Conseil de
l'Union européenne

Bruxelles, le 23 mai 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	23 mai 2022
Destinataire:	délégations
Objet:	Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne - Conclusions du Conseil approuvées par le Conseil lors de sa session du 23 mai 2022

Les délégations trouveront en annexe les conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne, approuvées par le Conseil lors de sa session du 23 mai 2022.

ANNEXE

Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne

LE CONSEIL DE L'UNION EUROPÉENNE,

RAPPELANT:

– ses conclusions relatives à la communication conjointe au Parlement européen et au Conseil du 25 juin 2013 concernant la stratégie de cybersécurité de l'Union européenne: "un cyberespace ouvert, sûr et sécurisé"[1];

– le cadre d'action de l'UE en matière de cyberdéfense[2];

– ses conclusions sur la gouvernance de l'internet[3];

– ses conclusions sur la cyberdiplomatie[4];

– ses conclusions intitulées "Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité"[5],

– ses conclusions sur la communication conjointe au Parlement européen et au Conseil du 20 novembre 2017 intitulée: "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide"[6],

– ses conclusions relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")[7];

– ses conclusions sur la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs[8];

– ses conclusions sur des lignes de conduite de l'UE concernant le renforcement des cybercapacités externes[9];

– la décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise[10];

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.

– ses conclusions sur le renforcement des capacités en matière de cybersécurité dans l'UE[11];

– ses conclusions sur l'importance de la 5G pour l'économie européenne et sur la nécessité d'atténuer les risques pour la sécurité liés à la 5G[12];

– ses conclusions sur l'avenir d'une Europe fortement numérisée après 2020: "Stimuler la compétitivité numérique et économique dans l'ensemble de l'Union et la cohésion numérique"[13];

– ses conclusions intitulées "Efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides"[14];

– ses conclusions intitulées "Façonner l'avenir numérique de l'Europe"[15];

– ses conclusions sur la cybersécurité des dispositifs connectés[16];

– ses conclusions sur la stratégie de cybersécurité de l'UE pour la décennie numérique[17];

– ses conclusions sur la sécurité et la défense[18];

– ses conclusions intitulées "Explorer le potentiel de l'initiative consistant à créer une unité conjointe de cybersécurité, en complément de la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs"[19];

– le document intitulé "Une boussole stratégique en matière de sécurité et de défense - Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales"[20],

---

10 JO L 320, du 17.12.2018, p. 28.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. SOULIGNE que les actes de cybermalveillance, de la part d'acteurs étatiques et non étatiques, se sont multipliés ces dernières années, notamment sous la forme d'activités malveillantes en augmentation rapide et constante ciblant les infrastructures critiques, les chaînes d'approvisionnement et la propriété intellectuelle de l'UE et de ses États membres, d'un risque accru d'effets d'entraînement, ainsi que d'une intensification des attaques par rançongiciels contre nos entreprises, nos organisations et nos citoyens; NOTE qu'avec le retour de la politique des rapports de force, certains pays tentent de plus en plus de remettre en question et de saper l'ordre international fondé sur des règles dans le cyberespace, en faisant de la cybersphère, à l'instar de la haute mer, du domaine aérien et de l'espace extra-atmosphérique, un domaine de plus en plus disputé; CONSTATE que les cyberattaques à grande échelle ou les tentatives d'intrusion dans les réseaux et systèmes d'information, ou de perturbation et de destruction de ces réseaux et systèmes d'information, qui entraînent des effets systémiques, sont devenues plus fréquentes, pourraient nuire à notre sécurité économique et affecter nos institutions ainsi que nos processus démocratiques, et montrent que certains acteurs sont prêts à mettre en péril la sécurité et la stabilité internationales; SOULIGNE que l'agression militaire de la Russie contre l'Ukraine a démontré que des cyberoffensives peuvent être menées dans le cadre de stratégies hybrides combinant intimidation, déstabilisation et perturbations économiques;

2. RAPPELLE que, face aux mutations géopolitiques actuelles, la force de notre Union réside dans l'unité, la solidarité et la détermination, et que la mise en œuvre de la boussole stratégique renforcera l'autonomie stratégique de l'UE et sa capacité à travailler avec ses partenaires pour préserver ses valeurs et ses intérêts, y compris dans le cyberespace; SOULIGNE qu'une Union plus forte et plus capable sur les questions de sécurité et de défense contribuera positivement à la sécurité globale et transatlantique et est complémentaire à l'OTAN, qui reste le fondement de la défense collective pour ses membres; RÉAFFIRME que L'UE a l'intention d'accroître son soutien à l'ordre international fondé sur des règles et articulé autour des Nations unies;

3. Conformément aux conclusions du Conseil sur la stratégie de cybersécurité de l'UE et à la boussole stratégique, RÉAFFIRME la nécessité de développer la posture cyber de l'Union en améliorant notre capacité à prévenir les cyberattaques grâce au renforcement et au développement des capacités, à la formation, à l'organisation d'exercices et à l'accroissement de la résilience ainsi qu'en réagissant fermement aux cyberattaques visant l'UE et ses États membres, en faisant pleinement usage de tous les outils disponibles au niveau de l'UE. Il s'agit notamment de continuer à manifester notre détermination à apporter des réponses immédiates et à long terme aux acteurs de la menace qui cherchent à refuser à l'UE et à ses partenaires un accès sûr et ouvert au cyberespace, et à nuire à nos intérêts stratégiques, y compris la sécurité de nos partenaires; dans ce contexte, SOULIGNE que la posture cyber vise à combiner les diverses initiatives concourant aux actions de l'UE qui consolident la paix et la stabilité dans le cyberespace et soutiennent un cyberespace ouvert, libre, mondial, stable et sûr, tout en améliorant la coordination des actions à court, moyen et long terme pour prévenir, décourager et dissuader les cybermenaces ainsi que les cyberattaques et y réagir, et en tirant mieux parti des cybercapacités; SOULIGNE que ces éléments devraient être intégrés dans la posture cyber de l'UE selon cinq fonctions de l'UE dans le domaine cyber: renforcer notre cyber-résilience et nos capacités de protection; renforcer la gestion solidaire et globale des crises; promouvoir notre vision du cyberespace; renforcer la coopération avec les pays partenaires et les organisations internationales; prévenir les cyberattaques, se défendre contre elles et y réagir;

I. RENFORCER NOTRE CYBERRÉSILIENCE ET NOS CAPACITÉS DE PROTECTION

4. RÉAFFIRME la nécessité de relever le niveau global de cybersécurité de l'UE, ATTEND AVEC INTÉRÊT l'adoption rapide du projet de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (SRI 2), du projet de règlement sur la résilience opérationnelle numérique du secteur financier (DORA) et du projet de directive sur la résilience des entités critiques (CER) et PREND NOTE de la proposition de règlement établissant des mesures relatives à un niveau élevé de cybersécurité au sein des institutions, organes et organismes de l'Union, afin de promouvoir une Union européenne qui protège ses citoyens, ses services publics et ses entreprises dans le cyberespace; ENCOURAGE la Commission à finaliser l'adoption de propositions clés visant à garantir que les infrastructures, les technologies, les produits et les services numériques soient sécurisés, afin d'envoyer un signal clair concernant les ambitions de l'UE dans ces domaines et de permettre d'aider les entreprises à relever ce défi; INVITE la Commission à proposer des exigences communes de l'UE en matière de cybersécurité des dispositifs connectés et des processus et services associés au moyen de la loi sur la cyberrésilience, qui devrait être présentée par la Commission avant la fin de 2022, en tenant compte de la nécessité d'une approche horizontale et globale couvrant l'ensemble du cycle de vie des produits numériques, et au moyen de la réglementation existante, en particulier dans le domaine de la cybersécurité;

5. INVITE les autorités compétentes, telles que l'Organe des régulateurs européens des communications électroniques (ORECE), l'Agence de l'Union européenne pour la cybersécurité (ENISA) et le groupe de coopération sur la sécurité des réseaux et de l'information (SRI), ainsi que la Commission européenne, à formuler, sur la base d'une évaluation des risques, des recommandations aux États membres et à la Commission européenne afin de renforcer la résilience des réseaux et infrastructures de communication au sein de l'Union européenne, y compris la poursuite de la mise en œuvre de la boîte à outils 5G de l'UE;

6. INVITE l'UE et ses États membres à redoubler d'efforts pour relever le niveau global de cybersécurité, par exemple en facilitant l'émergence de fournisseurs de services de cybersécurité fiables, et SOULIGNE qu'encourager le développement de ces fournisseurs devrait constituer une priorité de la politique industrielle de l'UE dans le domaine de la cybersécurité; afin de mieux résister aux cyberattaques ayant des effets systémiques potentiels et de mieux les contrer, et en tirant les enseignements de la gestion des vulnérabilités de Solarwinds, Microsoft Exchange et Apache Log4J, INVITE la Commission à proposer des pistes pour encourager l'émergence d'un secteur des services de cybersécurité fiable, renforcer la cybersécurité de la chaîne d'approvisionnement TIC, remédier aux effets potentiels des vulnérabilités logicielles pour l'UE et ses États membres, y compris dans la perspective de la future loi sur la cyberrésilience, et améliorer les capacités de détection des cybermenaces et de partage d'informations en la matière dans les États membres et entre eux;

7. RAPPELANT qu'il est essentiel d'investir dans l'innovation et de mieux utiliser les technologies civiles pour renforcer notre souveraineté technologique, y compris dans le domaine du cyberespace, INVITE la Commission à rendre rapidement opérationnel le Centre de compétences européen en matière de cybersécurité afin de mettre en place un écosystème européen solide dans les secteurs de la recherche, de l'industrie et des technologies cybernétiques, et SOULIGNE qu'il est nécessaire de dynamiser la recherche et l'innovation, d'investir davantage dans les domaines civil et de la défense pour renforcer la base industrielle et technologique de défense (BITDE) de l'UE et de développer les cybercapacités de l'UE et de ses États membres, y compris les capacités de soutien stratégique; FAIT RESSORTIR qu'il importe d'exploiter pleinement les nouvelles technologies, notamment dans le domaine de l'informatique quantique, de l'intelligence artificielle et des mégadonnées, en vue d'obtenir des avantages comparatifs, y compris en ce qui concerne les opérations de réponse aux cyberincidents;

8. CONSCIENT que le renforcement de notre cybersécurité permet d'accroître l'efficacité et la sécurité de notre action sur terre, dans les airs, en mer et dans l'espace extra-atmosphérique, SOULIGNE qu'il importe d'intégrer les considérations relatives à la cybersécurité dans toutes les politiques publiques de l'UE, y compris la législation sectorielle complétant la directive SRI 2, et INVITE la Commission à étudier les possibilités d'accroître la cybersécurité tout au long de la chaîne d'approvisionnement de la base industrielle et technologique de défense de l'UE;

9. CONSTATE qu'il est essentiel d'affecter des ressources financières et humaines suffisantes à la cybersécurité et de prendre des mesures visant à créer un environnement propice à la compétitivité du secteur privé pour développer la posture cyber de l'UE, et que la question du financement stable et à long terme de la cybersécurité devrait également être abordée au niveau de l'UE par la conception et la mise en œuvre d'un mécanisme horizontal combinant plusieurs sources de financement, y compris en ce qui concerne le coût lié à des ressources humaines hautement qualifiées; par conséquent, INVITE la Commission à étudier, avant la fin de 2022, les possibilités en ce qui concerne un tel mécanisme, qui seront examinées au sein des instances compétentes du Conseil;

10. SOULIGNE la nécessité de redoubler d'efforts et d'accroître la coopération dans la lutte contre la cybercriminalité internationale, en particulier les rançongiciels, par l'intermédiaire du mécanisme EMPACT (plateforme pluridisciplinaire européenne contre les menaces criminelles), grâce à des échanges entre les secteurs de la cybersécurité, de l'application des lois et de la diplomatie, et par le renforcement des capacités répressives pour les enquêtes et les poursuites en matière de cybercriminalité; RÉAFFIRME qu'il est résolu à informer le public sur les cybermenaces et les mesures prises à l'échelon national et au niveau de l'UE pour lutter contre ces menaces, en associant la société civile, le secteur privé et le monde universitaire, afin de sensibiliser à la cyberprotection et à l'hygiène cybernétique et d'encourager à les porter à un niveau approprié; INSISTE sur la nécessité de mettre l'accent sur les compétences et les capacités des citoyens en matière de cybersécurité au niveau de l'Union et des États membres, ainsi que sur la nécessité d'associer activement les utilisateurs à leur propre protection;

II. **RENFORCER LA GESTION DE CRISES SOLIDAIRE ET GLOBALE**

11. Tirant les enseignements des exercices annuels de cybersécurité, d'autres exercices comportant une dimension cyber et de l'exercice EU CyCLES 2022, SOULIGNE qu'il importe d'établir un programme d'exercices de cybersécurité intercommunautaires et multiniveaux réguliers afin de tester et de développer la réponse interne et externe de l'UE aux cyberincidents de grande ampleur, avec la participation du Conseil, du SEAE, de la Commission et des parties prenantes concernées, telles que l'ENISA et le secteur privé, qui sera élaboré et contribuera à la politique générale de l'UE en matière d'exercices; INSISTE sur l'importance que revêt l'approfondissement des exercices Cyber Europe et Blue OLEx, en combinant les réponses à différents niveaux; EST CONSCIENT de la nécessité d'évaluer et de consolider les exercices existants ainsi que d'étudier la possibilité d'exercices supplémentaires sur des segments spécifiques du domaine cyber, notamment un exercice pour les CERT militaires et un exercice axé sur la coopération en cas de crise entre les institutions, organes et organismes de l'UE; NOTE que la posture cyber de l'Union renforcera notre capacité à prévenir les cyberattaques grâce à différentes actions, dont la formation, et INVITE dès lors les États membres à améliorer la coopération civilo-militaire en matière de formations dans le domaine cyber et d'exercices conjoints;

12. SOULIGNE la nécessité de continuer à tester et à renforcer la coopération opérationnelle et l'appréciation commune de la situation entre les États membres, y compris par l'intermédiaire de réseaux établis tels que le réseau des CSIRT et le réseau européen pour la préparation et la gestion des crises cyber (UE-CyCLONe), afin de faire progresser la préparation de l'UE à faire face aux cyberincidents de grande ampleur; FAIT RESSORTIR qu'il importe de travailler à l'élaboration d'un langage commun entre les États membres et les institutions, organes et organismes de l'UE, qui soit adapté aux discussions au niveau politique, afin de soutenir la mise en place d'une évaluation consolidée de la gravité et de l'impact des cyberincidents pertinents ainsi que des scénarios d'évolution possibles et des besoins qui en découlent, le cas échéant; MET EN AVANT à cet égard qu'il est nécessaire de renforcer la complémentarité des rapports d'évaluation commune de la situation, y compris les rapports du réseau UE-CyCLONe sur l'impact et la gravité des cyberincidents de grande ampleur dans les États membres de l'UE et les évaluations des menaces fournies par le Centre de situation et du renseignement de l'UE (INTCEN) dans le cadre de la boîte à outils cyberdiplomatique de l'UE; INVITE la Commission, le haut représentant et le groupe de coopération SRI, en coordination avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau UE-CyCLONe, à procéder, d'ici la fin de 2022, à une évaluation des risques ainsi qu'à élaborer des scénarios de risque du point de vue de la cybersécurité portant sur une situation de menace ou d'attaque éventuelle contre des États membres ou des pays partenaires, et à les présenter aux instances compétentes au sein du Conseil; SOULIGNE qu'une communication au public appropriée et coordonnée sur la réponse de l'UE aux cyberincidents de grande ampleur est nécessaire;

13. Dans l'éventualité d'un cyberincident de grande ampleur, MET L'ACCENT sur la nécessité de renforcer la coordination et, le cas échéant, la mutualisation volontaire entre les États membres de nos capacités de réaction aux incidents, en s'appuyant sur les progrès accomplis et sur les travaux menés par les équipes CSP d'intervention rapide en cas d'incident informatique ainsi que sur les travaux du réseau des CSIRT et du réseau UE-CyCLONe; RECONNAÎT que nouer des liens avec le secteur privé pourrait permettre d'amplifier les capacités publiques, en particulier dans un contexte de pénurie de compétences dans l'ensemble de l'UE, et que le recensement et la coordination de ces partenaires privés pourraient être décisifs en cas d'incidents de grande ampleur; pour se préparer pleinement à faire face aux cyberincidents de grande ampleur, INVITE la Commission à présenter une proposition relative à un nouveau fonds d'intervention d'urgence en matière de cybersécurité d'ici la fin du troisième trimestre de 2022;

14. Conformément à la boussole stratégique, RÉAFFIRME la nécessité d'investir dans notre assistance mutuelle, en vertu de l'article 42, paragraphe 7, du traité sur l'Union européenne, ainsi que dans notre solidarité, en vertu de l'article 222 du traité sur le fonctionnement de l'Union européenne, notamment par des exercices fréquents; dans ce cadre, MET L'ACCENT sur la nécessité de poursuivre les travaux sur la fourniture et la coordination d'un appui civil et/ou militaire bilatéral, y compris en étudiant la possibilité que l'UE apporte un appui à la demande expresse des États membres, et sur la définition de mesures de réaction appropriées, y compris par le développement d'une stratégie de communication coordonnée, dans le contexte de la mise en œuvre de l'article 42, paragraphe 7; NOTE que cela devrait également inclure l'exploration des liens avec les mécanismes de gestion de crises existants de l'UE et avec le mécanisme de protection civile de l'Union;

15. SOULIGNE qu'une posture cyber renforcée de l'UE nécessitera des communications plus sécurisées; à cette fin, RÉAFFIRME les orientations données par la boussole stratégique sur cette question et INVITE la Commission et les autres institutions, organes et organismes concernés à procéder, d'ici la fin de 2022, à une cartographie des outils de communication sécurisée existants dans le domaine cyber, qui sera examinée au sein des instances compétentes du Conseil et avec les groupes de coopération concernés, tels que le réseau des CSIRT et le réseau UE-CyCLONe;

III. PROMOUVOIR NOTRE VISION DU CYBERESPACE

16. RAPPELLE que l'approche commune et globale de l'UE en matière de cyberdiplomatie vise à contribuer à la prévention des conflits, à l'atténuation des menaces en matière de cybersécurité et au renforcement de la stabilité des relations internationales; dans ce contexte, RÉAFFIRME l'attachement de l'UE au règlement des différends internationaux dans le cyberespace par des moyens pacifiques et l'application du droit international, y compris le droit international relatif aux droits de l'homme et le droit international humanitaire, aux actions des États dans le cyberespace; SOULIGNE que l'UE et ses États membres sont déterminés à agir conformément aux normes volontaires non contraignantes adoptées par tous les États membres des Nations unies en matière de comportement responsable des États dans le cyberespace; MET L'ACCENT sur l'importance que revêt un cyberespace ouvert, libre, mondial, stable et sécurisé, dans lequel les droits de l'homme, les libertés fondamentales et l'État de droit s'appliquent pleinement en faveur du bien-être social, de la croissance économique, de la prospérité et de l'intégrité de nos sociétés libres et démocratiques, et RÉAFFIRME l'engagement de l'UE et de ses États membres à continuer de promouvoir ces valeurs et principes; en vue d'établir des canaux de dialogue constructif, franc et ouvert avec les principales parties prenantes du cyberespace, MET L'ACCENT sur le fait qu'il importe que les questions liées au cyberespace, y compris la boîte à outils cyberdiplomatique de l'UE, fassent partie intégrante des négociations d'adhésion à l'Union et des dialogues stratégiques et politiques que l'UE mène avec les partenaires et concurrents internationaux; et dans le même temps, INVITE le haut représentant à réexaminer les dialogues bilatéraux existants sur le cyberespace et, si nécessaire, à proposer d'entamer une coopération similaire avec d'autres pays ou organisations internationales concernées;

17. RAPPELLE l'importance de la coopération multipartite, d'autres parties prenantes ayant aussi une responsabilité en matière de cybersécurité, notamment pour ce qui est de la mise en œuvre des recommandations et des décisions prises dans les enceintes internationales et régionales; INVITE l'UE et ses États membres à continuer de promouvoir notre modèle de cyberespace et de l'internet sur la base de l'approche multipartite et au moyen d'initiatives telles que l'appel de Paris pour la confiance et la sécurité dans le cyberespace et la déclaration sur l'avenir de l'internet, en mettant l'accent sur les avantages communs que procure la stabilité dans le cyberespace et en sensibilisant à l'échelle mondiale aux dangers d'une vision autoritaire et centrée sur l'État de l'internet, et INVITE l'UE et ses États membres à renforcer encore la coopération avec la communauté multipartite, y compris en recourant à des projets pertinents tels que l'initiative de cyberdiplomatie de l'UE au titre de l'instrument de politique étrangère de l'Union;

18. S'ENGAGE à s'impliquer sans relâche dans les organisations internationales compétentes, en particulier dans le cadre des processus liés aux première et troisième commissions des Nations unies, tout en soulignant que le droit international en vigueur s'applique, sans réserve, au cyberespace et à l'égard de celui-ci; MET EN AVANT qu'il importe de poursuivre les efforts visant à faire respecter et à promouvoir le cadre des Nations unies pour le comportement responsable des États, et FAIT RESSORTIR que l'UE et ses États membres s'emploieront activement à en renforcer la mise en œuvre, y compris par la mise en place du programme d'action des Nations unies pour un comportement responsable des États dans le cyberespace; INSISTE sur le fait que l'UE et ses États membres participeront activement aux négociations en vue d'une future convention des Nations unies destinée à servir d'instrument efficace pour les autorités répressives et judiciaires dans la lutte contre la cybercriminalité à l'échelle mondiale, en tenant pleinement compte du cadre existant des instruments internationaux et régionaux dans ce domaine, en particulier la convention de Budapest sur la cybercriminalité; SOULIGNE qu'il importe de continuer à soutenir l'élaboration et la mise en œuvre opérationnelle de mesures de confiance (MDC) aux niveaux régional et international, et de continuer à encourager le recours aux MDC existantes dans le domaine cyber au sein de l'OSCE, y compris en période de tensions internationales;

19. RAPPELLE qu'il est essentiel d'adopter une approche proactive fondée sur les droits de l'homme visant à faire en sorte que des normes internationales soient en place dans les domaines des technologies émergentes et de l'architecture de base de l'internet, conformément aux valeurs et principes démocratiques, pour garantir que l'internet reste mondial, non fragmenté et ouvert, et SOUTIENT le principe selon lequel l'utilisation et le développement de technologies respectant les droits de l'homme, axées sur le respect de la vie privée et dont l'utilisation soit licite, sûre et éthique; ENCOURAGE le haut représentant et la Commission à élaborer une vision stratégique concernant les questions techniques dans le domaine numérique qui ont des implications en matière de politique étrangère et qui pourraient avoir une incidence sur la stabilité du cyberespace et de l'internet en particulier, y compris au sein des organisations internationales spécialisées concernées (Union internationale des télécommunications, etc.);

IV. RENFORCER LA COOPÉRATION AVEC LES PAYS PARTENAIRES ET LES ORGANISATIONS INTERNATIONALES

20. MET L'ACCENT sur la nécessité de mieux relier la stratégie de l'UE en matière de renforcement des cybercapacités aux normes des Nations unies en matière de comportement responsable des États dans le cyberespace, y compris en élaborant des programmes de coopération et de renforcement des capacités sur mesure pour soutenir les États tiers dans leurs efforts de mise en œuvre, et, ce faisant, en poursuivant et en intensifiant nos efforts visant à promouvoir le programme d'action des Nations unies pour un comportement responsable des États dans le cyberespace; SOULIGNE qu'il importe d'intégrer pleinement le renforcement des cybercapacités dans l'offre de l'UE en tant que garante de la sécurité, avec une coordination adéquate des efforts entre les institutions, organes et agences de l'UE et, en particulier, SE FÉLICITE de la coopération entre États membres, ainsi qu'avec des partenaires des secteurs public et privé, notamment au moyen du réseau de l'UE pour le renforcement des cybercapacités (EU Cybernet) et du Forum mondial sur la cyberexpertise (GFCE), afin d'assurer la coordination et d'éviter les doubles emplois;

INVITE le haut représentant et la Commission à mettre en place un *comité pour le renforcement des cybercapacités* d'ici au troisième trimestre de 2022 et à organiser des échanges réguliers au sein du groupe horizontal "Questions cyber"; APPELLE la Commission et le haut représentant à mobiliser davantage l'instrument de voisinage, de coopération au

développement et de coopération internationale (IVCDCI), l'instrument d'aide de préadhésion (IAP III) et d'autres instruments financiers, tels que la facilité européenne pour la paix (FEP) et la stratégie "Global Gateway", afin de soutenir le renforcement de la résilience de nos partenaires, de leur capacité à identifier les cybermenaces et à y faire face, ainsi qu'à enquêter sur la cybercriminalité et à en poursuivre les auteurs, et le développement de projets de coopération, y compris dans un contexte de crise, et, en particulier, PROMEUT la coopération avec les partenaires des Balkans occidentaux et du voisinage oriental et méridional de l'UE, ainsi que le déploiement d'experts de l'UE et des États membres pour offrir un soutien en cas de crises cyber, compte tenu des mandats juridiques existants;

21. INSISTE sur la nécessité d'intensifier les efforts visant à élaborer une approche de sensibilisation structurée et ouverte de l'UE concernant la manière de promouvoir une compréhension commune à l'échelle mondiale de l'application du droit international dans le cyberespace et du cadre des Nations unies pour le comportement responsable des États dans le cyberespace, y compris l'initiative relative à un programme d'action pour un comportement responsable des États dans le cyberespace, et concernant la position de l'UE et de ses États membres dans le cadre des négociations en cours portant sur une convention des Nations unies sur la cybercriminalité, et, dans le cadre de ces efforts, DEMANDE au haut représentant de présenter un plan de sensibilisation au Conseil d'ici la fin de 2022; ENCOURAGE le haut représentant et les services de la Commission à utiliser pleinement et de manière systématique les 145 délégations et à mettre en place une coopération régulière et fructueuse entre celles-ci et les ambassades des États membres dans les pays tiers, sous les auspices du réseau européen de cyberdiplomatie envisagé; INCITE le haut représentant à mettre en place le réseau européen de cyberdiplomatie d'ici au troisième trimestre de 2022, en contribuant à l'échange d'informations, à des activités de formation conjointes destinées au personnel de l'UE et des États membres, à des efforts cohérents de renforcement des capacités et à une consolidation de la mise en œuvre du cadre des Nations unies pour le comportement responsable des États, ainsi qu'à l'adoption de mesures visant à instaurer un climat de confiance entre les États;

22. MET EN AVANT sa détermination à coopérer davantage avec les organisations internationales et les pays partenaires afin de faire progresser la compréhension commune du paysage des cybermenaces, d'établir des mécanismes de coopération et de définir des réponses diplomatiques coopératives de manière proactive; RAPPELANT les grandes réalisations de la coopération UE-OTAN en matière de cybersécurité dans le cadre de la mise en œuvre des déclarations conjointes de Varsovie et de Bruxelles, de 2016 et 2018 respectivement, dans le plein respect de l'autonomie décisionnelle et des procédures décisionnelles des deux organisations et sur la base des principes de transparence, de réciprocité et d'inclusivité, FAIT RESSORTIR la nécessité de renforcer davantage la coopération en matière de cybersécurité avec l'OTAN au moyen d'exercices, de partage d'informations et d'échanges entre experts, y compris en ce qui concerne le développement des capacités, le renforcement des capacités pour les partenaires, les missions et les opérations, ainsi que l'applicabilité du droit international et les normes des Nations unies en matière de comportement responsable des États dans le cyberespace, et d'éventuelles réponses coordonnées aux actes de cybermalveillance;

V. PRÉVENIR LES CYBERATTAQUES, SE DÉFENDRE CONTRE ELLES ET Y RÉAGIR

23. CONSTATE que le cyberespace est devenu une arène de compétition géopolitique et, par conséquent, RÉAFFIRME que l'UE doit être en mesure de réagir rapidement et vigoureusement aux cyberattaques, telles que les actes de cybermalveillance soutenus par un acteur étatique ciblant l'UE et ses États membres, et a donc besoin de renforcer la boîte à outils cyberdiplomatique de l'UE et de faire pleinement usage de tous ses instruments, notamment les outils de communication politique, économique, diplomatique, juridique et stratégique dont elle dispose pour empêcher, décourager et prévenir les actes de cybermalveillance ainsi qu'y faire face; FAIT VALOIR que les acteurs hostiles doivent être conscients du fait que les cyberattaques contre les États membres et les institutions de l'UE seront détectées à un stade précoce, rapidement identifiées et traités avec l'ensemble des outils et des politiques nécessaires; en s'appuyant notamment sur les éléments de la posture cyber qui y figurent et sur les enseignements tirés de la mise en œuvre de la boîte à outils cyberdiplomatique depuis sa création et de l'exercice cyber EU CyCLES, INVITE les États membres et le haut représentant à œuvrer, avec le soutien de la Commission, à l'élaboration d'une version révisée des lignes directrices de mise en œuvre de la boîte à outils cyberdiplomatique de l'UE, d'ici la fin du premier trimestre de 2023, notamment en étudiant des mesures de riposte supplémentaires;

24. SOULIGNE la nécessité d'organiser des échanges réguliers sur le paysage des cybermenaces au sein des organes et comités compétents du Conseil, tout en coopérant régulièrement avec le secteur privé et en s'appuyant sur l'évaluation de l'impact et de la gravité des incidents récents, afin d'accroître la sensibilisation générale et la préparation à de nouvelles applications de la boîte à outils cyberdiplomatique de l'UE, et de mettre au point de nouveaux outils pour en soutenir la mise en œuvre; alors que la sécurité nationale reste de la seule responsabilité de chaque État membre, NOTE qu'il est nécessaire de renforcer le partage de renseignements et d'informations et la coopération entre les États membres, ainsi qu'avec l'INTCEN, afin de pouvoir échanger des renseignements au début du processus décisionnel, y compris sur la question de l'attribution, et de permettre ainsi une réponse rapide, efficace et étayée aux actes de cybermalveillance ciblant l'UE et ses partenaires; RAPPELLE qu'il importe de renforcer les capacités de l'INTCEN dans le domaine du cyberespace, sur la base de contributions volontaires des États membres en matière de renseignement et sans préjudice des compétences de ces derniers, et d'étudier la proposition relative à la mise en place éventuelle d'un groupe de travail des États membres en matière de cyber-renseignement;

25. RECONNAISSANT que les déclarations de l'UE et les mesures restrictives prises dans le cadre de la boîte à outils cyberdiplomatique de l'UE ont envoyé un message fort comme quoi les actes de cybermalveillance constituant une menace extérieure pour l'UE, ses États membres et ses partenaires sont inacceptables, et contribuent ainsi à empêcher, décourager et prévenir les actes de cybermalveillance ainsi qu'à y faire face, RÉAFFIRME sa détermination à recourir à ces mesures en vue de rappeler les obligations qui s'appliquent au cyberespace en vertu du droit international, y compris la charte des Nations unies dans son intégralité, et de promouvoir le cadre des Nations unies pour le comportement responsable des États dans le cyberespace, y compris l'obligation de diligence qui oblige tous les États à ne pas permettre sciemment que leur territoire soit utilisé pour commettre des actes internationalement illicites à l'aide des TIC, en vue de continuer à élaborer et à promouvoir la vision partagée de l'UE sur l'applicabilité du droit international dans le cyberespace; notant que des messages appropriés et rapides atténuent les risques d'escalade et peuvent dissuader les agresseurs qui ciblent les intérêts européens, INVITE le haut représentant à élaborer et à soumettre aux États membres une stratégie de communication cohérente sur l'utilisation de la boîte à outils cyberdiplomatique de l'UE;

26. ENCOURAGE l'élaboration d'approches et de réponses progressives, ciblées et durables en réaction aux actes de cybermalveillance, en ayant recours au large éventail d'outils fournis par la boîte à outils cyberdiplomatique de l'UE, y compris le régime de sanctions de l'UE contre les cyberattaques, et en envisageant des mesures supplémentaires; MET L'ACCENT sur la nécessité d'accroître la possibilité de mobiliser, au cas par cas, tous les outils disponibles, internes et externes, pour empêcher, décourager et prévenir les cyberattaques ainsi qu'y faire face, par une mise en œuvre dans le cadre d'une approche rapide, efficace, progressive, ciblée et soutenue fondée sur un engagement stratégique à long terme; APPELLE le haut représentant, en coopération avec la Commission, à définir d'éventuelles réponses communes de l'UE aux cyberattaques, y compris des options en matière de sanctions, dans tous les domaines afin d'être prêt à prendre des mesures rapides et efficaces, le cas échéant, et de les présenter au Conseil d'ici la fin du premier trimestre de 2023;

27. Prenant note du fait que la cyberdéfense relève essentiellement de la responsabilité des pays, INCITE les États membres à développer davantage leurs propres capacités à mener des opérations de cyberdéfense, y compris par des mesures proactives de protection, de détection, de défense et de dissuasion concernant les cyberattaques, et ce, éventuellement, en appui à d'autres États membres et à l'UE; chaque État membre est encouragé à renforcer, en tant que de besoin, ses propres capacités à fournir et à recevoir une aide et une assistance; SOULIGNE que la poursuite du développement de ces capacités devrait être l'un des principaux objectifs de la future politique de l'UE en matière de cyberdéfense; NOTE que la politique de l'UE en matière de cyberdéfense devrait accorder davantage d'attention au rôle que les institutions et organes compétents de l'UE peuvent jouer pour renforcer la coopération entre les acteurs pertinents de l'UE et des États membres dans le domaine de la cyberdéfense et développer leurs propres capacités, conformément à leurs mandats respectifs; INVITE le haut représentant, conjointement avec la Commission, à compléter le développement d'une posture cyber de l'UE en présentant une proposition ambitieuse de politique de l'UE en matière de cyberdéfense, en 2022, qui ouvrira la voie à la poursuite du développement de la posture cyber de l'UE par le Conseil;

28. INSISTE sur la nécessité de renforcer l'interopérabilité et le partage d'informations grâce à la coopération entre les équipes militaires d'intervention en cas d'urgence informatique (milCERT); INVITE les États membres à créer, sur la base des travaux de l'AED, un réseau d'équipes milCERT afin de développer la coopération et de faciliter l'échange d'informations, ce qui contribuerait également à favoriser la coordination avec d'autres cybercommunautés, ainsi qu'un réseau des commandants militaires cyber visant à renforcer la coopération stratégique entre les commandements cyber des États membres de l'UE ou d'autres autorités correspondantes; La mise en place de ces réseaux, ainsi que de cyberprojets relevant de la CSP, contribuerait à renforcer la cyberdéfense au niveau de l'UE; fait ressortir l'importance de la coopération entre le réseau proposé pour les équipes milCERT et le réseau civil (des CSIRT) déjà existant pour renforcer le partage des informations et améliorer l'appréciation de la situation;

29. Sur la base de la stratégie et vision militaires de l'UE sur le cyberespace en tant que domaine d'opérations et compte tenu du développement en cours du concept militaire de cyberdéfense dans les opérations et missions militaires dirigées par l'UE, RÉAFFIRME la nécessité d'intégrer la dimensison cyber dans la planification et la conduite des missions et opérations PSDC, y compris en en renforçant les cybercapacités, et SOULIGNE que cela contribuera à une meilleure appréciation de la situation cyber au niveau de l'UE;

30. Pour conclure, NOTE que la posture cyber constituera une étape vers l'établissement d'une doctrine de l'UE en matière d'action dans le cyberespace, fondée sur le renforcement de la résilience, des capacités et des options de réaction, ainsi que sur une position commune relative à l'application du droit international dans le cyberespace. Le Conseil FERA LE POINT sur les progrès accomplis dans la mise en œuvre des présentes conclusions en 2023, afin d'assurer la poursuite du développement de la posture cyber de l'UE.