions existantes au niveau des États membres et de l'UE en matière d'appréciation de la situation, en tenant compte des sources de menaces, et à faire un meilleur usage de l'analyse du renseignement provenant du Centre de situation et du renseignement de l'UE et de sa cellule de fusion contre les menaces hybrides, notamment dans les processus de l'UE en matière de prise de décision et de gestion des crises dans le domaine de la lutte contre les menaces hybrides.

23. Le Conseil prend acte de la contribution pertinente que les missions et opérations de la PSDC pourraient apporter, le cas échéant, à l'identification et à l'analyse d'indicateurs concernant d'éventuelles actions hybrides menées par des tiers, y compris en matière de désinformation visant à discréditer et à entraver l'action de l'UE et de ses États membres, et reconnaît la valeur qu'il y a à étudier plus avant la possibilité de développer cette contribution.

Protection des infrastructures critiques

24. La protection des infrastructures critiques nationales et européennes, ainsi que des fonctions et des services indispensables au bon fonctionnement de l'État, de l'économie et de la société, est une priorité essentielle, notamment dans le cadre du renforcement de la résilience face aux menaces hybrides, nécessitant une approche réunissant pouvoirs publics et société dans leur ensemble. Ce travail doit prendre en compte les interdépendances fortes entre les différents fonctions et services critiques, y compris les services financiers, le rôle clé du secteur privé, l'évolution de l'environnement de sécurité et les risques émergents, tant dans le domaine physique que dans le domaine du cyberespace.

25. Par ailleurs, en complément des obligations juridiques, réglementaires et de surveillance instaurées par l'UE et les pays et régissant la résilience opérationnelle et la continuité des activités, il convient de promouvoir des arrangements avec les propriétaires et opérateurs d'infrastructures et de services du secteur privé, afin de garantir la continuité des services critiques et l'accès à ces services également en dehors des cas de force majeure, en assurant un niveau acceptable de préparation pour répondre à toutes les menaces pertinentes ainsi que la flexibilité nécessaire pour faire face à des événements dont la probabilité est faible mais l'impact élevé, les atténuer et s'en remettre.

26. Le Conseil souligne que, si la responsabilité de la protection des infrastructures critiques est avant tout une question de compétence nationale, le degré élevé d'interdépendances transfrontières et transsectorielles exige des efforts concertés ou, si nécessaire, harmonisés au niveau de l'UE, y compris au regard du fonctionnement ininterrompu du marché intérieur.

27. À la suite de l'évaluation de juillet 2019 relative à la mise en œuvre de la directive (2008/114/CE) concernant le recensement et la désignation des infrastructures critiques européennes, le Conseil invite la Commission à se concerter avec les États membres sur une éventuelle proposition de révision de la directive dès le début du nouveau cycle législatif, s'étendant aux mesures supplémentaires qui pourraient être prises pour renforcer la protection et la résilience des infrastructures critiques dans l'UE, compte tenu des interdépendances fortes entre les fonctions et les services critiques.

28. Le Conseil invite la Commission à poursuivre le dialogue avec les États membres et, au besoin, à élaborer des accords de coopération non contraignants entre les États membres partageant des infrastructures critiques connectées.

29. Le Conseil est conscient de l'importance que revêt la directive relative à la sécurité des réseaux et des systèmes d'information (directive SRI) pour le développement d'une culture de la gestion des risques et de la sécurité au sein des opérateurs présents dans les secteurs critiques ainsi que pour les capacités et stratégies nationales garantissant un niveau élevé de sécurité des réseaux et des systèmes d'information sur leur territoire, y compris dans le contexte des menaces hybrides.
Le Conseil invite les États membres, la Commission et l'Agence de l'Union européenne pour la cybersécurité (ENISA) à continuer d'étoffer leur coopération sur la base de la recommandation de la Commission sur la réponse concertée à apporter à tous les niveaux pertinents en cas de crises et d'incidents majeurs liés à la cybersécurité (schéma directeur).

Lutter contre la désinformation et garantir des élections libres et équitables

30. Le Conseil se félicite du rapport sur la mise en œuvre du plan d'action contre la désinformation et prend acte de ce que la poursuite de la mise en œuvre du plan d'action reste au cœur des efforts déployés par l'UE. Le Conseil souligne qu'il est nécessaire de réexaminer régulièrement et, si besoin est, de mettre à jour le plan d'action afin de garantir une approche à long terme efficace.

31. Le Conseil relève que le travail effectué par la division "Communication stratégique" du SEAE et, en particulier, par les trois task forces (Est, Balkans occidentaux, Sud) doit être soutenu par des ressources suffisantes permettant une planification, une mise en œuvre et une évaluation sur le long terme. Ces trois task forces devraient notamment avoir pour mission d'être capables de détecter, d'analyser et de contrecarrer de manière continue les activités de désinformation entreprises par des acteurs étatiques étrangers et des acteurs non étatiques extérieurs. Elles devraient également continuer de contribuer à une communication efficace et positive fondée sur les faits et à la promotion des principes et valeurs de l'UE ainsi que des politiques qu'elle mène dans son voisinage oriental et méridional et dans les Balkans occidentaux, et au renforcement de l'environnement médiatique et de la société civile dans leur ensemble dans leurs régions respectives. Le Conseil invite le SEAE à évaluer les besoins et les possibilités afin de renforcer son travail de communication stratégique dans d'autres zones géographiques, telles que l'Afrique subsaharienne, tout en conservant les capacités nécessaires pour mener à bien les tâches de communication stratégique existantes.

32. Le Conseil est conscient qu'une approche globale à tous les niveaux est nécessaire pour relever les défis liés à la désinformation, y compris les ingérences visant à compromettre la tenue d'élections libres et équitables en Europe, en tirant le meilleur parti de tous les outils disponibles en ligne et hors ligne. Cette approche doit inclure le suivi et l'analyse de la désinformation et des interventions manipulatrices, l'application des règles européennes en matière de protection des données, l'application de garanties électorales, des efforts visant à renforcer le pluralisme des médias, le professionnalisme des journalistes et l'éducation aux médias, ainsi que l'information des citoyens. Le Conseil recommande que l'on poursuive la consolidation d'un réseau transeuropéen actif et indépendant composé de vérificateurs de faits et de chercheurs pour lutter contre la désinformation. Le Conseil mesure l'importance de la société civile, du monde universitaire et du secteur privé et du rôle qu'ils jouent dans la lutte contre la désinformation et dans le renforcement de la résilience.

33. Le Conseil prend acte du potentiel du système d'alerte rapide en ce qui concerne la lutte contre la désinformation, en particulier pour ce qui est des ingérences dans les élections. Il demande instamment à la Commission et au SEAE, conjointement avec les États membres, de développer le système d'alerte rapide pour le transformer en une plateforme globale destinée aux États membres et aux institutions de l'UE et visant à renforcer la coopération, la coordination et l'échange d'informations, comme les connaissances issues de la recherche et de l'analyse, les bonnes pratiques, et les produits de communication, dans le but de soutenir la lutte contre les campagnes de désinformation dans le cadre des efforts déployés aux niveaux européen et national.

34. Le Conseil reconnaît l'utilité des mesures et recommandations présentées par la Commission le 12 septembre 2018 dans le cadre de son train de mesures visant à garantir des élections européennes libres et équitables. Le Conseil encourage la Commission et les États membres à examiner les possibilités de poursuivre les activités des réseaux européens de coopération dans le domaine électoral afin de faciliter l'échange d'informations et de bonnes pratiques. Le Conseil salue les efforts déployés par la Commission pour mobiliser tous les acteurs concernés et soutenir un large éventail de mesures, comme l'exercice sur la cybersécurité des élections européennes (EU ELEx19), en tenant compte des compétences nationales dans ce domaine.

35. Le Conseil est conscient qu'il est nécessaire de continuer à travailler avec les plateformes de médias sociaux afin d'appliquer des normes plus élevées en matière de responsabilité, de transparence et d'obligation de rendre des comptes dans la lutte contre la désinformation. En outre, il convient d'accorder, pour la recherche universitaire, un accès sans entrave aux données anonymisées provenant des fournisseurs de plateformes de médias sociaux, afin de faciliter l'élaboration de politiques fondées sur des données probantes. Le Conseil invite la Commission à présenter des initiatives sur la voie à suivre pour lutter contre la désinformation sur les plateformes en ligne. Ces initiatives devraient s'appuyer sur une évaluation de la mise en œuvre du code de bonnes pratiques contre la désinformation, qui devrait tenir compte des travaux d'analyse effectués et des rapports établis par les universités et les organisations de la société civile, du rapport de suivi du code élaboré par le groupe des régulateurs européens pour les services de médias audiovisuels, ainsi que des enseignements tirés des élections au Parlement européen de mai 2019. Dans ce contexte, le Conseil invite la Commission à examiner les moyens d'améliorer encore la mise en œuvre du code de bonnes pratiques, y compris d'éventuels mécanismes permettant d'assurer le respect des règles sur les plateformes en ligne, notamment en prévoyant une évaluation indépendante du respect, par les signataires, des engagements auxquels ils ont souscrit.

Sécurité des institutions, organes et agences de l'UE

36. La sécurité du personnel, des institutions, des organes et des agences de l'UE contre les menaces hybrides et autres activités malveillantes est dans l'intérêt tant de l'UE que de ses États membres. Le Conseil demande aux institutions, organes et agences de l'UE de veiller, avec le soutien des États membres, à ce que l'Union soit en mesure de protéger son intégrité et de renforcer la sécurité de ses réseaux d'information et de communication et de ses processus décisionnels pour les protéger des activités malveillantes de tous types, sur la base d'une évaluation globale de la menace. À cet effet, les institutions, organes et agences, soutenus par les États membres, devraient élaborer et mettre en œuvre un ensemble complet de mesures destinées à assurer leur sécurité, conformément au mandat du Conseil européen de juin 2019. Le Conseil souligne qu'il importe de garantir l'interopérabilité des infrastructures informatiques de l'UE pour l'échange d'informations classifiées entre les institutions, organes et agences de l'UE et les États membres.