Conseil de
l'Union européenne

**Bruxelles, le 12 décembre 2017**
**(OR. en)**

**15748/17**

**CYBER 215**
**TELECOM 362**
**ENFOPOL 618**
**JAI 1206**
**MI 959**
**COSI 333**
**JAIEX 117**
**RELEX 1122**
**IND 377**
**CSDP/PSDC 720**
**COPS 400**
**POLMIL 167**

**RÉSULTATS DES TRAVAUX**

| | |
|---|---|
| Origine: | Secrétariat général du Conseil |
| en date du: | 12 décembre 2017 |
| Destinataire: | délégations |
| Nº doc. préc.: | 14435/17 + COR 1 |
| Objet: | Plan d'action mettant en œuvre les conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil: Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide - Plan d'action (12 décembre 2017) |

Les délégations trouveront en annexe le plan d'action mettant en œuvre les conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil intitulée "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide", adoptées par le Conseil des affaires générales le 12 décembre 2017.

**ANNEXE**

Le présent plan d'action mettant en œuvre les conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil intitulée "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide" constitue un document stratégique élaboré en réponse aux demandes formulées par le Conseil européen et le Conseil en date respectivement des 19 et 24 octobre 2017. Comme indiqué dans les conclusions du Conseil du 20 novembre 2017, le plan d'action est destiné à être utilisé comme un document évolutif et, à ce titre, sera régulièrement réexaminé et actualisé par le Conseil. Il est conçu comme un instrument de contrôle horizontal et de suivi stratégique de la mise en œuvre des conclusions du Conseil et des actions exposées ci-après.

| **Action**[1] | **Chef de file / responsable principal** | **Parties prenantes et/ou autres parties concernées** | **Délai** | **Progrès** | **Notes / commentaires** |
|---|---|---|---|---|---|
| **Assurer la transposition et la mise en œuvre intégrales et effectives de la directive SRI** | | | | | |
| Transposition et mise en œuvre de la directive SRI | États membres; Commission européenne | | Mai 2018 | Progrès résumés par la Commission et discutés au sein du groupe de coopération | |
| Assurer une coopération stratégique efficace entre les États membres au sein du groupe de coopération | États membres / présidence du Conseil | Commission européenne, ENISA | | Progrès résumés dans le rapport régulier du groupe de coopération | Les travaux du groupe de coopération sont expliqués plus en détail dans le programme de travail bisannuel du groupe |

[1] Le cas échéant, les actions sont exécutées compte tenu des ressources prévues au titre du CFP.

| | | | | | |
|---|---|---|---|---|---|
| Faire en sorte que le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT) atteigne sa pleine capacité opérationnelle | États membres / présidence du Conseil | ENISA, Commission européenne | | Progrès accomplis résumés dans le rapport régulier adressé par le réseau au groupe de coopération | |
| **Renforcer la réponse au niveau de l'UE aux incidents de cybersécurité majeurs en réalisant régulièrement des exercices paneuropéens de cybersécurité** | | | | | |
| Mener des exercices de cyberdiplomatie portant sur l'utilisation du cadre diplomatique conjoint pour lutter contre les actes de cybermalveillance | SEAE | États membres, Commission européenne et ENISA | | Présidences successives du Conseil, les discussions sur les exercices portant sur l'utilisation du cadre ont débuté sous la présidence EE | |
| Mener régulièrement des exercices CYBER EUROPE | Présidence en coopération avec les États membres | États membres, y compris le réseau des CSIRT, ENISSA, SEAE, Commission européenne | | | Fréquence définie dans le cadre du mandat de l'ENISA et au cours des discussions au sein du CA de l'ENISA |

| | | | | | |
|---|---|---|---|---|---|
| Mener régulièrement des exercices stratégiques de cybersécurité dans le cadre des différentes formations du Conseil | Présidence | avec le soutien du SEAE et/ou de la Commission européenne | | Exercice EU CYBRID 2017 mené sous la présidence EE en ce qui concerne le Conseil des affaires étrangères (défense) | Fréquence définie par les États membres au sein du Conseil |
| **Adoption par les colégislateurs du RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)[2]** | | | | | |
| Examiner en détail la proposition législative au sein du groupe horizontal dans la perspective d'une orientation générale | Présidence BG | | Juin 2018 | Examen de la proposition mené par la présidence EE | |
| Conclure les négociations entre les colégislateurs | Présidence AT | | Décembre 2018 | | Délai indicatif |

[2] La mise en œuvre s'entend sans préjudice des compétences du Parlement européen.

| **Mettre en place le réseau de centres de compétences en cybersécurité et un centre européen de recherche et de compétences en cybersécurité** | | | | | |
|---|---|---|---|---|---|
| Établir une analyse d'impact, un budget prévisionnel et les instruments juridiques nécessaires aux fins de la mise en place du réseau de centres de compétences en cybersécurité et d'un centre européen de recherche et de compétences en cybersécurité | Commission européenne | États membres, SEAE, AED | Juin 2018 | | Travaux ultérieurs sur les instruments fournis à déterminer par les États membres au sein du Conseil |
| Lancement d'une phase pilote dans le cadre d'Horizon 2020 | Commission européenne | États membres, groupe de coopération SRI | Fin 2018 / début 2019 | | |

| | | | | | |
|---|---|---|---|---|---|
| Développer une capacité européenne dans le domaine de l'évaluation de la force de la cryptographie utilisée dans les produits et services mis à la disposition des citoyens, des entreprises et des pouvoirs publics au sein du marché unique numérique | États membres | | 2019 | | |
| **Assurer un financement suffisant pour soutenir le développement de la cyber-résilience et les efforts de recherche et de développement en matière de cybersécurité dans toute l'UE** | | | | | |
| Assurer un financement suffisant de la cybersécurité, dans le respect des ressources disponibles | États membres, Commission européenne | | 2020 | | |

| | | | | | |
|---|---|---|---|---|---|
| Accroître les contributions du secteur public pour développer la cyber-résilience et renforcer les efforts de recherche et de développement en matière de cybersécurité | États membres | | 2020 | | |
| Encourager les investissements du secteur privé pour développer la cyber-résilience et renforcer les efforts de recherche et de développement en matière de cybersécurité. | Commission européenne | avec le soutien du Bureau de sécurité de la Commission | 2018 | | |
| Accroître les investissements dans les applications de nouvelles technologies en matière de cybersécurité | Commission européenne, États membres | avec le soutien du Bureau de sécurité de la Commission | 2020 | | |

| | | | | | |
|---|---|---|---|---|---|
| Examiner une éventuelle proposition relative à la création d'un fonds d'intervention d'urgence en matière de cybersécurité | Conseil[3] | | | | D'éventuels travaux dans ce domaine ne seront menés que sur la base d'une proposition présentée par la Commission européenne |
| Consacrer des ressources financières suffisantes à la cybersécurité dans le cadre des instruments existants et des programmes approuvés | États membres, Commission européenne | BEI | 2020 | | |

[3] Sans préjudice des compétences du Parlement européen, le cas échéant.

| | | | | | |
|---|---|---|---|---|---|
| **Fournir des services crédibles, fiables et coordonnés en matière de cybersécurité et en assurer la gouvernance pour les institutions de l'UE** | | | | | |
| Clarifier et harmoniser la gouvernance, en matière de cybersécurité, des institutions, organes et agences de l'UE | Conseil, Commission européenne et SEAE | Institutions, organes et agences de l'UE | 2020 | Un rapport devrait être présenté au groupe horizontal "Questions liées au cyberespace" en ce qui concerne la gouvernance et les progrès enregistrés en la matière. | |
| Prévoir des ressources et un soutien appropriés pour le renforcement de l'équipe CERT-UE | Institutions, organes et agences de l'UE | | 2020 | L'équipe CERT-UE fait régulièrement rapport au groupe horizontal "Questions liées au cyberespace" en ce qui concerne les cybermenaces pesant sur les entités qui la composent. L'affectation de ressources à l'équipe CERT-UE peut être abordée dans le cadre des discussions concernées du groupe horizontal "Questions liées au cyberespace". | |
| **Mettre davantage l'accent sur la sensibilisation à la cybersécurité, les compétences numériques, ainsi que sur l'éducation et la formation** | | | | | |
| Renforcer les campagnes de sensibilisation à la cybersécurité dans les États membres | États membres | ENISA | 2020 | | |

| | | | | | |
|---|---|---|---|---|---|
| Renforcer la cybersécurité dans les programmes universitaires, d'éducation et de formation professionnelle | États membres | Commission européenne, Bureau de sécurité de la Commission | 2020 | Suivi des progrès assuré par les États membres et la Commission européenne | |
| Mettre en place un réseau de points de contact en matière d'éducation | États membres | ENISA | 2020 | | |
| Intégrer et renforcer les programmes de formation en matière de cybersécurité | États membres | Commission européenne, Bureau de sécurité de la Commission | 2020 | | |
| Assurer une sensibilisation en lien avec la cybersécurité dans les administrations publiques qui participent à des activités sociétales ou économiques critiques | États membres | | 2020 | Engagement en matière d'hygiène informatique signé par six États membres, le SEAE et l'AED en mai 2015 | |

| Renforcer la capacité de l'UE à prévenir, à dissuader et à déceler les actes de cybermalveillance ainsi que sa capacité à y répondre | | | | | |
|---|---|---|---|---|---|
| Intégrer la question de la cybersécurité dans les mécanismes de gestion des crises qui existent déjà au niveau de l'UE | Commission européenne, Conseil | SEAE, agences de l'UE | 2018 | | |
| Prendre en charge de manière satisfaisante la réaction aux cyberincidents dans les mécanismes de gestion de crises et prévoir les procédures de coopération nécessaires au niveau de l'UE | États membres | | 2018 | | |
| Mettre à jour le cadre stratégique de cyberdéfense de l'UE | États membres, SEAE, AED, Commission européenne | | 2018 | | |
| Encourager la coopération entre acteurs civils et militaires en cas de cyberincident | États membres | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Mettre en place une plateforme de formation et d'enseignement en matière de cyberdéfense | Commission européenne | SEAE, AED, CESD | fin 2018 | | |
| Tirer pleinement parti des initiatives proposées en matière de défense afin d'accélérer le développement de capacités de cyberdéfense en Europe | États membres | SEAE, AED, Commission européenne | | | Des projets de cyberdéfense peuvent être développés dans le cadre de la CSP, si cela est jugé nécessaire par les États membres participant à la CSP. Le FED peut financer des projets de cyberdéfense si cela est prévu dans les programmes de travail |

| Renforcer la lutte contre la criminalité et supprimer les obstacles à l'efficacité de la justice pénale dans le cyberespace | | | | | |
|---|---|---|---|---|---|
| Élaborer une feuille de route pour contrecarrer l'évolution de la criminalité sur le dark web | Europol | États membres | début 2018 | Le COSI doit approuver la feuille de route et assurer le suivi de sa mise en œuvre. | |
| Mettre en œuvre des mesures concrètes proposées par la Commission pour relever le défi du cryptage dans le contexte des procédures pénales, tout en assurant le respect des droits de l'homme et des libertés fondamentales | Commission européenne | États membres, Europol | en cours | Suivi des progrès assuré par le CATS | |

| | | | | | |
|---|---|---|---|---|---|
| Améliorer la capacité des autorités répressives et judiciaires à mener des enquêtes et à engager des poursuites en matière de criminalité | États membres | Commission européenne | | Suivi des progrès assuré par le COSI, codes de conduite volontaire avec les fournisseurs d'accès internet devant être proposés pour limiter le nombre d'abonnés derrière chaque adresse IPv4 par le déploiement d'autres technologies que la traduction d'adresses réseau à grande échelle (Carrier-Grade Network Address Translation) (États membres) La Commission européenne doit soulever la question de la constitution d'un registre des numéros de port de provenance avec les fournisseurs de contenu sur Internet dans le cadre du forum de l'UE sur Internet. | Prise en compte des recommandations du rapport final du groupe "Questions générales, y compris l'évaluation" sur la septième série d'évaluations mutuelles concernant la lutte contre la cybercriminalité |

| | | | | | |
|---|---|---|---|---|---|
| Encourager le déploiement du protocole IPv6 par le secteur privé, notamment par l'éventuelle introduction d'exigences pour les marchés publics | États membres | Commission européenne | en cours | Suivi des progrès assuré par les instances préparatoires compétentes du Conseil (groupe horizontal "Questions liées au cyberespace", COSI) | |
| Mettre au point et approuver un protocole de réaction d'urgence pour une réponse répressive coordonnée de l'UE aux cyberattaques de grande envergure | Europol | États membres, Commission européenne, SEAE, Conseil | début 2018 | Le COSI doit approuver le protocole et assurer le suivi de sa mise en œuvre. | |
| Présentation d'une proposition législative sur l'accès transfrontière aux preuves électroniques par les autorités répressives | Commission européenne | Conseil, Parlement européen | début 2018 | Suivi des progrès assuré par le CATS | |

| | | | | | |
|---|---|---|---|---|---|
| Présenter un rapport sur l'état des travaux relatifs à la mise en œuvre de mesures concrètes visant à améliorer l'accès transfrontière aux preuves électroniques (y compris en matière de coopération entre les autorités répressives et les prestataires de services du secteur privé) | Commission européenne | États membres | fin 2017 | Suivi des progrès assuré par le CATS | |
| Créer une plateforme pleinement opérationnelle permettant aux États membres d'échanger en toute sécurité des formulaires en ligne de décision d'enquête européenne, ainsi que des preuves électroniques. | Commission européenne | États membres | mi-2019 | Suivi des progrès assuré par le CATS | |

| Renforcer la coopération internationale pour un cyberespace ouvert, libre, pacifique et sûr au niveau mondial | | | | | |
|---|---|---|---|---|---|
| Poursuivre le dialogue avec les partenaires internationaux pour exercer une influence sur le soutien apporté au niveau mondial en faveur d'un cyberespace ouvert, libre, pacifique et sûr | SEAE, Conseil, Commission européenne | États membres | mi-2019 | Suivi des progrès assuré par le groupe horizontal "Questions liées au cyberespace" | |
| Mettre en place un réseau de l'UE pour le renforcement des cybercapacités et élaborer des lignes directrices de l'UE sur le renforcement des capacités en matière de cybersécurité | SEAE, Commission européenne, avec le soutien des États membres | | | | Coopération possible avec le forum mondial sur la cyberexpertise |
| Développer la coopération UE-OTAN en matière de formation et d'enseignement | SEAE, Conseil, AED | États membres | | | |
| Poursuivre la coopération UE-OTAN en ce qui concerne les exercices de cyberdéfense et partager les bonnes pratiques en matière de gestion de crises | SEAE, Conseil | États membres, AED, Commission européenne | | | |

| | | | | | |
|---|---|---|---|---|---|
| Traiter les applications des nouvelles technologies critiques en matière de cybersécurité, dans le cadre des régimes internationaux de contrôle des exportations pertinents | États membres, Commission européenne | | | | |
| Élaborer et faire connaître une position consolidée de l'UE concernant les discussions relatives à la gouvernance de l'internet | Conseil, Commission européenne, SEAE | États membres | 2018 et en cours | Le COSI doit faciliter l'adoption d'une position commune de l'UE relative à un système WHOIS conforme au règlement général sur la protection des données, qui assurera un accès rapide et en temps voulu à des données d'enregistrement fiables concernant les propriétaires des noms de domaines et des adresses IP (données WHOIS) et ce à des fins légitimes y compris en matière répressive ou pour la protection des consommateurs, la protection des droits de propriété intellectuelle et des activités de cybersécurité. | |