Conseil de
l'Union européenne

Bruxelles, le 19 novembre 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	19 novembre 2018
Destinataire:	délégations
Objet:	Cadre stratégique de cyberdéfense de l'UE (version actualisée 2018)

Les délégations trouveront en annexe le cadre stratégique de cyberdéfense de l'UE (dans sa version actualisée en 2018), adoptée par le Conseil lors de sa 3652e session, tenue le 19 novembre 2018.

ANNEXE

CADRE STRATÉGIQUE DE CYBERDÉFENSE DE L'UE

(DANS SA VERSION ACTUALISEE EN 2018)

Champ d'application et objectifs

Pour être en mesure de répondre aux défis qui ne cessent d'évoluer dans le domaine de la sécurité, l'UE et ses États membres doivent renforcer la cyber-résilience et mettre en place des capacités solides en matière de cybersécurité et de cyberdéfense.

Le cadre stratégique de cyberdéfense de l'UE (cadre stratégique de cyberdéfense) contribue au renforcement des capacités des États membres de l'UE en matière de cyberdéfense ainsi qu'au renforcement de la cyberprotection de l'infrastructure de sécurité et de défense de l'UE, sans préjudice de la législation des États membres et de celle de l'UE, y compris, lorsqu'il est défini, du champ d'application de la cyberdéfense.

Le cyberespace constitue le cinquième domaine d'opérations, parallèlement aux domaines terrestre, maritime, aérien et spatial: le succès de la mise en œuvre des missions et opérations de l'UE est de plus en plus tributaire d'un accès ininterrompu à un cyberespace sécurisé, ce qui nécessite donc des capacités opérationnelles solides et résilientes dans le domaine cyber.

Le cadre stratégique de cyberdéfense actualisé a pour objectif de développer la politique de l'UE en la matière, compte tenu des évolutions dans les autres cadres de discussion et domaines d'action pertinents ainsi que de la mise en œuvre du cadre stratégique de cyberdéfense depuis 2014. Il recense les domaines prioritaires pour la cyberdéfense et clarifie les rôles des différents acteurs européens, tout en respectant pleinement les responsabilités et les compétences des acteurs de l'Union et des États membres ainsi que le cadre institutionnel de l'UE et son autonomie décisionnelle.

Contexte

Les conclusions du Conseil européen sur la PSDC de décembre 2013 ainsi que les conclusions du Conseil sur la PSDC de novembre 2013 ont préconisé de définir un cadre stratégique de cyberdéfense de l'UE, sur la base d'une proposition élaborée par la haute représentante, en coopération avec la Commission européenne et l'Agence européenne de défense (AED). Le cadre stratégique de cyberdéfense de l'UE a été adopté par le Conseil le 18 novembre 2014[1] et, depuis cette date, sa mise en œuvre s'est accompagnée de contributions concrètes qui ont permis de renforcer considérablement les capacités de cyberdéfense des États membres. Dans le contexte du rapport annuel 2017 sur la mise en œuvre du cadre stratégique de cyberdéfense de l'UE[2], et compte tenu des initiatives lancées par l'UE dans le domaine de la sécurité et de la défense, notamment l'examen annuel coordonné en matière de défense (EACD), la coopération structurée permanente (CSP), le Fonds européen de la défense et le pacte en matière de PSDC civile, ainsi que le plan de développement des capacités dans sa version révisée de 2018 et le plan de développement des capacités civiles, les États membres ont demandé que le cadre stratégique de cyberdéfense de l'UE soit actualisé.

La cybersécurité est une priorité s'inscrivant dans le cadre tant de la stratégie globale pour la politique étrangère et de sécurité de l'UE que du niveau d'ambition de l'UE[3]. La stratégie globale insiste sur la nécessité de renforcer les capacités afin de protéger l'UE et ses citoyens et de réagir en cas de crises extérieures. Elle souligne aussi qu'il est indispensable de renforcer l'UE en tant que communauté de sécurité. Dans ce contexte, l'action menée en faveur de la sécurité et de la défense devrait aussi renforcer le rôle stratégique de l'UE et sa capacité à agir de manière autonome lorsque cela est nécessaire et avec des partenaires chaque fois que cela est possible. Ces objectifs supposent une coopération plus étroite dans le renforcement des capacités, ce qui contribuera à l'efficacité et à l'interopérabilité des capacités civiles et militaires qui en résulteront.

---

1 Document 15585/14 du Conseil du 18.11.2014.
2 Document 15870/17 du Conseil du 19.12.2017.
3 Conclusions du Conseil sur la mise en œuvre de la stratégie globale de l'UE dans le domaine de la sécurité et de la défense, du 14.11.2016.

L'ensemble commun de propositions pour la mise en œuvre de la déclaration commune signée à Varsovie le 8 juillet 2016 par le président du Conseil européen, le président de la Commission européenne et le secrétaire général de l'Organisation du Traité de l'Atlantique Nord[4] prévoit des actions concrètes visant à élargir la coopération entre l'UE et l'OTAN dans le domaine de la cybersécurité et de la cyberdéfense, notamment dans le contexte des missions et opérations, ainsi que dans le cadre du renforcement des capacités de cyberdéfense, de la recherche et de la technologie, de la formation, de l'éducation et des exercices, et lorsqu'il s'agit d'intégrer les aspects relatifs à la cybersécurité dans les mécanismes de gestion des crises. Cette coopération se déroule dans le plein respect des principes d'ouverture, de transparence, d'inclusion, de réciprocité et d'autonomie décisionnelle de l'UE. Signé en février 2016, un arrangement technique entre l'équipe d'intervention en cas d'urgence informatique de l'UE (CERT-UE) et la capacité OTAN de réaction aux incidents informatiques (NCIRC) facilite le partage d'informations techniques afin d'améliorer la prévention et la détection des cyberincidents ainsi que la réaction face à ceux-ci dans les deux organisations.

Il convient de rappeler que plusieurs politiques de l'UE contribuent aux objectifs de la politique de cyberdéfense exposée dans le présent document, le présent cadre prenant aussi en considération les réglementations, les politiques et le support technologique dans le domaine civil. Par exemple, le Parlement européen et le Conseil ont adopté en juillet 2016 la directive sur la sécurité des réseaux et des systèmes d'information[5] (SRI), qui améliorera l'état général de préparation des États membres pour lutter contre les cybermenaces et renforcera la coopération à l'échelle de l'UE. Cette directive établit des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur. La date limite de transposition de la directive était fixée au 9 mai 2018.

---

4 Conclusions du Conseil sur la mise en œuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du Traité de l'Atlantique Nord (6 décembre 2016, doc. 15283/16; 5 décembre 2017, doc. 14802/17).

5 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

L'acte législatif sur la cybersécurité de l'UE, proposé en septembre 2017, comprend le nouveau mandat de l'Agence de l'UE pour la cybersécurité (ENISA) et prévoit l'établissement d'un cadre de certification à l'échelle de l'UE. Une fois en place, ce cadre de certification devrait favoriser des normes élevées pour les processus, produits et services TIC, être une source d'avantage concurrentiel et renforcer la confiance chez les consommateurs et les acheteurs. En septembre 2017 également, la Commission a pris une autre mesure pour préparer l'UE à faire face à des incidents de cybersécurité transfrontières de grande envergure (le "plan") et elle travaille maintenant, en collaboration avec les États membres et d'autres institutions, agences et organes, à la mise en place d'une coopération européenne concernant les crises de cybersécurité, en établissant la mise en œuvre pratique et la documentation relative à tous les acteurs, processus et procédures pertinents dans le cadre des mécanismes de l'UE existants pour la gestion des crises et des catastrophes, en particulier le dispositif intégré pour une réaction au niveau politique dans les situations de crise.

Les conclusions du Conseil de novembre 2016 intitulées "Renforcer le système européen de cyber-résilience" insistent sur l'objectif commun de contribuer à l'autonomie stratégique de l'Europe, comme indiqué dans les conclusions du Conseil de novembre 2016 sur la stratégie globale de l'UE concernant les questions de politique étrangère et de sécurité, y compris dans le cyberespace. Le Conseil européen a réaffirmé ce message en juin 2018 et il a également souligné la nécessité de renforcer les capacités de lutte contre les menaces sur la cybersécurité qui proviennent de l'extérieur de l'UE.

En 2017, le Conseil a adopté un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")[6]. Ce cadre devrait encourager la coopération, faciliter la réduction des menaces et influencer le comportement d'agresseurs potentiels à long terme. Il s'appuie sur des mesures PESC, y compris les mesures restrictives, dans le but de prévenir les actes de cybermalveillance et d'y répondre. Les auteurs d'actes de cybermalveillance doivent rendre des comptes et les États membres de l'UE sont encouragés à développer leurs capacités de réaction face à de tels actes, de manière coordonnée conformément à la boîte à outils cyberdiplomatique. Les États ne devraient pas mener ou soutenir sciemment des activités informatiques contraires aux obligations qui leur incombent en vertu du droit international, et ils ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et de la communication.

Une communication conjointe[7] sur les questions liées au cyberespace a été présentée par la Commission et la HR/VP en septembre 2017, l'objectif étant d'atténuer les risques découlant de la nouvelle nature des menaces. Elle fait de la cyberdéfense l'un des principaux domaines d'action et le cadre stratégique de cyberdéfense est l'un des piliers sur lesquels repose sa mise en œuvre concrète[8].

Dans ses conclusions de novembre 2017 sur les questions liées au cyberespace, le Conseil s'est déclaré conscient de l'accroissement des liens entre cybersécurité et cyberdéfense et a demandé une intensification de la coopération en matière de cyberdéfense, notamment en encourageant la coopération entre acteurs civils et militaires en cas d'incident. Il y soulignait aussi qu'un cyberincident ou une crise de cybersécurité de nature particulièrement grave pourrait constituer un motif suffisant pour qu'un État membre invoque la clause de solidarité de l'UE et/ou la clause d'assistance mutuelle.

---

6 Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique"), doc. 9916/17 du 7 juin 2017

7 Communication conjointe au Parlement européen et au Conseil intitulée "Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide" (13 septembre 2017, doc. JOIN(2017) 450 final).

8 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 (20 novembre 2017, doc. 14435/17).

Le 11 décembre 2017, la coopération structurée permanente (CSP) a été lancée. Ce cadre de coopération ambitieux, contraignant et inclusif été mis en place entre 25 États membres et comporte un engagement à accroître les efforts de coopération concernant la cyberdéfense, ainsi que les projets CSP qui y sont liés. La première série de projets CSP recensés par les États membres participants en 2017 comprend deux projets liés à la cyberdéfense: "équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité" et "plateforme de partage d'informations en matière de réaction aux menaces et incidents informatiques". De nouvelles séries de projets CSP sont prévues. La CSP développera les capacités de cyberdéfense et, partant, renforcera la coopération entre les États membres et l'interopérabilité.

Dans la version actualisée du plan de développement des capacités de l'UE (PDC), qui a été approuvée par le comité directeur de l'AED en juin 2018, la cyberdéfense est considérée comme un élément essentiel; il y est fait état de la nécessité de prévoir des cyberopérations défensives dans tous les contextes opérationnels, sur la base d'une appréciation de la situation actuelle et prévisionnelle poussée en matière de cyberespace, y compris la capacité de combiner des quantités importantes de données et de renseignements provenant de nombreuses sources afin de contribuer à une prise de décision rapide et à une automatisation accrue de la collecte et de l'analyse de données ainsi que du processus d'aide à la décision. Le PDC de 2018 définit des priorités en matière de capacités de cyberdéfense dans les domaines suivants: coopération et synergies avec les acteurs concernés dans les domaines de la cyberdéfense et de la cybersécurité; activités de recherche et technologie en matière de cyberdéfense; cadres pour l'ingénierie des systèmes applicables aux cyberopérations; éducation, entraînement, exercices et évaluation (ETEE); défis en matière de cyberdéfense sur le plan aérien, spatial, maritime et terrestre.

Enfin, au cours des dernières années, la nécessité pour la communauté internationale de prévenir les conflits, coopérer et stabiliser le cyberespace est devenue évidente. L'UE promeut, en étroite coopération avec d'autres organisations internationales, en particulier les Nations unies, l'OSCE et le Forum régional de l'ANASE, un cadre stratégique pour la prévention des conflits, la coopération et la stabilité dans le cyberespace, qui comprend i) l'application du droit international, en particulier la charte des Nations unies dans son intégralité, dans le cyberespace; ii) le respect de normes, règles et principes non contraignants sur le comportement responsable des États; iii) l'élaboration et la mise en œuvre de mesures de confiance au niveau régional. Le cadre stratégique de cyberdéfense devrait également appuyer cet effort.

Priorités

Six domaines prioritaires ont été définis dans la version actualisée du cadre stratégique de cyberdéfense, qui est principalement axé sur le développement des capacités de cyberdéfense, ainsi que sur la protection des réseaux de communication et d'information de la PSDC de l'Union. Parmi les autres domaines prioritaires figurent la formation et les exercices, la recherche et technologie, la coopération civilo-militaire et la coopération internationale. Dans le domaine de la formation, l'accent est mis sur le renforcement de la formation des États membres à la cyberdéfense et à la sensibilisation de la chaîne de commandement de la PSDC dans le domaine du cyber. Par ailleurs, il est important que la dimension cyber soit dûment prise en compte dans les exercices afin d'améliorer la capacité de l'UE à réagir aux crises dans le domaine de la cybersécurité et aux crises hybrides par l'amélioration des procédures décisionnelles et de la disponibilité de l'information. Le cyberespace évolue rapidement et les nouveaux développements technologiques doivent être soutenus, dans les domaines aussi bien civil et militaire. La coopération civilo-militaire dans le domaine cyber est essentielle pour faire face aux cybermenaces de manière cohérente. Dernier point, mais non le moindre, le renforcement de la coopération avec les partenaires internationaux pourrait contribuer à renforcer la cybersécurité dans l'Union européenne et au-delà, et à promouvoir les principes et les valeurs de l'Union.

Le présent cadre présente des propositions et des possibilités de coordination entre les institutions, organes et agences concernés de l'UE. Il tient également compte du rôle important que joue le secteur privé pour la mise au point de technologies en matière de cybersécurité et de cyberdéfense.

En outre, le cadre stratégique de cyberdéfense soutient l'intégration de la cyberdéfense dans les mécanismes de gestion de crises de l'Union lorsque, pour faire face aux conséquences d'une crise dans le domaine de la cybersécurité, les dispositions pertinentes du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne[9] peuvent être applicables.

1. Soutenir le développement des capacités de cyberdéfense des États membres

Le développement des capacités et des technologies de cyberdéfense devrait prendre en compte tous les aspects du développement des capacités, y compris la doctrine, la direction, l'organisation, le personnel, la formation, l'industrie, la technologie, l'infrastructure, la logistique et l'interopérabilité. À cette fin, les États membres devraient renforcer leurs efforts pour assurer l'efficacité des capacités de cyberdéfense. Le SEAE, la Commission et l'AED devraient coopérer et soutenir ces efforts.

Il est nécessaire d'évaluer en permanence les vulnérabilités des infrastructures d'information qui soutiennent les missions et opérations PSDC, et de mesurer en temps quasi réel l'efficacité de la protection. D'un point de vue opérationnel, les activités de cyberdéfense viseront principalement à maintenir la disponibilité, l'intégrité et la confidentialité des réseaux de communication et d'information de la PSDC, sauf indication contraire dans le mandat des opérations ou des missions. En outre, le SEAE, en coopération avec les États membres, intégrera davantage les cybercapacités dans les missions et opérations PSDC.

Les auteurs d'actes de cybermalveillance doivent avoir à répondre de leurs actes. Il est important que les États membres, avec le soutien du SEAE, favorisent la coopération mutuelle pour faire face aux actes de ce type. La boîte à outils cyberdiplomatique est conçue pour contribuer à mettre en place cette réponse mutuelle. Le SEAE et l'AED organiseront périodiquement des exercices sur la base de la boîte à outils cyberdiplomatique, au cours desquels les États membres pourront s'y exercer.

---

[9] Article 222 du TFUE et article 42, paragraphe 7, du TUE, en tenant dûment compte de l'article 17 du TUE.

Compte tenu du fait que, dans la législation nationale des États membres, ainsi que dans celle de l'UE, le champ d'application de la cyberdéfense est large et diversifié, lorsqu'il est défini, il est nécessaire d'élaborer une conception commune agrégée dudit champ d'application.

Les opérations militaires PSDC reposant sur une infrastructure de commandement, de contrôle, de communications et informatique (C4) fournie par les États membres, un certain degré de convergence stratégique est nécessaire lors de la planification des besoins en matière de cyberdéfense pour l'infrastructure d'information.

S'appuyant sur les travaux de l'équipe chargée du projet de cyberdéfense de l'AED visant à développer les capacités de cyberdéfense, l'AED et les États membres:

- utiliseront le PDC et d'autres instruments, tels que l'EACD, qui facilitent et soutiennent la coopération entre les États membres afin d'améliorer le degré de convergence dans la planification de leurs besoins en matière de cyberdéfense au niveau stratégique, notamment en ce qui concerne le suivi, l'appréciation de la situation, la prévention, la détection et la protection, le partage d'informations, la criminalistique et la capacité d'analyse des logiciels malveillants, les enseignements tirés, la réduction des dommages, les capacités de récupération dynamique, le stockage de données distribuées et les sauvegardes de données;
- soutiendront projets actuels et futurs de mise en commun et de partage en matière de cyberdéfense dans le cadre d'opérations militaires (par exemple, en matière de criminalistique, d'interopérabilité et de fixation de normes);
- élaboreront un ensemble normalisé d'objectifs et d'exigences définissant le niveau minimum de cybersécurité et de confiance que devront atteindre les États membres, en s'appuyant sur l'expérience acquise à l'échelle de l'UE.

Le SEAE et l'AED:

- faciliteront les échanges entre les États membres sur les doctrines nationales dans le domaine de la cyberdéfense ainsi que sur les programmes de recrutement, de rétention et de réservistes axés sur la cyberdéfense.

L'AED:

- étudiera, dans la législation et les meilleures pratiques des États membres, les différents champs d'application des besoins militaires dans le domaine de la cyberdéfense. Cette étude aura pour principal objectif de mettre au point une architecture d'entreprise pour la cyberdéfense, en vue d'y inclure le champ d'application, les fonctionnalités et les exigences utilisés dans ce domaine dans le cadre de la législation des États membres et de l'UE.

Sur une base volontaire, les États membres:

- amélioreront la coopération entre leurs CERT militaires en vue d'améliorer la prévention et le traitement des incidents;
- tireront parti de la CSP afin de renforcer encore la coopération en matière de cyberdéfense, y compris de nouveaux projets;
- tireront parti du Fonds européen de la défense afin de développer conjointement les capacités de cyberdéfense;
- élaboreront une conception commune de l'application de la clause d'assistance mutuelle dans le domaine du cyberespace, tout en préservant sa souplesse;
- établiront des exigences de base en matière de cyberdéfense pour les infrastructures d'information;
- dans la mesure où l'amélioration des capacités de cyberdéfense dépend de l'expertise civile en matière de sécurité des réseaux et de l'information, mettront à profit l'expertise que possèdent l'ENISA, les autorités des États membres réunies au sein du groupe de coopération SRI ainsi que d'éventuelles autres entités au niveau de l'UE disposant d'une expertise civile en matière de cybersécurité.

Les États membres, le SEAE/État-major de l'UE, le CESD et l'AED:

- envisageront de mettre au point une formation à la cyberdéfense, en vue d'une certification des groupements tactiques de l'UE.

La Commission, en coopération avec les États membres:

- tiendront compte de la cyberdéfense dans les programmes de travail du programme européen de développement industriel dans le domaine de la défense et du Fonds européen de la défense.

2. Renforcer la protection des systèmes d'information et de communication PSDC utilisés par les entités de l'UE

Sans préjudice du rôle de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-EU) en tant que structure centrale de coordination de la réponse de l'UE aux incidents dans le domaine de la cybersécurité pour l'ensemble des institutions, organes et agences de l'Union et dans le cadre des règles pertinentes concernant le budget de l'Union, le SEAE élaborera une analyse adéquate et autonome des questions de sécurité et de défense des réseaux et mettra au point sa propre capacité de sécurité informatique. Il s'attachera à améliorer la résilience de ses réseaux PSDC, en mettant l'accent sur les mécanismes de prévention, de détection, de réponse aux incidents, d'appréciation de la situation, d'échange d'informations et d'alerte rapide.

La protection des systèmes de communication et d'information du SEAE et le développement des capacités de sécurité informatique sont placés sous la direction de la direction générale Budget et administration du SEAE (DG BA). Des ressources et un soutien supplémentaires seront fournis par l'état-major de l'Union européenne (EMUE), la direction "Gestion des crises et planification" (CMPD) et la capacité civile de planification et de conduite (CPCC). Cette capacité de sécurité informatique couvrira à la fois les systèmes classifiés et les systèmes non classifiés et fera partie intégrante des entités opérationnelles existantes.

Il faut également rationaliser les règles de sécurité pour les systèmes informatiques fournis par les différents acteurs institutionnels de l'UE au cours des opérations et des missions PSDC. Dans ce contexte, une chaîne de commandement unifiée pourrait être envisagée en vue d'améliorer la résilience des réseaux utilisés pour la PSDC.

Afin de renforcer la coordination et d'accroître la protection et la résilience des réseaux et systèmes d'information et de communication PSDC, un conseil interne de cybergouvernance, placé sous l'autorité de la secrétaire générale du SEAE, a été créé en 2017.

La DG BA/SEAE:

- renforcera la capacité de sécurité informatique au sein du SEAE, sur la base de la capacité et des procédures techniques existantes, en mettant l'accent sur la prévention, la détection, la réponse aux incidents, l'appréciation de la situation, l'échange d'informations et un mécanisme d'alerte rapide. Une stratégie de coopération avec la CERT-EU et les capacités existantes de l'UE en matière de cybersécurité sera renforcée;

La DG BA/SEAE, en collaboration avec l'EMUE, la MPCC, la CMPE et la CPCC:

- élaborera une politique et des lignes directrices cohérentes en matière de sécurité informatique, en tenant également compte des exigences techniques pour la cyberdéfense dans le cadre des structures, missions et opérations PSDC, en gardant à l'esprit les cadres et politiques de coopération existants au sein de l'UE en vue d'assurer une convergence des règles, des politiques et de l'organisation;

La capacité unique d'analyse du renseignement (SIAC)/SEAE:

- sur la base des structures existantes, renforcera sa capacité d'évaluation de la cybermenace et de renseignement en la matière afin de recenser de nouveaux cyber-risques et fournira des évaluations régulières des risques basées sur l'analyse stratégique de la menace et des informations sur les incidents en temps quasi réel, coordonnées entre les structures pertinentes de l'UE et accessibles à différents niveaux de classification;

La SIAC/SEAE et la CERT-UE:

- encourageront le partage d'informations en temps réel sur la cybermenace entre les États membres et les entités pertinentes de l'UE. À cette fin, des mécanismes de partage d'informations et des mesures destinées à instaurer un climat de confiance seront élaborés entre les autorités nationales et européennes compétentes, selon une approche volontaire qui s'appuiera sur la coopération existante;

L'EMUE/SEAE et la MPCC:

- continueront à développer un concept sur la cyberdéfense pour les opérations et missions militaires PSDC, qu'ils intégreront dans la planification au niveau stratégique;
- élaboreront, en coopération avec l'état-major d'opération, des instructions permanentes dans le domaine cyber au niveau d'opérations génériques.

La CPCC/SEAE et la CMPD:

- continueront à développer un concept sur la cyberdéfense pour les missions civiles PSDC, qu'ils intégreront dans la planification stratégique;
- renforceront les capacités de cyberdéfense des missions civiles PSDC en s'appuyant sur l'infrastructure existante et en encourageant la normalisation et l'harmonisation des technologies utilisées dans le cadre des missions et opérations PSDC, et ce, lorsqu'il y a lieu, en puisant dans l'expertise de la CERT-UE, de l'ENISA et de l'AED;
- dans le cadre du processus de renforcement de la PSDC civile, étudieront plus en détail l'appui que pourraient éventuellement apporter les missions civiles PSDC aux pays hôtes en matière de cybersécurité.

Le SEAE:

- continuera à développer des exigences communes pour les missions et opérations militaires et civiles PSDC;
- renforcera la coordination de la cyberdéfense afin de mettre en œuvre les objectifs liés à la protection des réseaux utilisés par les acteurs institutionnels de l'UE soutenant la PSDC, en s'appuyant sur les expériences existantes à l'échelle de l'UE;
- réexaminera régulièrement les besoins en ressources et les autres décisions politiques pertinentes sur la base de l'évolution du contexte de la menace, en consultation avec les États membres et les autres institutions de l'UE;

3. Promotion de la coopération civilo-militaire

Le cyberespace évolue rapidement: les développements technologiques doivent être étayés par des systèmes de sécurité, dans les domaines aussi bien civil que militaire. Dans la mesure du possible, il conviendrait de prévoir une coordination entre les domaines civil et militaire dans les cas où des développements technologiques similaires offrent des solutions pour des applications aussi bien civiles que militaires. Dans d'autres cas, la spécificité des capacités militaires et des systèmes d'armes est telle qu'aucun échange n'est possible avec les technologies civiles. Sans préjudice de l'organisation et de la législation internes des États membres, la coopération civilo-militaire dans le domaine du cyberespace peut être envisagée notamment pour l'échange des meilleures pratiques, des mécanismes d'échange d'informations et d'alerte rapide, des évaluations des risques en matière de réponses aux incidents et une meilleure sensibilisation, ainsi qu'à des fins de formation et d'exercices.

L'amélioration de la cybersécurité civile est un facteur important qui contribue à la résilience globale de la sécurité des réseaux et de l'information. La directive SRI accroît le degré de préparation au niveau national, et renforce la coopération à l'échelle de l'Union entre les États membres au niveau tant stratégique qu'opérationnel. Cette coopération associe les autorités nationales qui supervisent les politiques sur la cybersécurité ainsi que les CERT nationales et la CERT-EU. La coopération entre les CERT civiles et militaires devrait être renforcée compte tenu de ces développements. Le nouveau règlement européen sur la cybersécurité vise à améliorer la résilience européenne face aux cyberattaques et à proposer un cadre de certification en matière de cybersécurité pour les produits et les services, renforçant ainsi la confiance à l'égard de l'environnement numérique civil.

L'AED, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), le Centre européen de lutte contre la cybercriminalité (EC3) et la CERT-UE, mais aussi d'autres agences et organismes compétents de l'UE, dans le cadre de leur mandat respectif et dans le respect des compétences des États membres, ainsi que les États membres sont encouragés à renforcer encore leur coopération dans les domaines suivants:

- élaborer des profils communs de compétences sur la cybersécurité et la cyberdéfense sur la base des meilleures pratiques internationales et de la certification utilisée par les institutions, organes et agences de l'UE, en tenant compte également des normes de certification du secteur privé;
- contribuer à développer et à adapter les normes organisationnelles et techniques en matière de cybersécurité et de défense du secteur public pour les utiliser dans le secteur de la défense et de la sécurité. Si nécessaire, s'appuyer sur les travaux en cours de l'ENISA et de l'AED;
- établir ou continuer à développer des mécanismes et des dispositifs de travail pour échanger les meilleures pratiques, notamment en matière d'éducation, de formation et d'exercices, mais aussi de recherche et de technologie, ainsi que dans d'autres domaines offrant des possibilités de synergies civilo-militaires;
- tirer parti de l'expérience existante de l'UE en matière de prévention, d'enquête et de criminalistique concernant la cybercriminalité et de leur utilisation accrue dans le développement des capacités de cyberdéfense;

Sur une base volontaire, les États membres:

- renforceront leur coopération entre CERT civiles et militaires.

Le SEAE, la Commission et les États membres:

- incluront la cyberdéfense dans les procédures de l'UE en matière de gestion des crises et des catastrophes (par le processus d'élaboration de plans en la matière).

4. Recherche et technologie

Les exploitants d'infrastructures et de services de technologie de l'information et de la communication (TIC) à des fins civiles et militaires sont confrontés à des défis similaires en matière de cybersécurité, étant donné qu'ils ont des exigences communes en matière de technologie et de capacité opérationnelle. Les besoins communs en matière de recherche et de technologie (R&T) et les exigences communes des systèmes sont anticipés afin d'améliorer l'interopérabilité à long terme de ces systèmes et de réduire les coûts liés à l'élaboration de solutions. Il est nécessaire de réaliser des économies d'échelle afin de faire face au nombre sans cesse croissant de menaces et de vulnérabilités, ce qui devrait permettre de faciliter le maintien et la croissance d'un secteur de la cyberdéfense compétitif en Europe.

La R&T constitue une dimension importante du développement des capacités de cyberdéfense. Dans le contexte du programme de recherche dans le domaine de la cyberdéfense, l'AED a fourni une base solide pour l'établissement d'un ordre de priorités concernant le financement futur de la R&T au sein du cadre intergouvernemental. Le programme de recherche stratégique ultérieur élaboré au sein du groupe de travail ad hoc compétent de l'AED prévoit l'établissement d'un ordre de priorités étayé en ce qui concerne les technologies relatives au cyberespace qui sont nécessaires pour le domaine militaire, tout en recensant des possibilités d'actions et d'investissements dans le domaine des technologies à double usage, que cela soit dans le contexte d'un financement au niveau national, multinational ou de l'UE.

Il est essentiel de développer des capacités technologiques en Europe pour atténuer les menaces et les vulnérabilités. L'industrie restera le principal moteur de la technologie et de l'innovation liées à la cyberdéfense. La cryptographie, les systèmes intégrés sécurisés, la détection de logiciels malveillants, les techniques de simulation et de visualisation, la protection des systèmes de réseau et de communication et les technologies d'identification et d'authentification figurent au nombre des domaines sur lesquels il est nécessaire de se pencher. Il est également important de promouvoir en Europe une chaîne d'approvisionnement industrielle compétitive dans le domaine de la cybersécurité en contribuant à la participation des petites et moyennes entreprises (PME).

La capacité de l'Europe à faire face à la concurrence internationale en ce qui concerne les capacités dans le domaine de la cybertechnologie dépend également de notre capacité à stimuler l'innovation radicale, au moyen d'instruments nationaux et de l'UE, tels que le Conseil européen de l'innovation.

Afin de faciliter la coopération civilo-militaire destinée à développer les capacités de cyberdéfense, de renforcer la base industrielle et technologique de défense européenne[10] et de contribuer à l'autonomie stratégique de l'UE dans le domaine du cyberespace également, lorsque cela est nécessaire et avec des partenaires chaque fois que cela est possible,

l'AED, la Commission et les États membres:

- rechercheront des synergies entre les efforts de R&T déployés dans le secteur militaire et les programmes de recherche et développement civils, en particulier ceux qui concernent les innovations radicales, et tiendront compte du volet "cybersécurité et cyberdéfense" lors de la mise en œuvre de l'action préparatoire concernant la recherche dans le domaine de la défense;
- diffuseront les programmes de recherche dans le domaine de la cybersécurité (tels que le programme de recherche stratégique sur la cybersécurité de l'AED), ainsi que les feuilles de route et les actions qui en découlent; à cette fin, un programme de recherche transsectoriel dans le domaine de la cyberdéfense sera élaboré, en coopération étroite avec la Commission et les États membres;
- contribueront à améliorer l'intégration de la cybersécurité et de la cyberdéfense dans les programmes qui comportent un volet sécurité et technologies de défense à double usage, tels que le programme de recherche sur la gestion du trafic aérien dans le ciel unique européen (SESAR);

[10] Communication intitulée "Vers un secteur de la défense et de la sécurité plus compétitif et plus efficace", COM (2013) 542.

la Commission:

- envisagera la création d'un centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité associé à un réseau de centres nationaux de coordination afin de soutenir les capacités technologiques et industrielles dans le domaine de la cybersécurité et de renforcer la compétitivité du secteur de la cybersécurité de l'Union, en assurant la complémentarité et en évitant les doubles emplois au sein du réseau de centres de compétences en matière de cybersécurité et avec d'autres agences de l'UE. Ce centre devrait, entre autres, permettre de renforcer la coopération entre les technologies et les applications civiles et de défense, en collaboration étroite et en pleine complémentarité avec l'AED dans le domaine de la cyberdéfense;
- contribuera à la création d'écosystèmes industriels et de pôles d'innovation couvrant l'ensemble de la chaîne de valeur dans le domaine de la sécurité en s'appuyant sur les connaissances universitaires, l'innovation dans les PME et la production industrielle;

la Commission, en coopération avec les États membres:

- prendra en compte les questions liées à la cyberdéfense dans les appels à propositions relatifs à l'action préparatoire concernant la recherche dans le domaine de la défense;
- intégrera la cyberdéfense dans les questions devant être prises en compte dans le cadre du Fonds européen de la défense;
- contribuera à la cohérence des politiques de l'UE afin que les aspects stratégiques et techniques de la cyberprotection par l'UE demeurent au premier plan de l'innovation dans le domaine de la technologie et soient harmonisés dans l'ensemble de l'UE (analyse et capacité d'évaluation de la cybermenace, initiatives "sécurité dès la conception", gestion de la dépendance pour l'accès à la technologie, etc.).

5. Améliorer les possibilités d'éducation, de formation et d'exercices

Afin de mieux se préparer à faire face aux cybermenaces et de créer une culture commune de la cyberdéfense dans l'ensemble de l'UE, qui bénéficie également aux missions et opérations de l'UE, il est nécessaire d'améliorer et d'élargir les possibilités de formation en matière de cyberdéfense. Il est essentiel que les budgets dans le domaine de l'éducation et de la formation soient utilisés efficacement, tout en offrant la meilleure qualité possible. Il sera primordial de mutualiser et de mettre en commun au niveau européen les activités d'éducation et de formation en matière de cyberdéfense.

Le Collège européen de sécurité et de défense (CESD), le SEAE, l'AED, la Commission et les États membres:

- sur la base de l'analyse, par l'AED, des besoins de formation en matière de cyberdéfense et de l'expérience acquise dans le cadre des activités de formation à la cybersécurité proposées par le CESD, mettront au point des activités de formation et d'éducation dans le domaine de la PSDC destinées à différents publics, y compris le SEAE, le personnel des missions et opérations PSDC et les fonctionnaires des États membres, qui devraient également permettre de remédier aux problèmes de fidélisation de personnel qualifié à court, moyen et long terme;
- proposeront l'instauration d'un dialogue dans le domaine de la cyberdéfense, portant sur les normes de formation et sur la certification, avec les États membres, les institutions de l'UE, les pays tiers et d'autres organisations internationales, ainsi qu'avec le secteur privé;
- coopéreront avec des organismes européens de formation du secteur privé, ainsi qu'avec des établissements universitaires, afin d'améliorer les compétences et aptitudes du personnel participant aux missions et opérations PSDC.

Le CESD:

- continuera à développer la plateforme de formation, d'entraînement, d'exercices et d'évaluation dans le domaine du cyber mise en place en son sein (plateforme ETEE dans le domaine du cyber);
- créera des synergies avec les programmes de formation d'autres parties prenantes telles que l'ENISA, Europol, l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) et le Centre coopératif d'excellence pour la cyberdéfense de l'OTAN;
- explorera la possibilité de mettre en place des programmes de formation à la cyberdéfense organisés conjointement par le CESD et l'OTAN, qui soient ouverts à tous les États membres de l'UE, afin de favoriser une culture commune de la cyberdéfense.

La Commission:

- examinera les moyens d'élargir les possibilités de formation et d'éducation dans les États membres mis en évidence par la plateforme ETEE dans le domaine du cyber.

L'AED:

- mettra au point d'autres cours de l'AED, en collaboration avec le CESD, pour répondre aux besoins des États membres en matière d'éducation, de formation et d'exercices dans le domaine de la cyberdéfense;
- soutiendra la plateforme ETEE dans le domaine du cyber notamment en intégrant progressivement des modules de formation, d'entraînement, d'exercices et d'évaluation dans le domaine du cyber élaborés dans le cadre de l'AED.

Le SEAE et les États membres:

- assureront le suivi des mécanismes de certification établis par le CESD pour les programmes de formation, en étroite coopération avec les services compétents des institutions, organes et agences de l'UE, sur la base des normes et connaissances existantes; envisageront la possibilité de créer des modules spécialisés sur le cyberespace dans le cadre de l'initiative "Erasmus militaire".

Il est nécessaire d'améliorer les possibilités d'exercices dans le domaine de la cyberdéfense pour les acteurs militaires et civils de la PSDC. Les exercices conjoints servent à développer des connaissances et une compréhension communes de la cyberdéfense. Ainsi, les forces nationales seront mieux préparées à intervenir dans un environnement multinational. En outre, la conduite d'exercices communs en matière de cyberdéfense renforcera l'interopérabilité et la confiance.

Le SEAE, l'AED, la CERT-UE et les États membres s'attacheront à promouvoir les éléments liés à la cyberdéfense dans les exercices relevant de la PSDC et d'autres exercices:

- intégrer la cyberdéfense dans les scénarios d'exercice existants pour *MILEX* et *MULTILAYER*;
- organiser régulièrement des exercices au niveau stratégique/politique tels que *CYBRID 2017* en coordination avec l'exercice parallèle et coordonné (PACE) conduit par l'UE, et des exercices technico-opérationnels tels que *DEFNET*;
- mettre au point, le cas échéant, un exercice spécialisé de cyberdéfense dans le cadre de la PSDC de l'UE et envisager une éventuelle coordination avec des exercices paneuropéens en la matière, tels que l'exercice "*CyberEurope*" organisé par l'ENISA;
- continuer de participer à d'autres exercices de cyberdéfense multinationaux, tels que *Locked Shields*;
- inviter des partenaires internationaux pertinents, comme l'OTAN, à participer aux exercices, dans le respect du cadre stratégique mis en place par l'UE pour les exercices;
- organiser régulièrement des exercices en s'appuyant sur la boîte à outils cyberdiplomatique, dans lesquels les États membres de l'UE peuvent s'entraîner à réagir face à des cas de cybermalveillance.

6. Renforcer la coopération avec les partenaires internationaux concernés

Dans le cadre de la coopération internationale, il est nécessaire de mener un dialogue avec les partenaires internationaux, en particulier l'OTAN et d'autres organisations internationales, afin de contribuer à la mise en place de capacités efficaces en matière de cyberdéfense. Il conviendrait de s'attacher à participer davantage aux activités en cours dans le cadre de l'Organisation pour la sécurité et la coopération en Europe (OSCE) et des Nations unies, dans la perspective de proposer un cadre stratégique pour la prévention des conflits, la coopération et la stabilité dans le cyberespace.

Il y a au sein de l'UE une volonté politique de coopérer plus étroitement avec l'OTAN dans le domaine de la cyberdéfense afin de développer des capacités de cyberdéfense solides et résilientes, comme le demande la déclaration commune signée à Varsovie le 8 juillet 2016 par le président du Conseil européen, le président de la Commission européenne et le secrétaire général de l'Organisation du Traité de l'Atlantique Nord. Des concertations régulières entre les services de ces organisations, des réunions d'information interinstitutionnelles ainsi que d'éventuelles réunions entre le Groupe politico-militaire et les comités compétents de l'OTAN aideront à éviter d'inutiles doubles emplois et à assurer la cohérence et la complémentarité des efforts déployés, conformément au cadre susmentionné.

Le SEAE et l'AED, avec les États membres, continueront à développer comme suit la coopération dans le domaine de la cyberdéfense entre l'UE et l'OTAN, dans le respect du cadre institutionnel et de l'autonomie décisionnelle des différentes organisations:

- accélérer les activités menées dans le cadre de la mise en œuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du Traité de l'Atlantique Nord;
- mettre en commun les meilleures pratiques mises en œuvre dans les domaines de la gestion des crises et de la cyberdéfense ainsi que dans le cadre des missions et opérations militaires et civiles;
- viser la cohérence des résultats dans l'élaboration des besoins de capacités en matière de cyberdéfense, lorsqu'ils se chevauchent, notamment en ce qui concerne le développement à long terme des capacités en matière de cyberdéfense;
- tirer davantage parti du cadre de coopération mis en place par l'AED avec le Centre coopératif d'excellence pour la cyberdéfense de l'OTAN, point de départ de la collaboration renforcée dans le cadre de projets de cyberdéfense multinationaux, sur la base d'évaluations appropriées.

Le CESD, le SEAE et l'AED:

- renforceront la coopération concernant des formules de formation et d'enseignement en matière de cyberdéfense ainsi que des exercices;
- assureront une participation réciproque des services concernés aux exercices conformément au cadre établi d'un commun accord.

La CERT-UE:

- va mieux exploiter l'arrangement technique qu'elle a conclu avec la NCIRC (capacité OTAN de réaction aux incidents informatiques) afin d'améliorer l'appréciation des situations, l'échange d'informations et les mécanismes d'alerte rapide et d'anticiper les menaces qui pourraient affecter les deux organisations.

En ce qui concerne les autres organisations internationales et les partenaires internationaux de l'UE concernés, le SEAE et les États membres, pour autant que de besoin:

- suivront l'évolution des stratégies et tiendront des consultations sur des questions liées à la cyberdéfense avec des partenaires internationaux (organisations internationales et pays tiers);
- envisageront des possibilités de coopération sur des questions liées à la cyberdéfense, y compris avec les pays tiers participant aux missions et opérations PSDC;
- promouvront dans les organisations internationales pertinentes, en particulier les Nations unies, l'OSCE et le Forum régional de l'ASEAN, l'application, dans le cyberespace, du droit international en vigueur, notamment la Charte des Nations unies dans son intégralité, et l'établissement et la mise en œuvre de normes universelles non contraignantes définissant un comportement responsable des États, ainsi que de mesures de confiance au niveau régional entre les États pour renforcer la transparence et réduire le risque d'une perception erronée du comportement d'un État.

La Commission et le SEAE:

- soutiendront au besoin le renforcement des cybercapacités des partenaires de l'UE, par l'intermédiaire de l'instrument contribuant à la stabilité et à la paix dans sa version modifiée.

Suivi

Dans le cadre du travail de coordination mené par le SEAE pour la mise en œuvre du cadre stratégique de cyberdéfense, le SEAE / l'AED / la Commission devraient présenter au groupe politico-militaire, avec la participation des membres du groupe horizontal "Questions liées au cyberespace", et au Comité politique et de sécurité un rapport annuel sur l'état d'avancement des travaux, portant sur les six domaines exposés plus haut, afin d'évaluer la mise en œuvre du cadre stratégique. Une présentation orale sera par ailleurs faite tous les six mois.

Il est essentiel, au fur et à mesure que la cybermenace évolue, d'identifier les nouveaux besoins en matière de cyberdéfense, afin de les inclure ensuite dans le cadre stratégique de cyberdéfense. La prochaine version révisée du cadre stratégique de cyberdéfense devrait être présentée au plus tard à la mi-2022, en étroite concertation avec les États membres.