COUR DES COMPTES EUROPÉENNE

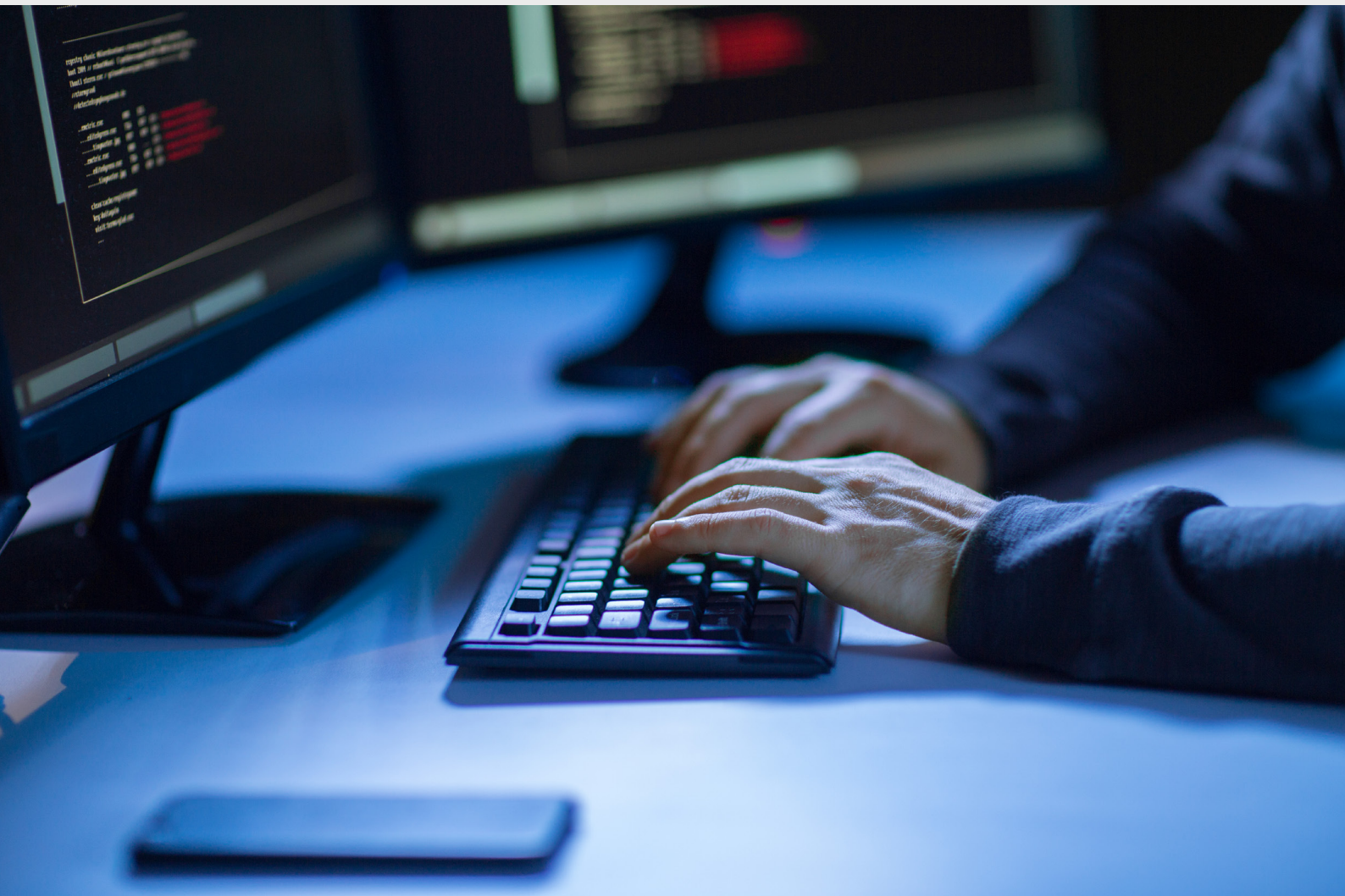
FR

2019

Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité

Document d'information

Mars 2019



À propos du document:

Le présent document d'information, qui ne constitue pas un rapport d'audit, vise à donner une vue d'ensemble du paysage complexe de la politique de l'UE dans le domaine de la cybersécurité et à recenser les principales difficultés à surmonter pour mettre en place une politique efficace. Il porte sur la sécurité des réseaux et de l'information, la cybercriminalité, la cyberdéfense et la désinformation. Il servira aussi de base aux éventuels futurs travaux d'audit dans ce domaine.

Nous avons fondé notre analyse sur un examen documentaire d'informations accessibles au public dans des documents officiels, des documents de prise de position et des études réalisées par des tiers. Les travaux sur le terrain ont été menés entre avril et septembre 2018, et les développements intervenus jusqu'à décembre 2018 sont pris en considération. Nous avons complété nos travaux par une enquête auprès des institutions supérieures de contrôle des États membres, ainsi que par des entretiens avec des acteurs clés des institutions de l'UE et des représentants du secteur privé.

Les défis que nous avons recensés se répartissent en quatre grands groupes selon qu'ils concernent: i) le cadre stratégique; ii) le financement et les dépenses; iii) le renforcement de la cyberrésilience; iv) l'efficacité de la réponse en cas de cyberincident. Assurer un degré plus élevé de cybersécurité dans l'UE reste un impératif. Nous concluons donc chaque chapitre par une série d'idées pouvant donner matière à réflexion aux décideurs politiques, aux législateurs et aux acteurs de terrain.

Nous tenons à remercier les services de la Commission, le Service européen pour l'action extérieure, le Conseil de l'Union européenne, l'ENISA, Europol, l'Organisation européenne pour la cybersécurité et les institutions supérieures de contrôle des États membres pour leurs réponses constructives.

Contents

	Paragraph
Synthèse	**I-XIII**
Introduction	**01-24**
Qu'est-ce que la cybersécurité?	02-06
Quelle est l'ampleur du problème?	07-10
L'action de l'UE en matière de cybersécurité	11-24
Politiques	13-18
Législation	19-24
Établir un cadre stratégique et législatif	**25-39**
Défi n° 1 – Une réelle obligation de rendre compte et une véritable évaluation	26-32
Défi n° 2 – Remédier aux lacunes du droit de l'UE et à sa transposition inégale	33-39
Financement et dépenses	**40-64**
Défi n° 3 – Aligner les niveaux d'investissement sur les objectifs	41-46
Augmenter les investissements	41-44
Amplifier l'impact	45-46
Défi n° 4 – Disposer d'une vue claire des dépenses de l'UE	47-60
Traçabilité des dépenses de cybersécurité	50-56
Autres dépenses de cybersécurité	57-58
Perspectives	59-60
Défi n° 5 – Attribution de ressources adéquates aux agences de l'UE	61-64
Bâtir une société cyberrésiliente	**65-100**
Défi n° 6 – Renforcer la gouvernance et les normes	66-81
Gouvernance en matière de sécurité de l'information	66-75
Évaluations de la menace et des risques	76-78

Mesures incitatives 79-81

Défi n° 7 – Développer les compétences et la prise de conscience 82-90

Formation, compétences et développement des capacités 84-87

Sensibilisation 88-90

Défi n° 8 – Améliorer l'échange d'informations et la coordination 91-100

Coordination entre les institutions de l'UE et avec les États membres 92-96

Coopération et échange d'informations avec le secteur privé 97-100

Répondre efficacement aux cyberincidents 101-117

Défi n° 9 – Efficacité de la détection et de la réaction 102-111

Détection et signalement 102-105

Intervention coordonnée 106-111

Défi n° 10 – Protéger les infrastructures et fonctions sociétales critiques 112-117

Protéger les infrastructures 112-115

Renforcer l'autonomie 116-117

Observations finales 118-121

Annexe I — Un paysage complexe et stratifié qui mobilise de nombreux acteurs

Annexe II — Dépenses consacrées par l'UE à la cybersécurité depuis 2014

Annexe III — Rapports des institutions supérieures de contrôle des États membres de l'UE

Acronymes et abréviations

Glossaire

Équipe de la Cour

Synthèse

I La technologie ouvre tout un horizon de nouvelles possibilités, avec l'intégration de produits et services novateurs dans notre quotidien. En contrepartie, le risque d'être victime de la cybercriminalité ou d'une cyberattaque va croissant, de même que l'impact de celles-ci sur la société et l'économie. L'intensification récente (depuis 2017) des efforts de l'UE visant à renforcer la cybersécurité et l'autonomie numérique intervient donc à un moment critique.

II Établi sur la base d'informations accessibles au public, le présent document d'information, qui ne constitue pas un rapport d'audit, vise à donner une vue d'ensemble du paysage complexe et bigarré des politiques dans ce domaine, ainsi qu'à recenser les principales difficultés qu'il convient de surmonter pour mettre en place une politique efficace. Il porte sur la politique de l'UE dans le domaine de la cybersécurité, sur la cybercriminalité et sur la cyberdéfense, ainsi que sur les mesures de lutte contre la désinformation. Les défis que nous avons recensés se répartissent en quatre grands groupes selon qu'ils concernent: i) le cadre stratégique et législatif; ii) le financement et les dépenses; iii) le renforcement de la cyberrésilience; iv) l'efficacité de la réponse en cas de cyberincident. Chaque chapitre propose quelques éléments de réflexion sur les défis présentés.

Le cadre stratégique et législatif

III En l'absence d'objectifs mesurables et compte tenu du peu de données fiables disponibles, l'élaboration d'actions conformes à l'ambition de la stratégie de cybersécurité de l'UE, qui est d'offrir à l'Union l'environnement numérique le plus sûr au monde, relève de la gageure. Les effets sont rarement mesurés et peu de domaines d'action ont été évalués. L'un des principaux défis consiste donc à **garantir une réelle obligation de rendre compte et une véritable évaluation**, en passant à une culture de la performance qui intègre des pratiques d'évaluation.

IV Quant au cadre législatif, il reste incomplet. **Les lacunes du droit de l'Union et sa transposition incohérente** peuvent empêcher la législation d'atteindre son plein potentiel.

Financement et dépenses

V **Aligner les niveaux d'investissement sur les objectifs** est une tâche difficile qui suppose non seulement d'accroître l'investissement global dans la cybersécurité (faible et fragmenté au sein de l'UE) mais aussi d'en amplifier l'impact, et plus

particulièrement de mieux exploiter les résultats obtenus grâce aux dépenses consacrées à la recherche et d'assurer un ciblage et un financement efficaces des jeunes entreprises.

VI **Une vue claire des dépenses de l'UE** est essentielle pour permettre à l'Union et à ses États membres de déterminer les lacunes à combler pour atteindre les objectifs affichés. En l'absence d'un budget de l'UE spécialement consacré au financement de la stratégie de cybersécurité, il est difficile de distinguer clairement quels crédits sont utilisés à quelles fins.

VII En ces temps où les priorités politiques sont de plus en plus axées sur la sécurité, **les obstacles que rencontrent les agences de l'UE concernées par la cybersécurité pour se doter de ressources adéquates** peuvent compromettre la réalisation des ambitions de l'UE. Face à ces défis, il importe aussi de trouver les moyens d'attirer et de retenir les talents.

Renforcement de la cyberrésilience

VIII La gouvernance en matière de cybersécurité dans le secteur public et le secteur privé présente de nombreuses lacunes partout dans l'UE ainsi qu'au niveau mondial. Celles-ci réduisent la capacité de la communauté internationale à limiter les cyberattaques et à y faire face, ainsi que la possibilité d'établir une approche cohérente à l'échelle de l'UE. Le défi consiste donc à **renforcer la gouvernance en matière de cybersécurité**.

IX Compte tenu de la pénurie de compétences en cybersécurité au niveau mondial, il est essentiel de **développer les compétences et la prise de conscience** dans tous les secteurs et à tous les niveaux de la société. Actuellement, il existe peu de normes communes à l'échelle de l'UE dans les domaines de la formation, de la certification ou de l'évaluation des risques.

X Un socle de confiance est essentiel pour renforcer la cyberrésilience globale. La Commission a elle-même estimé que la coordination en général reste insuffisante. **Améliorer l'échange d'informations et la coordination** entre les secteurs public et privé relève encore du défi.

Répondre efficacement aux cyberincidents

XI Les systèmes numériques sont devenus si complexes qu'il est impossible de prévenir toutes les attaques. La réponse à ce défi réside dans **la détection et la**

réaction rapides. Cependant, la cybersécurité n'est pas encore pleinement intégrée dans les mécanismes de coordination de la réaction aux crises au niveau de l'UE, ce qui pourrait limiter la capacité de celle-ci à répondre aux cyberincidents transfrontières à grande échelle.

XII La **protection des infrastructures et fonctions sociétales critiques** est cruciale. L'ingérence potentielle dans les processus électoraux ainsi que les campagnes de désinformation représentent un défi majeur.

XIII Les défis actuellement posés par les cybermenaces dont font l'objet l'UE et le monde en général requièrent un engagement continu et un attachement sans faille aux valeurs fondamentales de l'UE.

Introduction

01 La technologie ouvre tout un horizon de nouvelles possibilités. À mesure que des produits et services novateurs prennent de l'essor, ils s'installent dans notre quotidien. Cependant, chaque nouvelle évolution accroît notre dépendance aux technologies, ce qui rend la cybersécurité d'autant plus importante. Plus nous livrons des données à caractère personnel en ligne et plus nous sommes connectés, plus nous sommes susceptibles d'être victimes d'une forme ou autre de cybercriminalité ou de cyberattaque.

Qu'est-ce que la cybersécurité?

02 Il n'existe aucune définition normalisée et universellement acceptée de la cybersécurité[1]. Au sens large, le terme désigne toutes les garanties et mesures adoptées pour défendre les systèmes informatiques et leurs utilisateurs contre les accès non autorisés, les attaques et les dommages, de manière à assurer la confidentialité, l'intégrité et la disponibilité des données.

03 La cybersécurité suppose de prévenir ou de détecter les cyberincidents, d'y répondre puis de rétablir la situation. Ces incidents peuvent être provoqués volontairement ou pas, et aller, par exemple, de la divulgation accidentelle d'informations à l'ingérence dans les processus démocratiques, en passant par les attaques contre les entreprises et les infrastructures critiques et le vol de données à caractère personnel. Ils peuvent tous avoir des effets néfastes considérables sur les personnes, les organisations et les collectivités.

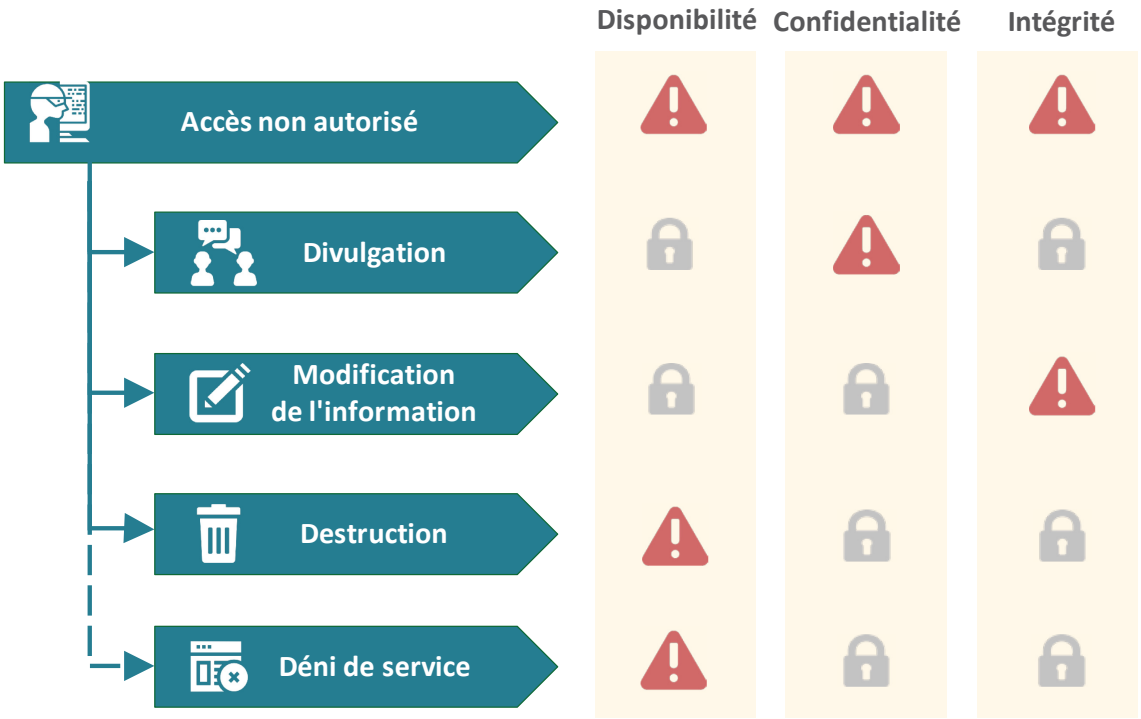
04 Dans les cercles politiques de l'UE, l'utilisation du terme cybersécurité n'est pas limitée à la sécurité des réseaux et de l'information. Elle couvre toute activité illicite impliquant l'utilisation de technologies numériques dans le cyberespace. Elle peut donc concerner des actes cybercriminels tels que le lancement d'attaques par virus informatiques et la fraude aux paiements autres qu'en espèces, mais aussi d'autres crimes et délits liés davantage au contenu qu'aux systèmes, comme la diffusion en ligne de contenu à caractère pédopornographique. Elle peut en outre intéresser les campagnes de désinformation visant à influer sur les débats en ligne ainsi que les interférences électorales présumées. Par ailleurs, Europol considère qu'il existe une convergence entre la cybercriminalité et le terrorisme[2].

05 Différents acteurs (États, groupes criminels, hacktivistes, …) provoquent des cyberincidents, pour des motifs divers. Les répercussions de ces incidents se ressentent

aux niveaux national, européen et même mondial. Cependant, le caractère intangible et essentiellement transfrontière d'internet, ainsi que les outils et les tactiques utilisés, compliquent souvent l'identification des auteurs d'une attaque (ce que l'on appelle «le problème d'attribution des responsabilités»).

06 Les nombreuses formes de menaces qui pèsent sur la cybersécurité peuvent être classées en fonction de leurs effets sur les données (divulgation, altération, destruction ou refus d'accès) ou des principes fondamentaux en matière de sécurité de l'information qu'elles violent, comme l'illustre la ***figure 1***. Des exemples d'attaques sont décrits à l'***encadré 1***. Avec l'augmentation du degré de sophistication des attaques contre les systèmes informatiques, nos mécanismes de défense perdent en efficacité[3].

Figure 1 – Types de menaces et principes de sécurité qu'elles mettent en péril



Source: Cour des comptes européenne, sur la base d'une étude du Parlement européen[4]. Le cadenas indique que la sécurité n'est pas affectée; le point d'exclamation indique qu'elle est compromise.

Encadré 1

Types de cyberattaques

Chaque nouvel appareil qui se connecte à internet ou à d'autres appareils augmente ce que l'on appelle la «surface d'attaque» en matière de cybersécurité. La croissance exponentielle de l'«internet des objets», de l'informatique en nuage, des mégadonnées et de la numérisation de l'industrie s'accompagne d'une exposition et d'une vulnérabilité grandissantes, qui permettent aux acteurs malveillants de cibler toujours plus de victimes. Du fait de la diversité des types d'attaques et de leur sophistication croissante, il est véritablement difficile de suivre le rythme[5].

Un **maliciel** (logiciel malveillant) est conçu pour perturber le fonctionnement des appareils et des réseaux. Il peut s'agir d'un virus, d'un cheval de Troie, d'un logiciel rançonneur, d'un ver, d'un logiciel publicitaire ou d'un logiciel espion. Un **logiciel rançonneur** crypte les données, empêchant ainsi les utilisateurs d'accéder à leurs dossiers jusqu'à ce qu'ils versent une rançon, généralement en cryptomonnaie, ou qu'ils réalisent une action donnée. Selon Europol, les attaques par logiciels rançonneurs sont de loin les plus fréquentes et la variété des logiciels de ce type a explosé ces dernières années. Les attaques par **déni de service distribué**, qui consistent à rendre des services ou des ressources indisponibles en les saturant de requêtes, connaissent également une augmentation, un tiers des organisations ayant été visées par ce type d'attaques en 2017[6].

Les utilisateurs peuvent être manipulés de sorte à ce qu'ils effectuent une action ou divulguent des informations confidentielles de manière involontaire. Ce stratagème, qui peut être utilisé pour les vols de données ou le cyberespionnage, est appelé **piratage psychologique**. Il existe plusieurs méthodes pour ce faire, mais la plus répandue est l'**hameçonnage**, un procédé qui consiste à envoyer des courriels semblant provenir de sources fiables afin de piéger le destinataire et de l'amener ainsi à révéler des informations ou à cliquer sur des liens qui infecteront ses appareils en y installant des logiciels malveillants. Plus de la moitié des États membres ont fait état d'enquêtes sur des attaques visant des réseaux[7].

Mais les attaques les plus néfastes sont les **menaces persistantes avancées**. Ces attaques sophistiquées impliquent des activités à long terme de surveillance et de vols de données et visent parfois aussi à semer la destruction. Le but est d'échapper à toute détection aussi longtemps que possible. Souvent associées à un État, les menaces persistantes avancées ciblent les secteurs particulièrement sensibles comme les technologies, la défense et les infrastructures critiques. Selon certaines estimations, le cyberespionnage représente au moins un quart de tous les cyberincidents, ainsi que la plus grande partie des coûts engendrés[8].

Quelle est l'ampleur du problème?

07 Compte tenu du manque de données fiables, il est difficile de mesurer l'impact d'une préparation insuffisante aux cyberattaques. L'impact économique de la cybercriminalité a été multiplié par cinq entre 2013 et 2017[9], frappant de plein fouet les administrations publiques et les entreprises de toutes tailles. La croissance escomptée des primes de cyberassurance de 3 milliards d'euros en 2018 à 8,9 milliards d'euros en 2020 reflète cette tendance.

08 Tandis que l'impact financier des cyberattaques ne cesse de croître, la disparité est alarmante entre le coût du lancement d'une attaque et les coûts de prévention, d'enquête et de réparation. À titre d'exemple, 15 euros par mois peuvent suffire pour mener une attaque par déni de service, alors que les pertes subies par l'entreprise visée, y compris celles résultant de l'atteinte à la réputation, sont bien plus conséquentes[10].

09 Même si 80 % des entreprises de l'UE ont subi au moins un incident lié à la cybersécurité en 2016[11], la prise de conscience des risques reste d'une faiblesse alarmante. Dans l'UE, 69 % des entreprises n'ont qu'une compréhension de base, voire aucune compréhension, de leur exposition aux cybermenaces[12], tandis que 60 % n'ont jamais évalué les pertes financières potentielles[13]. Par ailleurs, selon une étude réalisée à l'échelle mondiale, un tiers des organisations préféreraient verser une rançon à des pirates plutôt qu'investir dans la sécurité informatique[14].

10 Les cyberattaques d'envergure mondiale perpétrées en 2017 à l'aide du logiciel rançonneur *Wannacry* et du logiciel malveillant d'effacement *NotPetya* ont fait, à elles deux, plus de 320 000 victimes dans 150 pays environ[15]. Ces incidents ont en quelque sorte entraîné une prise de conscience mondiale de la menace que représentent les cyberattaques, qui a donné une nouvelle impulsion à la prise en considération de la cybersécurité dans la réflexion politique générale. En outre, 86 % des citoyens de l'UE estiment aujourd'hui que le risque d'être victime de la cybercriminalité est en augmentation[16].

L'action de l'UE en matière de cybersécurité

11 En 2001, l'Union européenne a intégré le Comité de la Convention du Conseil de l'Europe sur la cybercriminalité[17] (dite convention de Budapest) en qualité d'observatrice. Depuis lors, elle a élaboré des politiques, adapté sa législation et engagé des dépenses pour renforcer sa cyberrésilience. Dans un contexte d'augmentation du nombre de cyberattaques et de cyberincidents majeurs, l'activité s'est intensifiée depuis 2013,

comme le montre la ***figure 2***. Parallèlement, les États membres ont adopté (voire déjà mis à jour, pour certains d'entre eux) leurs premières stratégies nationales de cybersécurité.

12 Les principaux acteurs de l'UE exerçant des responsabilités en matière de cybersécurité sont présentés dans l'***encadré 2*** et à l'***annexe I***.

Encadré 2

Qui est concerné?

La **Commission européenne** cherche à renforcer les capacités et la coopération en matière de cybersécurité, à faire de l'UE un acteur majeur dans ce domaine et à intégrer celui-ci dans les autres politiques de l'Union. Les principales directions générales (DG) responsables de la cybersécurité sont les DG **CNECT** (cybersécurité) et HOME (cybercriminalité), respectivement en charge du marché unique numérique et de l'union de la sécurité. La DG **DIGIT** est responsable de la sécurité informatique des propres systèmes de la Commission.

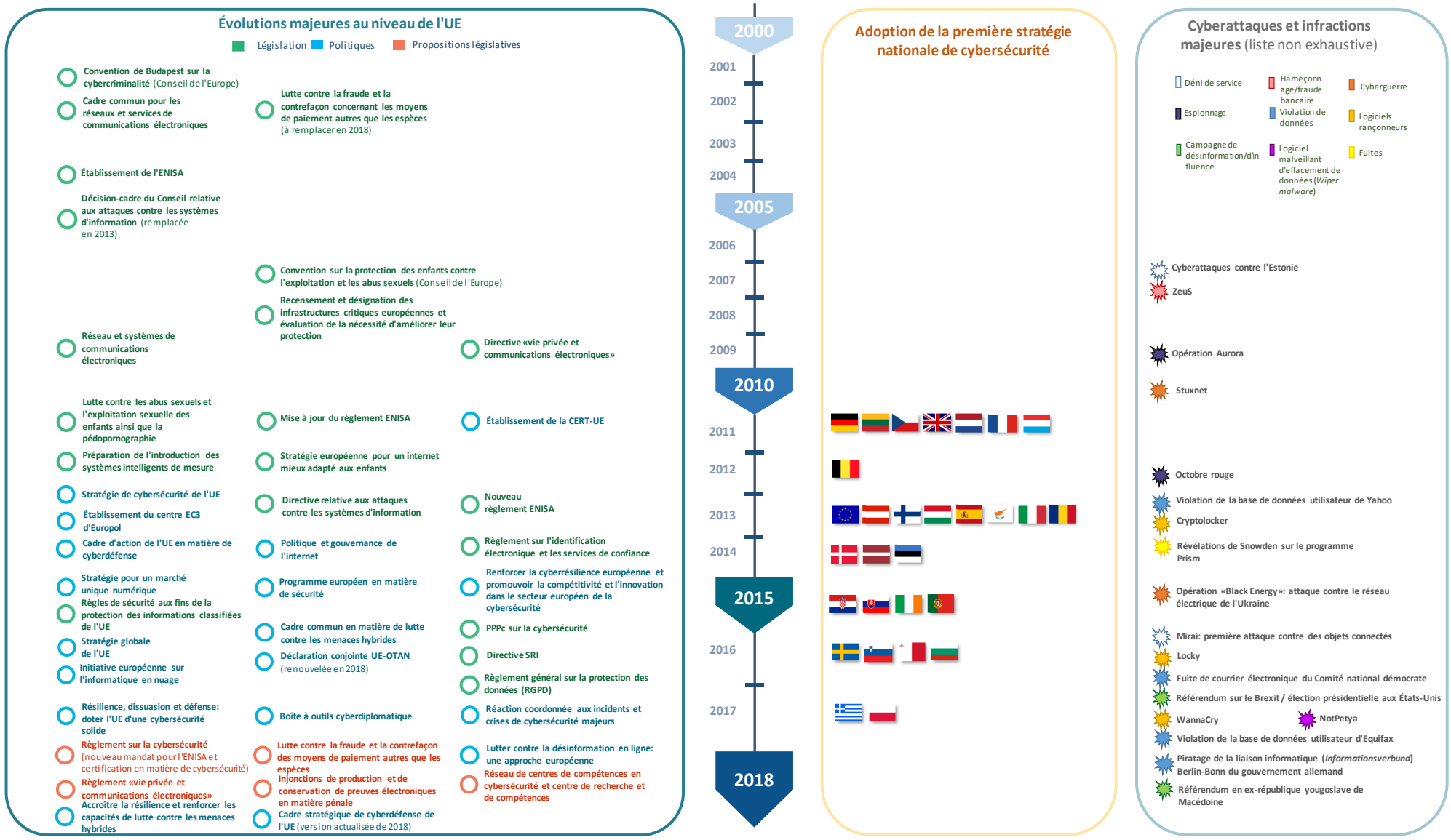
Toute une série d'agences de l'UE soutiennent la Commission, parmi lesquelles l'**ENISA** (Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information), l'agence de l'UE pour la cybersécurité, un organe essentiellement consultatif qui soutient l'élaboration des politiques, le renforcement des capacités et la sensibilisation. Le Centre européen de lutte contre la cybercriminalité (**EC3**) a été créé pour renforcer l'action répressive de l'UE à l'encontre de la cybercriminalité. Une équipe d'intervention en cas d'urgence informatique (CERT-UE), chargée de soutenir l'ensemble des institutions, organes et agences de l'UE, est hébergée par la Commission.

Le **Service européen pour l'action extérieure** (SEAE) agit en qualité de chef de file dans les domaines de la cyberdéfense, de la cyberdiplomatie et de la communication stratégique et héberge des centres de renseignement et d'analyse. L'**Agence européenne de défense** (ADE) vise à développer des capacités de cyberdéfense.

Les **États membres** sont responsables au premier chef de leur propre cybersécurité et ils agissent, à l'échelle de l'UE, par l'intermédiaire du **Conseil**, qui dispose de nombreux organes de coordination et de partage de l'information (dont le groupe horizontal «Questions liées au cyberespace»). Le **Parlement européen** agit en tant que colégislateur.

Les **organisations du secteur privé**, y compris des organisations de l'industrie, des organes de gouvernance de l'internet et des universités, participent et contribuent à l'élaboration et à la mise en œuvre des politiques (notamment dans le cadre de **partenariats public-privé contractuels**).

Figure 2 – Accélération de l'élaboration des politiques et de la législation (au 31 décembre 2018)



Source: Cour des comptes européenne.

Politiques

13 Le cyberécosystème de l'UE est complexe et stratifié. Il englobe toute une série de domaines d'action internes, tels que la justice et les affaires intérieures, le marché unique numérique et les politiques de recherche. Dans les domaines d'action externes, la cybersécurité se retrouve dans la diplomatie, et devient progressivement partie intégrante de la politique de défense de l'Union.

14 La pierre angulaire de la politique de l'UE dans ce domaine est la stratégie de cybersécurité de 2013[18], qui vise à offrir à l'UE l'environnement numérique le plus sûr du monde, sans compromettre les valeurs et les libertés fondamentales. Elle poursuit les cinq grands objectifs suivants: i) renforcer la cyberrésilience; ii) faire reculer la cybercriminalité; iii) développer une politique et des moyens de cyberdéfense; iv) développer les ressources industrielles et technologiques en matière de cybersécurité; v) instaurer une politique internationale en matière de cyberespace qui soit conforme aux valeurs essentielles de l'UE.

15 La stratégie de cybersécurité est en corrélation avec trois stratégies adoptées ultérieurement:

— le **programme européen en matière de sécurité** (2015), dont le but est d'améliorer l'action répressive et judiciaire à l'encontre de la cybercriminalité, principalement en actualisant les politiques et la législation existantes[19]. Ce programme vise également à faire le point sur les obstacles aux enquêtes pénales concernant la cybercriminalité et à renforcer les capacités dans le domaine de la cybersécurité;

— la **stratégie pour un marché unique numérique**[20] (2015), qui vise à améliorer l'accès aux biens et services numériques en mettant en place un environnement propice à l'optimisation du potentiel de croissance de notre économie numérique. Pour ce faire, il est essentiel de renforcer la sécurité, la confiance et l'inclusion de tous sur internet;

— la **stratégie globale**[21] de 2016, qui vise à renforcer le rôle de l'UE dans le monde. La cybersécurité en constitue un pilier central, grâce à un engagement renouvelé face aux questions liées au cyberespace, à la coopération avec les principaux partenaires et à la volonté de traiter les questions liées au cyberespace dans tous les domaines d'action, y compris en opposant un démenti à toute désinformation grâce à une communication stratégique.

16 Ces dernières années, le cyberespace est devenu de plus en plus militarisé[22,23] et il est aujourd'hui considéré comme le cinquième domaine d'activité militaire[24]. La cyberdéfense consiste à protéger les systèmes, les réseaux et les infrastructures critiques liées au cyberespace contre les attaques, militaires et autres. Un **cadre stratégique de cyberdéfense de l'UE** a été adopté en 2014 et actualisé en 2018[25]. Dans sa version actualisée de 2018, il définit six domaines prioritaires, y compris la mise en place de capacités de cyberdéfense, ainsi que la protection des réseaux de communication et d'information de la politique de sécurité et de défense commune (PSDC) de l'UE. La cyberdéfense relève également du cadre de coopération structurée permanente (PESCO) et de la coopération UE-OTAN.

17 Adoptée par l'UE en 2016, la communication conjointe relative au **cadre commun en matière de lutte contre les menaces hybrides** vise à contrer les cybermenaces pesant sur les infrastructures critiques et les utilisateurs privés et souligne que les cyberattaques peuvent prendre la forme de campagnes de désinformation sur les médias sociaux[26]. Elle rappelle également la nécessité d'améliorer la connaissance de la situation et celle de renforcer la coopération entre l'UE et l'OTAN, à laquelle font écho les déclarations communes UE-OTAN de 2016 et de 2018[27].

18 En 2017, la Commission a présenté un nouveau train de mesures sur la cybersécurité, qui reflétait le besoin urgent et croissant d'assurer une protection numérique. Il s'agissait notamment d'une nouvelle communication de la Commission relative à la mise à jour de la stratégie de cybersécurité de 2013[28], d'un plan d'action pour une réponse rapide et coordonnée à une cyberattaque majeure et d'une communication pour une mise en œuvre dans les meilleurs délais de la directive relative à la sécurité des réseaux et des systèmes d'information (directive SRI)[29]. Le train de mesures prévoyait en outre un certain nombre de propositions législatives (voir point ***22***).

Législation

19 Depuis 2002, toute une série d'actes législatifs plus ou moins en rapport avec la cybersécurité ont été adoptés.

20 Au cœur de la stratégie de cybersécurité de 2013, on retrouve la pièce maîtresse de cette législation, à savoir la **directive concernant la sécurité des réseaux et des systèmes d'information (SRI)**[30] de 2016, premier acte législatif de l'UE sur la cybersécurité. Cette directive, qui devait être transposée en droit interne pour mai 2018, vise à parvenir à un niveau minimum de capacités harmonisées en obligeant

les États membres à adopter des stratégies SRI nationales et à mettre en place des points de contact uniques et des centres de réponse aux incidents de sécurité informatique (CSIRT)[31]. Elle établit également des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels dans les secteurs critiques et pour les fournisseurs de services numériques.

21 Par ailleurs, le **règlement général sur la protection des données**[32] (RGPD), entré en vigueur en 2016, est applicable depuis mai 2018. Il a pour objectif de protéger les données à caractère personnel de citoyens européens en fixant des règles relatives à leur traitement et à leur diffusion. Il confère aux personnes concernées certains droits et impose des obligations aux responsables du traitement (les fournisseurs de services numériques) concerne l'utilisation et la transmission des informations. Il prévoit également des obligations de notification en cas de violation et, dans certains cas, la possibilité d'infliger des amendes. La ***figure 3*** illustre la complémentarité entre l'objectif de renforcement de la cybersécurité poursuivi par la directive SRI et celui de garantir la protection des données assigné au RGPD.

22 Les actes législatifs actuellement à l'examen comprennent le règlement sur la cybersécurité proposé pour renforcer l'ENISA et instituer un mécanisme de certification à l'échelle de l'UE[33], la proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques[34] et la proposition de directive sur les preuves électroniques[35]. La proposition de 2018 relative à l'établissement d'un centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et d'un réseau de centres nationaux de coordination (ci-après dénommés «réseau de centres de compétences en cybersécurité» et «centre de recherche et de compétences») fait partie du train de mesures de 2017 sur la cybersécurité[36].

23 Il peut s'avérer difficile de se faire une idée de l'ampleur du cadre stratégique et législatif concernant la cybersécurité et de son incidence sur notre vie quotidienne.

24 La ***figure 4*** montre des situations dans lesquelles différents actes législatifs ou d'autres initiatives influent sur la vie d'une citoyenne européenne fictive.

Figure 3 – Complémentarité entre le RGPD et la directive SRI

Source: Cour des comptes européenne.

Figure 4 – Comment l'approche de l'UE en matière de cybersécurité se fond dans la vie quotidienne des citoyens

Source: Cour des comptes européenne.

Établir un cadre stratégique et législatif

25 Complexe et comportant plusieurs niveaux, le cyberécosystème de l'UE fait intervenir de nombreuses parties prenantes (voir ***annexe I***). Rassembler tous les éléments disparates qui le composent constitue un véritable défi. Depuis 2013, des efforts concertés ont été déployés pour apporter de la cohérence dans le domaine de la cybersécurité de l'UE[37].

Défi n° 1 – Une réelle obligation de rendre compte et une véritable évaluation

26 Comme la Commission l'a fait observer, il est difficile d'établir un lien de cause à effet entre la stratégie de 2013 et tout changement constaté. Les objectifs de cette stratégie étaient formulés de manière très large, et correspondaient davantage à une vision qu'à des valeurs cibles mesurables[38]. En l'absence d'objectifs mesurables, l'élaboration d'actions conformes à ces grands objectifs est une gageure. La version actualisée du cadre stratégique de cyberdéfense (2018) vise à formuler des objectifs définissant le degré minimum de cybersécurité et de confiance à assurer. Cependant, cette stratégie est limitée à la cyberdéfense, aucun objectif n'ayant été fixé qui définisse le degré de résilience voulu pour l'UE dans son ensemble.

27 Les effets sont rarement mesurés et peu de domaines d'action ont été évalués[39]. Cela tient en partie au fait que bon nombre de ces mesures (législatives ou autres) ont été mises en œuvre récemment et que leur impact ne peut donc pas encore être pleinement évalué. La difficulté réside donc dans la définition de critères d'évaluation pertinents qui permettent de mesurer cet impact. En outre, de manière générale, une évaluation rigoureuse n'est pas encore devenue la norme dans le domaine de la cybersécurité. Il est donc nécessaire de passer à une culture de la performance intégrant des pratiques d'évaluation et un système normalisé d'établissement de rapports. Actuellement, le mandat de l'ENISA ne couvre par l'évaluation et le suivi de la situation et de l'état de préparation de l'UE en matière de cybersécurité.

28 Pour élaborer des politiques en se fondant sur des données factuelles, il faut suffisamment de données et de statistiques fiables pour pouvoir suivre et analyser les tendances et les besoins. En l'absence d'un système de suivi commun et obligatoire, les données fiables sont rares. Les indicateurs sont rarement à disposition et sont difficiles à définir[40]. Des paramètres spécifiques ont toutefois été mis au point dans

certains domaines tels que le cycle politique de l'UE qui sert à lutter contre la grande criminalité organisée.

29 Les États membres qui collectent régulièrement des données officielles sur les questions liées au cyberespace sont peu nombreux, ce qui limite la comparabilité. À ce jour, l'UE ne s'est guère exprimée sur la nécessité de consolider les statistiques au niveau européen[41]. Il n'existe pas non plus beaucoup d'analyses indépendantes à l'échelle de l'UE concernant des thèmes clés tels que[42]: les paramètres économiques de la cybersécurité, y compris les aspects comportementaux (déséquilibre des incitations, asymétrie de l'information); la compréhension de l'impact de la cybercriminalité et des défaillances en matière de sécurité; les statistiques macroéconomiques concernant les tendances et les défis escomptés du cyberespace; les solutions les plus appropriées pour traiter les menaces.

30 Compte tenu de l'absence d'objectifs spécifiques et de la rareté des données fiables et des indicateurs clairement définis, l'évaluation des résultats de la stratégie est essentiellement qualitative à ce jour. Les rapports sur l'état d'avancement décrivent souvent les activités réalisées ou les étapes franchies, sans mesurer précisément les résultats. Par ailleurs, les données de référence pour l'évaluation de la résilience des systèmes n'ont pas encore été établies. En outre, en l'absence de définition codifiée de la cybercriminalité, il est pratiquement impossible de trouver des indicateurs pertinents au niveau européen qui puissent faciliter le suivi et l'évaluation.

31 Le contrôle indépendant de la mise en œuvre de la politique de cybersécurité varie d'un État membre à l'autre. Nous avons interrogé les institutions supérieures de contrôle nationales sur leur expérience en matière d'audit dans ce domaine. La moitié des répondants[43] n'en avaient aucune. Pour les autres, leurs audits avaient porté principalement sur: la gouvernance de l'information, la protection des infrastructures critiques, l'échange d'informations et la coordination entre les principales parties prenantes, ou encore la notification des incidents ainsi que la préparation et la réaction à ceux-ci. Les mesures de sensibilisation et le déficit de compétences numériques faisaient partie des sujets moins souvent traités. Pour des motifs de sécurité nationale, les résultats de ces audits ou évaluations ne sont pas toujours rendus publics. Une liste des rapports d'audit publiés par les institutions supérieures de contrôle nationales est fournie à l'***annexe III***.

32 La disponibilité limitée des compétences relatives au cyberespace (voir également les points ***82 à 90***) et la difficulté à évaluer les progrès en matière de cybersécurité étaient perçues comme les principaux écueils de l'audit des mesures gouvernementales dans ce domaine.

Défi n° 2 – Remédier aux lacunes du droit de l'UE et à sa transposition inégale

33 Le rythme auquel se développent les nouvelles technologies et les nouvelles menaces dépasse de loin celui de la conception et de la mise en œuvre de la législation de l'UE. Les procédures de l'Union n'ayant pas été pensées pour l'ère numérique, la mise en place de procédures innovantes et souples permettant de garantir un cadre stratégique et légal adapté aux besoins[44] afin de mieux anticiper et façonner l'avenir constitue une priorité absolue[45].

34 Malgré les efforts déployés pour renforcer la cohérence, le cadre législatif de la cybersécurité reste incomplet (voir exemples au ***tableau 1***). Sa fragmentation et ses lacunes empêchent la réalisation des grands objectifs stratégiques et se traduisent par un manque d'efficience. Les lacunes mises au jour par la Commission dans l'évaluation de la stratégie concernaient notamment l'internet des objets, l'équilibre des responsabilités entre les utilisateurs et les fournisseurs de produits numériques, ainsi que certains aspects non couverts par la directive SRI. La proposition de règlement sur la cybersécurité vise à les combler en partie en promouvant la sécurité dès la conception, dans le cadre d'un système de certification à l'échelle de l'UE. Certaines parties prenantes estiment que l'absence de politique industrielle clairement définie pour le cyberespace et d'approche commune du cyberespionnage reste criante[46].

Tableau 1 – Lacunes et transposition inégale du cadre législatif (liste non exhaustive)

Domaine d'action	Exemples
Marché unique numérique	o La directive actuelle sur la vente des biens de consommation ne couvre pas la cybersécurité. Les propositions de directives relatives au contenu numérique[47] et à la vente en ligne[48] visent à combler cette lacune. o Les cadres juridiques des États membres de l'UE concernant les obligations de vigilance sont limités et divergents, ce qui entraîne une insécurité juridique et des difficultés à obtenir réparation en justice[49]. o Des politiques relatives au signalement des failles logicielles sont élaborées à des rythmes divers dans l'ensemble des États membres, en l'absence de cadre juridique global au niveau de l'UE permettant d'appliquer une approche coordonnée[50].
Renforcement de la sécurité des réseaux et de l'information	o Les États membres ont la faculté d'ajouter des secteurs non couverts par la directive SRI[51]. Le secteur de l'hébergement touristique, qui n'est pas couvert par la directive, peut ouvrir la porte à d'autres crimes ou délits, comme la traite des êtres humains, le trafic de drogue ou l'immigration clandestine[52].
Lutte contre la cybercriminalité	o Nombreux sont les États membres qui n'ont pas encore défini la notion de preuve électronique dans leur législation nationale[53] (voir également point **22**). o L'actuelle décision cadre relative à la fraude aux moyens de paiement autres que les espèces ne couvre pas explicitement les instruments de paiement non matériels tels que les monnaies virtuelles ou électroniques et l'argent mobile, pas plus qu'elle ne porte sur les actes tels que l'hameçonnage, le clonage de carte ou encore la détention et la diffusion d'informations de paiement[54]. o La directive relative aux attaques contre les systèmes d'information ne traitant pas directement de l'acquisition illicite de données par intrusion (par exemple le cyberespionnage), il est difficile de l'invoquer pour entamer des poursuites[55]. o Au lendemain de l'arrêt de la Cour de justice de l'Union européenne sur la conservation des données[56], les différentes approches adoptées par les États membres dans l'application du cadre juridique ont entravé l'exécution de la législation, ce qui a pu conduire à la disparition de pistes d'enquête et compromettre l'efficacité des poursuites à l'encontre des auteurs d'activités criminelles en ligne[57].

Source: Cour des comptes européenne.

35 L'application de certains aspects de la législation revêt encore un caractère volontaire, aussi bien pour les autorités nationales que pour les opérateurs privés. Dans le cadre du groupe de coopération, par exemple, l'évaluation des stratégies nationales en matière de sécurité des réseaux et des systèmes d'information ainsi que celle de l'efficacité des centres de réponse aux incidents de sécurité informatique (CSIRT) sont facultatives. Cela vaut également pour l'application de la certification des produits et services informatiques au titre du système de certification prévu dans la proposition de règlement sur la cybersécurité.

36 Au sein de l'UE, la cybersécurité relève exclusivement des États membres. Malgré tout, l'UE a un rôle essentiel à jouer, à savoir créer des conditions permettant aux États membres d'améliorer leurs capacités, de coopérer entre eux et de susciter la confiance. Pourtant, compte tenu des différences considérables entre les États membres du point de vue des capacités et de l'engagement[58], la communication d'informations sensibles (liées à la sécurité nationale) restera facultative.

37 La transposition inégale du droit de l'UE dans les différents États membres peut être source d'incohérence sur le plan opérationnel et empêcher la législation d'atteindre son plein potentiel. Par exemple, les États membres ayant des interprétations différentes de la façon dont les contrôles des exportations de biens à double usage doivent être appliqués[59], certaines entreprises établies dans l'UE peuvent exporter des technologies et des services susceptibles d'être utilisés tant pour la cybersurveillance que pour exercer la censure ou intercepter des communications, ce qui constitue une atteinte aux droits de l'homme. Le Parlement européen s'est déclaré inquiet face à cette situation[60].

38 En outre, la protection de la vie privée et le respect de la liberté d'expression requièrent une réponse législative adaptée afin de trouver le juste équilibre entre la préservation des valeurs fondamentales et la réalisation des impératifs de sécurité de l'UE. Par exemple, comment garantir le chiffrement de bout en bout tout en soutenant autant que possible l'application de la loi? Ou comment satisfaire aux objectifs du RGPD lorsque l'on connaît ses conséquences sur les informations accessibles au public concernant les titulaires de noms de domaines et les propriétaires de plages d'adresses IP? Et quelle incidence négative cela peut-il avoir sur les enquêtes des services de répression[61]?

39 À elle seule, la législation ne suffit pas à garantir la résilience. La directive SRI a pour objectif d'assurer un niveau élevé de sécurité dans l'ensemble de l'UE, mais elle

vise explicitement une harmonisation minimale plutôt que maximale[62]. Des lacunes continueront à apparaître à mesure que le cyberespace évolue.

Éléments de réflexion – Cadre stratégique

- Quelles mesures faut-il absolument prendre pour amener les décideurs politiques et les législateurs à opérer une transition vers une culture de la performance dans le domaine de la cybersécurité, y compris en matière de définition de la résilience globale?
- Comment la recherche peut-elle contribuer davantage à générer les données et statistiques nécessaires pour permettre une véritable évaluation?
- Comment adapter les processus législatifs de l'UE pour qu'ils deviennent plus souples et qu'ils tiennent mieux compte de l'évolution rapide des technologies et des menaces?
- Comment la pratique consistant à élaborer des paramètres (indicateurs, valeurs cibles, etc.) dans le cadre du cycle politique de l'UE peut-elle être adaptée, développée et reproduite pour l'ensemble du domaine de la cybersécurité?
- Quels enseignements les institutions supérieures de contrôle nationales peuvent-elles tirer des approches des unes et des autres en matière d'audit des politiques et mesures de cybersécurité?
- Quelles incohérences dans la transposition et la mise en œuvre du cadre juridique de l'UE rendent moins efficaces les réponses apportées aux déficits de cybersécurité et à la cybercriminalité, et comment les États membres et les institutions de l'UE pourraient-ils remédier au mieux à ce problème?
- Dans quelle mesure les contrôles des exportations de biens et de services de l'UE sont-ils efficaces pour prévenir les atteintes aux droits de l'homme à l'extérieur de l'Union?

Financement et dépenses

40 L'UE aspire à avoir l'environnement en ligne le plus sûr du monde. La réalisation de cette ambition requiert des efforts considérables de la part de toutes les parties prenantes, ainsi qu'une assise financière solide et bien gérée.

Défi n° 3 – Aligner les niveaux d'investissement sur les objectifs

Augmenter les investissements

41 Selon les estimations, les dépenses totales en cybersécurité représentent environ 0,1 % du PIB à l'échelle mondiale. Aux États-Unis[63], ce chiffre s'élève à quelque 0,35 % (secteur privé compris). Les dépenses de cybersécurité inscrites au budget du gouvernement fédéral pour 2019 s'élèvent à quelque 21 milliards de dollars des États-Unis, soit environ 0,1 % du PIB[64].

42 Les dépenses consacrées à la cybersécurité dans l'UE sont comparativement faibles, fragmentées et rarement accompagnées de programmes concertés gérés par les pouvoirs publics. Les chiffres sont difficiles à obtenir, mais selon certaines estimations, les dépenses publiques consacrées à la cybersécurité dans l'UE se situent entre un et deux milliards d'euros par an[65]. Exprimées en pourcentage du PIB, les dépenses de certains États membres représentent un dixième de celles des États-Unis, voire moins[66]. L'UE et les États membres doivent connaître le montant global de tous leurs investissements pour déterminer quelles sont les lacunes à combler.

43 Il est difficile d'avoir une vision d'ensemble, d'une part parce que la nature transsectorielle de la cybersécurité ne permet pas de disposer de données claires et, d'autre part, parce qu'il est souvent impossible de distinguer les dépenses informatiques générales de celles relatives à la cybersécurité[67]. Notre enquête a confirmé qu'il est difficile d'obtenir des statistiques fiables sur ces dépenses, tant dans le secteur public que dans le secteur privé. Trois quarts des institutions supérieures de contrôle nationales ont déclaré ne pas disposer d'une vue centralisée des dépenses publiques liées au cyberespace, et aucun État membre n'oblige les entités publiques à faire apparaître distinctement les dépenses de cybersécurité dans leurs plans financiers.

44 L'augmentation des investissements publics et privés dans les entreprises spécialisées en cybersécurité en Europe représente un défi particulier. Des capitaux

publics sont souvent disponibles pour les premières phases, mais moins souvent pour les phases de croissance et d'expansion[68]. Il existe de nombreuses initiatives de financement de l'UE, qui ne sont toutefois pas exploitées, en grande partie en raison des formalités administratives[69]. Globalement, les entreprises de l'UE spécialisées en cybersécurité affichent des performances inférieures à celles de leurs homologues internationaux: elles sont moins nombreuses et le montant moyen des fonds qu'elles lèvent est nettement plus faible[70]. Il est donc indispensable de garantir un ciblage et un financement efficaces des jeunes entreprises pour atteindre les objectifs de la politique numérique de l'UE.

Amplifier l'impact

45 La résorption du déficit d'investissement dans le cyberespace doit produire des effets utiles. Par exemple, malgré la puissance du secteur de la recherche et de l'innovation de l'UE, les résultats ne sont pas suffisamment brevetés, commercialisés ou développés pour permettre de gagner en résilience, en compétitivité et en autonomie numérique[71]. Ce constat est particulièrement vrai par comparaison avec les concurrents de l'UE au niveau mondial. Le fait que les résultats soient rarement exploités de manière appropriée tient à une série de facteurs[72], dont:

- l'absence de stratégie transnationale cohérente permettant d'étendre l'approche afin de répondre aux besoins de l'UE dans le domaine plus général du numérique, à savoir renforcer la compétitivité et l'autonomie;
- la longueur du cycle de la chaîne de valeur, qui fait que les outils deviennent rapidement obsolètes;
- la durabilité insuffisante, les projets prenant généralement fin avec la dissolution de l'équipe et l'arrêt du soutien, y compris les mises à jour et l'installation de correctifs.

46 La proposition de la Commission d'instituer un réseau de centres de compétences en cybersécurité et un centre de recherche et de compétences vise à surmonter la fragmentation du domaine de la recherche en cybersécurité et à stimuler les investissements à grande échelle[73]. Il existe au total 665 centres d'expertise dans l'ensemble de l'UE.

Défi n° 4 – Disposer d'une vue claire des dépenses de l'UE

47 Pour assurer la transparence et améliorer la coordination, il importe d'avoir une vue centralisée des dépenses. Sans cela, les responsables politiques peuvent difficilement vérifier si les dépenses sont suffisamment en adéquation avec les besoins pour permettre d'atteindre les objectifs prioritaires.

48 Aucun budget spécifique n'est consacré à la stratégie de cybersécurité. Au niveau de l'UE, les dépenses en matière de cybersécurité sont plutôt financées par le budget général et le cofinancement des États membres. Notre analyse révèle une structure complexe composée d'au moins dix instruments différents relevant du budget général de l'UE, mais il est impossible de déterminer avec précision quels crédits sont utilisés à quelles fins (voir ***annexe II***).

49 Dresser un tableau clair des dépenses pour un sujet qui touche à un grand nombre de domaines d'action constitue donc une épreuve de taille. Les programmes de dépenses sont gérés par différents services de la Commission, ayant chacun leurs propres objectifs, règles et calendriers. Le tableau se complique encore si l'on intègre dans l'analyse le cofinancement par les États membres, à prendre en compte par exemple pour le volet «police» du Fonds pour la sécurité intérieure[74].

Traçabilité des dépenses de cybersécurité

50 Lors de la période 2014-2018, la Commission a dépensé au moins 1,4 milliard d'euros pour mettre en œuvre la stratégie[75]. La plus grande partie de ce montant a été allouée au programme Horizon 2020[76]. Les fonds d'Horizon 2020 consacrés à la cybersécurité sont principalement octroyés au titre des objectifs «sociétés sûres» et «primauté dans le domaine des technologies génériques et industrielles»[77]. Nous avons recensé 279 projets liés à la cybersécurité qui avaient fait l'objet de contrats au plus tard en septembre 2018, pour un financement total de 786 millions d'euros apporté par l'UE[78]. La ***figure 5*** présente la typologie de ces projets telle qu'elle ressort de notre analyse.

Figure 5 – Projets de cybersécurité d'Horizon 2020 ayant fait l'objet de contrats (montants en millions d'euros)

Source: Cour des comptes européenne.

51 Un partenariat public-privé contractuel (PPPc) a été conclu en 2016 pour stimuler le secteur de la cybersécurité en Europe. Le but était d'injecter 450 millions d'euros du programme Horizon 2020 dans ce PPPc et d'attirer 1,8 milliard d'euros supplémentaires provenant du secteur privé pour 2020 au plus tard. Le 31 décembre 2017, après une période de 18 mois, les fonds octroyés au titre d'Horizon 2020 s'élevaient à 67,5 millions d'euros et les investissements du secteur privé, à 1 milliard d'euros[79]

52 La lutte contre la cybercriminalité bénéficie également du soutien du volet «police» du Fonds pour la sécurité intérieure (FSI-Police). Le FSI-Police finance des études, des réunions d'experts et des activités de communication, auxquelles il a consacré près de 62 millions d'euros entre 2014 et 2017. Dans le cadre de la gestion partagée, les États membres peuvent en outre bénéficier de subventions d'équipement, de formation, de recherche et de collecte de données. Dix-neuf États membres ont fait appel à ces subventions, pour un montant de 42 millions d'euros.

53 Les fonds alloués au titre du programme «Justice», géré par la DG JUST, pour soutenir la coopération judiciaire et le fonctionnement des traités d'entraide judiciaire, avec un accent particulier sur l'échange de données électroniques et d'informations financières, se sont élevés à 9 millions d'euros.

54 La directive SRI prévoit explicitement que les CSIRT doivent disposer de ressources suffisantes pour pouvoir s'acquitter efficacement de leurs tâches[80]. Entre 2016 et 2018, 13 millions d'euros ont été mis à disposition chaque année au titre du mécanisme pour l'interconnexion en Europe. Les États membres pouvaient demander à s'en servir pour satisfaire aux exigences de la directive. Aucune étude n'a été menée pour déterminer les ressources financières dont le réseau des CSIRT et le groupe de coopération SRI auraient réellement besoin pour produire un impact.

55 Plusieurs agences ont spécifiquement axé leurs dépenses opérationnelles sur la cybersécurité ou les activités cybercriminelles. Il est toutefois difficile de dégager des chiffres précis des informations accessibles au public.

56 La convention de Budapest (voir point ***11***) constitue le fondement des dépenses externes de l'UE liées au cyberespace. L'Union a dépensé environ 50 millions d'euros pour renforcer la cybersécurité au-delà de ses frontières lors de la période 2014-2018. Près de la moitié de ce montant a été acheminée par l'intermédiaire de l'instrument contribuant à la stabilité et à la paix, et a bénéficié notamment à un grand projet (le projet GLACY+, doté de 13,5 millions d'euros) qui vise à renforcer dans le monde entier la coopération internationale et les capacités d'élaboration et de mise en œuvre d'une législation sur la cybercriminalité[81]. Par ailleurs, les dépenses au titre d'autres instruments de financement de l'UE ont été largement concentrées sur les Balkans occidentaux[82], ainsi que sur le voisinage européen, par exemple dans le cadre du projet Cybercrime@EAP, mené avec les pays du partenariat oriental et qui vise à améliorer la coopération internationale en matière de preuves électroniques et de lutte contre la cybercriminalité.

Autres dépenses de cybersécurité

57 Il n'est pas toujours possible de distinguer les dépenses spécifiquement liées à la cybersécurité dans les programmes de l'UE.

- Les financements d'Horizon 2020 ont aussi été acheminés par l'intermédiaire de l'entreprise commune «Composants et systèmes électroniques pour un leadership européen» (ECSEL) en ce qui concerne les systèmes cyber-physiques. Cependant, nous n'avons pas été en mesure de déterminer quels moyens avaient été spécifiquement consacrés à la cybersécurité dans le cadre des 27 projets financés au total à hauteur de 437 millions d'euros entre 2015 et 2016.

- Jusqu'à 400 millions d'euros sont disponibles au titre des Fonds structurels et d'investissement européens pour couvrir les dépenses liées à la cybersécurité et

aux services de confiance. Celles-ci concernent la sécurité et la protection des données et doivent permettre d'améliorer l'interopérabilité et l'interconnexion des infrastructures numériques, l'identification électronique, ainsi que les services de confiance et de protection de la vie privée.

58 Dans son plan d'activité 2018, la Banque européenne d'investissement a annoncé son intention d'augmenter le financement dans les domaines des technologies à double usage, de la cybersécurité et de la sécurité civile pour le porter à 6 milliards d'euros sur une période de trois ans[83].

Perspectives

59 Les 2 milliards d'euros prévus pour le volet cybersécurité du nouveau programme pour une Europe numérique proposé par la Commission[84] pour la période 2021-2027 sont destinés à renforcer le secteur de la cybersécurité et la protection globale de la société dans l'UE, y compris en contribuant à la mise en œuvre de la directive SRI. Le réseau de centres de compétences en cybersécurité et le centre de recherche et de compétences envisagés, dont l'objectif est d'introduire une approche plus rationnelle, sont censés constituer les principaux mécanismes d'exécution des dépenses au titre du programme pour une Europe numérique.

60 Les dépenses en matière de défense financées sur le budget de l'UE ont récemment augmenté avec le programme européen de développement industriel dans le domaine de la défense, doté de 500 millions d'euros pour la période 2019-2020[85] Ce programme doit servir à améliorer la coordination et l'efficience des dépenses des États membres en matière de défense grâce à des incitations au développement conjoint. L'objectif est de mobiliser au total 13 milliards d'euros d'investissements dans les capacités de défense après 2020 par l'intermédiaire du Fonds européen de la défense, dont une partie concerne la cyberdéfense[86].

Défi n° 5 – Attribution de ressources adéquates aux agences de l'UE

61 Les trois principaux organes au cœur de la politique de l'UE en matière de cybersécurité, à savoir l'ENISA, le centre EC3 d'Europol et la CERT-UE (voir ***encadré 2***), connaissent des problèmes de ressources en cette période où les priorités politiques axées sur la sécurité sont exacerbées. Avec la dotation actuelle en ressources humaines et financières des agences de l'UE, répondre aux attentes demeure un défi[87].

62 Les ressources supplémentaires réclamées par les agences pour répondre à la demande croissante ne leur ont été accordées qu'en partie, ce qui pourrait compromettre la réalisation (en temps utile) des objectifs stratégiques. À titre d'exemples:

- le caractère limité des ressources est l'un des facteurs qui ont empêché l'ENISA d'atteindre pleinement ses objectifs en 2017[88]. Une augmentation des ressources a été proposée dans le cadre du train de mesures de 2017 afin de permettre à l'ENISA de s'acquitter de ses nouvelles missions;

- le recrutement d'analystes et les investissements dans les capacités informatiques au centre EC3 d'Europol n'ont pas suivi la cadence de la demande[89]. De même, la Force d'action anticybercriminalité européenne (J-CAT) du centre EC3 d'Europol emploie des experts des États membres et de pays tiers chargés de soutenir les enquêtes fondées sur le renseignement. Mais les coûts sont supportés en grande partie par les États d'origine, ce qui ne les encourage pas à déployer des experts en plus grand nombre. Un déploiement temporaire au cas par cas a été imaginé, avec certains financements d'Europol et du cadre du cycle politique de l'UE, pour permettre à davantage de pays de participer.

63 Les agences s'imposent elles-mêmes certaines contraintes. Ainsi, bon nombre d'agents de la CERT-UE et de l'ENISA sont des agents contractuels, dont le recrutement implique des procédures généralement lentes. D'autres difficultés, comme celle d'attirer et de retenir des talents, résultent de l'incapacité des agences à concurrencer le secteur privé au niveau des salaires, ou des perspectives limitées qu'elles offrent en matière de progression de carrière. C'est pourquoi l'ENISA a sous-traité la plus grande partie de ses travaux entre 2014 et 2016[90].

64 Le manque de personnel et d'outils nécessaires peut entraîner un risque substantiel, notamment pour la collecte de renseignements sur les menaces. Le volume des données provenant de sources ouvertes et fermées ne cesse de croître et risque de dépasser les capacités des experts à analyser correctement les menaces. En l'absence de capacités et d'outils adéquats permettant de les intégrer et de les relier intelligemment entre elles, ces données ne seront pas traduites en renseignements utiles sur les menaces, susceptibles d'être partagés et analysés dans l'ensemble de l'UE[91].

Éléments de réflexion – Financement et dépenses

- Comment la Commission et les législateurs peuvent-ils rationaliser les dépenses de cybersécurité et les mettre plus explicitement en adéquation avec des objectifs clairement définis?

- Comment le problème de l'insuffisance des ressources allouées aux agences de l'UE peut-il être traité de manière globale compte tenu des besoins et des objectifs de l'Union?

- Quelles mesures sont définies au niveau de l'UE et dans les États membres pour réduire les obstacles qui empêchent les PME d'accéder à des capitaux leur permettant d'investir dans des activités à plus grande échelle?

- Quels résultats concrets et durables les fonds d'Horizon 2020 permettent-ils d'obtenir dans la mise au point de solutions de cybersécurité?

- Dans quelle mesure les efforts déployés par l'UE lui permettent-ils de renforcer les capacités en dehors de ses frontières dans le respect de ses propres valeurs?

Bâtir une société cyberrésiliente

65 La gouvernance en matière de cybersécurité concerne le traitement des menaces et des risques, le renforcement des capacités et de la prise de conscience, ainsi que la coordination et le partage d'informations fondés sur la confiance.

Défi n° 6 – Renforcer la gouvernance et les normes

Gouvernance en matière de sécurité de l'information

66 La gouvernance en matière de sécurité de l'information consiste à mettre en place des structures et des politiques permettant d'assurer la confidentialité, l'intégrité et la disponibilité des données. Plus qu'une simple question technique, elle requiert une direction efficace, des processus fiables et des stratégies conformes aux objectifs de l'organisation[92]. Un de ses volets est la gouvernance en matière de cybersécurité, qui traite de tous les types de menaces liées au cyberespace, y compris les attaques ciblées et sophistiquées, ainsi que les violations et incidents difficiles à détecter ou à gérer.

67 Au sein des modèles de gouvernance de la cybersécurité, qui varient d'un État membre à l'autre, les responsabilités en matière de cybersécurité sont souvent réparties entre différentes entités. Ces différences pourraient entraver la coopération nécessaire pour réagir aux incidents transfrontières à grande échelle, ainsi que l'échange de renseignements sur les menaces au niveau national et, a fortiori, à celui de l'UE. Notre enquête auprès des institutions supérieures de contrôle nationales a révélé que les faiblesses dans les dispositifs de gouvernance des autorités publiques et dans leur gestion des risques étaient perçues comme induisant les risques les plus élevés.

68 Même si les conséquences pour les organisations du secteur privé peuvent être graves, les faiblesses de la cybergouvernance sont légion. Près de neuf organisations sur dix déclarent que leur fonction de cybersécurité ne répond pas entièrement à leurs besoins[93], tandis que les responsables de la cybersécurité sont souvent séparés de l'organe directeur par au moins deux niveaux hiérarchiques[94].

69 Les directives de l'UE sur le droit des sociétés ne fixent pas d'exigences spécifiques concernant la communication d'informations sur les risques liés au cyberespace. Aux États-Unis, la commission des valeurs mobilières (*Securities and*

Exchange Commission) a récemment publié des orientations non contraignantes pour aider les entreprises publiques dans le choix des informations à communiquer sur les risques et les incidents liés à la cybersécurité[95]. Le comité mixte des autorités européennes de surveillance[96] (AES) a alerté sur l'augmentation des risques liés au cyberespace et encouragé les institutions financières à améliorer les systèmes informatiques fragiles et à étudier les risques inhérents à la sécurité de l'information, à la connectivité et à l'externalisation[97].

70 Renforcer la gouvernance des PME en matière de sécurité de l'information s'avère particulièrement difficile, étant donné que celles-ci sont, le plus souvent, incapables de mettre en œuvre les systèmes appropriés. Les PME ne disposent pas de lignes directrices appropriées sur l'application des exigences en matière de sécurité de l'information et de protection de la vie privée ni sur l'atténuation des risques technologiques[98]. Les principaux défis consistent donc à mieux comprendre leurs besoins et à prendre les mesures d'incitation et de soutien nécessaires.

71 L'absence de cadre de gouvernance cohérent au niveau international en matière de cybersécurité réduit la capacité de la communauté internationale à réagir aux cyberattaques et à les limiter. Il importe, dès lors, de parvenir à un consensus sur un cadre de gouvernance qui reflète au mieux les intérêts et les valeurs de l'UE[99]. Les tentatives visant à fixer des normes internationales contraignantes pour le cyberespace sont de plus en plus incertaines, comme le montre l'absence de consensus dégagé en 2017 au sein du groupe d'experts gouvernementaux des Nations unies sur la manière dont le droit international doit s'appliquer aux mesures prises par les pouvoirs publics face aux incidents.

72 Pour enrichir son programme de gouvernance du cyberespace, l'UE a également formalisé six partenariats afin d'établir un dialogue politique régulier visant à instaurer un climat de confiance et à créer des espaces communs de coopération[100]. Les effets sont mitigés, mais, globalement, sur le plan international, l'UE ne peut pas encore être considérée comme un «acteur majeur de la cybersécurité», même si elle a rehaussé son image[101].

Sécurité de l'information au sein des institutions de l'UE

73 Chaque institution de l'UE dispose de ses propres règles de gouvernance de la sécurité de l'information. Un accord interinstitutionnel prévoit que la Commission prête assistance aux autres institutions et aux agences en ce qui concerne la sécurité de l'information. Les institutions et organes de l'UE ont admis la nécessité de développer leurs capacités de cyberdéfense et leurs approches de la gestion des

risques de manière cohérente. En 2020, la Commission, le Conseil et le SEAE doivent présenter au groupe horizontal «Questions liées au cyberespace» un rapport sur la gouvernance et les progrès accomplis dans la clarification et l'harmonisation de la gouvernance en matière de cybersécurité au sein des institutions et des agences de l'UE[102].

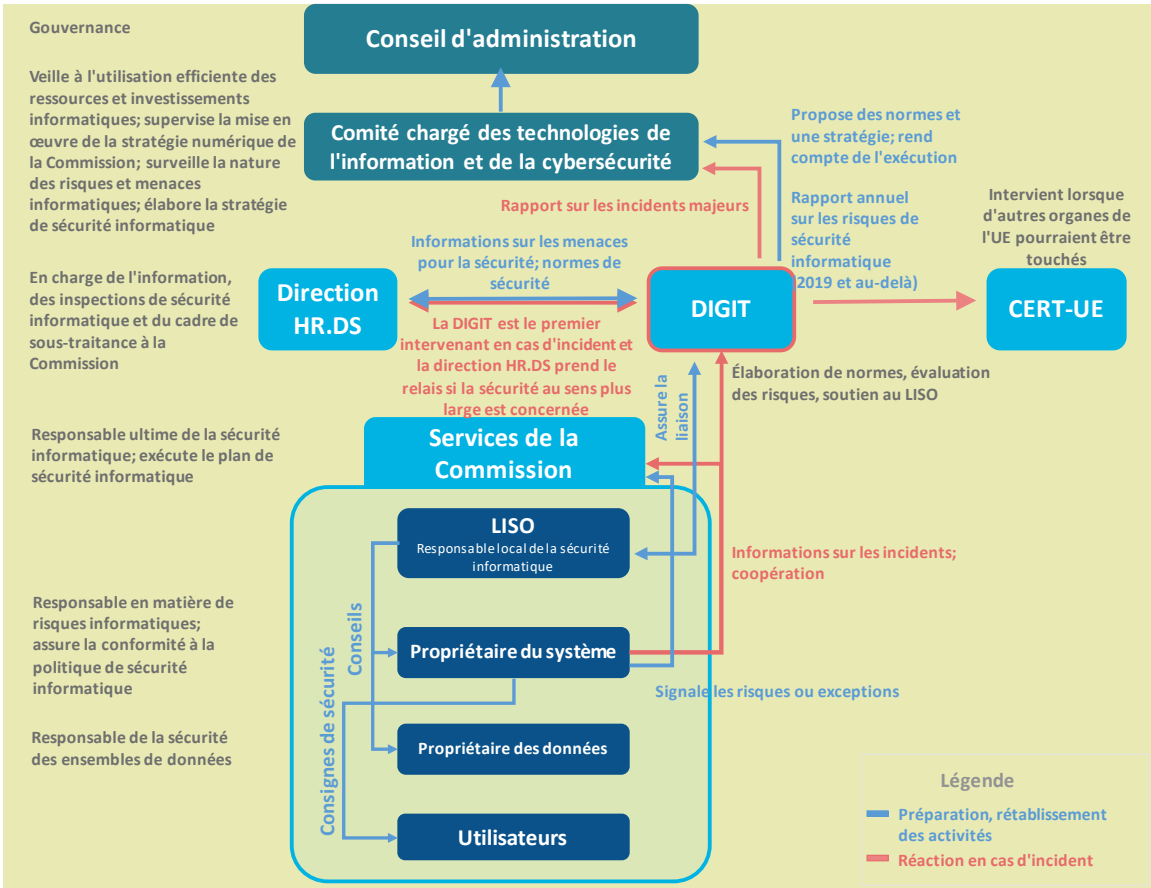
74 À la Commission, la direction générale de l'informatique (DIGIT) est responsable de la sécurité de l'infrastructure et des services informatiques (voir ***encadré 3***). En ce qui concerne la sécurité informatique, les principaux objectifs de la stratégie numérique de la Commission sont de l'intégrer dans les pratiques de gestion, d'assurer une infrastructure et une résilience efficaces (au regard des coûts), d'étendre la portée de la détection et de l'intervention en cas d'incident, ainsi que d'opérer une intégration de la gouvernance informatique et de la gouvernance en matière de sécurité[103]. Dans le cadre de son contrat de prestation de services, la Commission veille à ce que pratiquement tous les logiciels fassent l'objet d'une maintenance active, et à ce que seuls des logiciels bénéficiant d'un support fournisseur soient utilisés[104].

75 La nécessaire protection des institutions s'étend aussi aux missions et structures relevant de la PSDC de l'UE dans le monde entier. L'une des priorités du cadre stratégique de cyberdéfense de l'UE (version 2018) est de renforcer la protection des systèmes de communication et d'information relevant de la PSDC qui sont utilisés par les entités de l'Union. Un conseil interne de cybergouvernance a été créé au sein du SEAE et a tenu sa première réunion en juin 2017[105].

Encadré 3

Protection des systèmes d'information de la Commission

Les quelque 1 300 systèmes et 50 000 appareils de la Commission sont en permanence la cible de cyberattaques. La responsabilité en matière d'informatique est décentralisée, comme l'illustre la figure ci-après. La sécurité de l'information et celle des systèmes informatiques sont fondées sur un plan de sécurité informatique commun établi par la DIGIT. Le comité chargé des technologies de l'information et de la cybersécurité agit de fait en tant que responsable de la sécurité de l'information et assure le lien entre le volet opérationnel de la sécurité informatique et l'encadrement supérieur de la Commission, représenté par le conseil d'administration.



Source: Cour des comptes européenne, sur la base de décisions la Commission[106].

La direction «Sécurité» de la DG Ressources humaines et sécurité (DG.HR DS) a pour principale mission de protéger le personnel, les informations et les actifs de la Commission. Elle réalise également des enquêtes de sécurité concernant les incidents dont la dimension sécuritaire va au-delà de l'informatique, et qui entrent donc dans le champ de ses activités de contre-espionnage et de lutte contre le terrorisme.

La DIGIT est responsable de la sécurité informatique et héberge la CERT-UE (équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne). Instituée en 2011, la CERT-UE dispose d'un budget annuel de quelque 2,5 millions d'euros par an et emploie environ 30 agents. Elle est le premier intervenant pour tout incident relatif à la sécurité des informations qui touche plusieurs institutions, mais elle n'est pas opérationnelle 24 heures par jour et 7 jours par semaine. Elle accueille une plateforme de partage d'informations. En 2018, la CERT-UE a signé un protocole d'accord non contraignant avec l'ENISA, le centre EC3 et l'Agence européenne de défense en vue de renforcer la coopération et la coordination. Elle a également conclu un accord technique avec la capacité OTAN de réaction aux incidents informatiques (NCIRC).

Évaluations de la menace et des risques

76 Les évaluations bien fondées et continues de la menace et des risques sont des outils importants pour les organisations publiques et privées. Cependant, comme il n'existe pas d'approche commune en matière de classification et de cartographie des cybermenaces ou d'évaluation des risques, le contenu des évaluations est extrêmement variable, ce qui rend difficile l'application d'une approche cohérente de la cybersécurité à l'échelle de l'UE[107]. En outre, ces évaluations s'appuient souvent sur les mêmes sources, voire sur d'autres évaluations de la menace, ce qui donne lieu, comme par un effet d'écho, à la répétition des mêmes observations[108], au risque qu'une attention insuffisante soit accordée aux autres menaces. Ce phénomène est exacerbé par des réticences persistantes à partager les informations et par un sous-signalement des incidents.

77 La cellule de fusion contre les menaces hybrides[109] mise en place au sein du SEAE a été créée pour améliorer la connaissance des situations et appuyer la prise de décision grâce au partage d'analyses, mais elle doit élargir son champ d'expertise, notamment en matière de cybersécurité. En parallèle, la CERT-UE fournit aux institutions, organes et agences de l'UE des rapports et des notes d'information sur les cybermenaces qui les visent.

78 L'ENISA a fait observer par le passé que de nombreux États membres ont une perception qualitative des menaces et qu'il est nécessaire de modéliser davantage les cybermenaces[110]. Assurer le suivi des capacités d'analyse stratégique renforcera la compréhension commune. Cependant, l'évaluation des menaces pourrait se faire non seulement sur le plan technologique, mais également sur les plans sociopolitique et économique, ce qui permettrait de dresser un tableau plus complet. Elle pourrait couvrir en outre les éléments moteurs des menaces et les motivations de leurs auteurs.

Mesures incitatives

79 Les mesures juridiques et économiques incitant les organisations à signaler les incidents et à partager les informations sur ces derniers restent trop peu nombreuses. Par crainte pour leur réputation, beaucoup d'organisations préfèrent continuer à traiter les cyberattaques en toute discrétion ou payer les auteurs. Il reste à voir dans quelle mesure la directive SRI permettra effectivement d'augmenter le nombre des signalements. La Commission s'attend à ce que les améliorations se concrétisent avant tout au niveau national, mais le règlement sur la cybersécurité ajoutera une perspective européenne[111].

80 Lorsqu'elles acquièrent des produits et services numériques dans le cadre de marchés publics ou lorsqu'elles financent des programmes de recherche, les autorités publiques peuvent exercer une pression considérable sur les fournisseurs en intégrant certaines normes dans leurs cahiers des charges (par exemple en exigeant l'adoption de certaines normes techniques telles que le protocole internet IPv6 afin de faciliter la lutte contre la cybercriminalité). Il n'existe toutefois à l'heure actuelle aucun cadre de passation conjointe de marchés pour les infrastructures de cybersécurité[112]. De nombreuses possibilités s'offrent à la Commission pour remédier à cette situation. Le programme pour une Europe numérique proposé pour le prochain cadre financier pluriannuel vise à remédier au problème des investissements jusqu'ici limités du secteur public dans l'achat des technologies de cybersécurité les plus récentes.

81 En sa qualité d'autorité de régulation, la Commission peut veiller à ce que les normes appropriées soient élaborées puis adoptées à grande échelle afin de renforcer la sécurité. La Commission et Europol entretiennent avec les organes de gouvernance de l'internet tels que l'ICANN (voir point ***38***) et le RIPE-NCC[113], une collaboration indispensable à la mise en place d'une architecture de lutte contre la cybercriminalité permettant de faciliter le travail des autorités répressives et judiciaires.

Défi n° 7 – Développer les compétences et la prise de conscience

82 Comme l'a souligné l'ENISA, les utilisateurs jouent un rôle essentiel dans la lutte contre les cyberattaques et le renforcement des compétences, de la formation et de la prise de conscience est essentiel pour bâtir une société cyberrésiliente[114]. Que ce soit au travail ou dans la sphère privée, toute personne capable de détecter les signes avant-coureurs peut, avec les techniques appropriées, ralentir ou empêcher les attaques.

83 L'asymétrie croissante entre le savoir-faire nécessaire pour commettre un acte cybercriminel ou lancer une cyberattaque et les compétences requises pour y faire face est particulièrement inquiétante. Le modèle de service en ligne à la demande (*crime-as-a-service*) a réduit les obstacles à l'entrée sur le marché de la cybercriminalité: les personnes n'ayant pas les connaissances techniques pour créer des réseaux zombies, des kits d'exploitation ou des logiciels rançonneurs peuvent aujourd'hui en louer.

Formation, compétences et développement des capacités

84 Le monde connaît une pénurie croissante de compétences en cybersécurité. Ce déficit de main-d'œuvre s'est creusé de 20 % depuis 2015[115]. Les méthodes de recrutement traditionnelles ne permettent pas de répondre à la demande, notamment pour les postes d'encadrement et les fonctions interdisciplinaires[116]. Dans le domaine de la cybersécurité, près de 90 % de la main-d'œuvre mondiale est masculine. Cette faiblesse persistante de la mixité limite encore plus la réserve de talents disponibles[117]. Qui plus est, à l'université, les sujets liés au cyberespace sont sous-représentés dans les programmes non techniques.

85 La formation et l'enseignement sont nécessaires à tous les niveaux, pour les fonctionnaires, les membres des forces de l'ordre, les autorités judiciaires, les forces armées et le personnel enseignant. Les tribunaux doivent par exemple être capables d'appréhender les particularités techniques en mutation rapide de la cybercriminalité et de ses victimes[118], or il n'existe actuellement pas de normes de formation et de certification dans ce domaine à l'échelle de l'UE[119]. Il est important pour les institutions de l'UE de disposer d'un personnel possédant un éventail approprié de compétences. À défaut, elles pourraient se retrouver dans l'incapacité de définir correctement leur champ d'intervention, de trouver les bons partenaires et de déterminer les besoins en matière de sécurité, ou ne pas avoir les moyens de gérer leurs programmes. Il en va de l'efficacité des programmes de l'UE et de l'élaboration de ses politiques.

86 Si les politiques d'enseignement relèvent de la responsabilité des État membres, au niveau de l'UE, de nombreuses activités de formation (voir ***tableau 2***) et de nombreux exercices (voir ***encadré 4***) sont déjà organisés. L'UE peut faciliter l'intégration de normes européennes communes dans les programmes d'apprentissage, et ce dans toutes les disciplines concernées[120]. Par exemple, dans le domaine de la criminalistique numérique, des normes de formation communes sont indispensables pour ouvrir la voie à l'admissibilité des preuves dans les différents États membres. Parce que la cybercriminalité ne connaît pas de frontières, plusieurs juridictions peuvent être concernées, ce qui rend nécessaire une formation commune au niveau de l'UE. Malgré cela, selon le CEPOL, l'agence de l'UE en charge de la formation des services répressifs, plus de deux tiers des États membres ne proposent pas de formation régulière en cybersécurité aux agents des forces de l'ordre[121]. L'UE pourrait aussi éventuellement trouver comment mettre en place des synergies entre les domaines civil et militaire en matière d'enseignement et de formation[122]. Cela dit, l'ENISA a constaté que si l'offre de formation est actuellement étoffée dans les secteurs critiques, elle n'est pas suffisamment axée sur la résilience des infrastructures[123].

Tableau 2 — Exemples d'initiatives de formation de l'UE liées à la cybersécurité

Projets de l'Agence européenne de défense, par exemple le soutien aux exercices en matière de cyberdéfense par le secteur privé et le projet de plateformes informatiques de simulation en matière de cybersécurité (*cyber ranges*)	Formations civilo-militaires offertes par le réseau du Collège européen de sécurité et de défense, y compris une formation au cyberespace, des exercices d'entraînement et une plateforme d'évaluation	Formations de l'ENISA, qui propose des programmes de formations pas forcément disponibles sur le marché
Programmes de formation d'Europol, du CEPOL et de l'ECTEG[124] (y compris le modèle de gouvernance et le cadre de compétence en matière de formation, avec certification)	Réseau de centres de compétences et centre de recherche et de compétences (à l'examen)	Mesures sur le cryptage proposées dans le onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité
Coopération entre l'UE et l'OTAN en matière de formation à la cyberdéfense	Programme Erasmus militaire	Réseau européen de formation judiciaire

Source: Cour des comptes européenne.

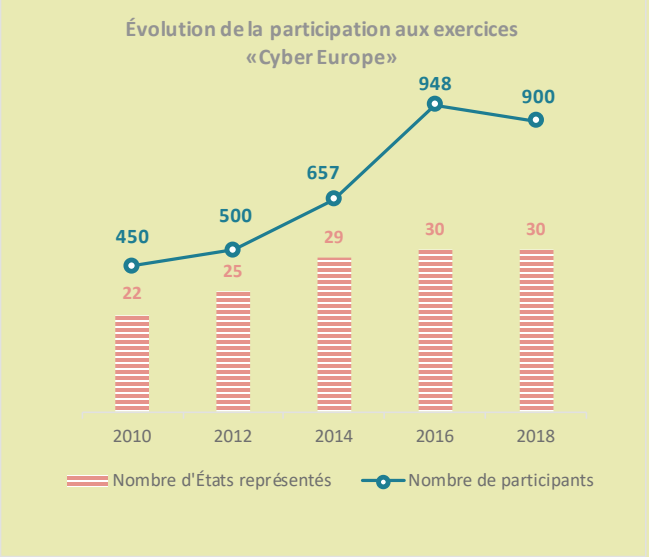
87 L'UE a détaché des experts de la lutte contre le terrorisme et de la sécurité dans 17 délégations pour renforcer le lien entre les dimensions intérieure et extérieure de sa sécurité[125]. Malgré les contraintes en matière de ressources, le renforcement des savoir-faire liés au cyberespace pourrait aider à mettre en place les projets appropriés, ainsi qu'à dégager des synergies avec d'autres programmes ou sources de financement[126]. Cela conférerait également à la cybersécurité une place plus en vue dans le dialogue politique, malgré la concurrence de nombreuses autres priorités, comme les migrations, la criminalité organisée ou le retour des combattants étrangers.

Encadré 4

Exercices

Les exercices sont une composante importante de l'enseignement et de la formation concernant le cyberespace. Visant à améliorer la préparation aux incidents, ils sont l'occasion rêvée de tester ses capacités et ses réactions en conditions réelles et de se constituer un réseau de relations de travail. Depuis 2010, leur fréquence a nettement augmenté.

Les participants y prennent part sur place ou à distance. Des évaluations sont organisées a posteriori pour dégager les enseignements tirés, même si ceux-ci ne percolent pas encore pleinement entre les différents niveaux (stratégique/politique, opérationnel et technique)[127].



Les exercices de cybersécurité phares de l'UE et de l'OTAN, à savoir «Cyber Europe» (de type opérationnel), organisé tous les deux ans, et Locked Shields (de type technique), qui a lieu chaque année, attirent plus de 1 000 participants provenant de quelque 30 pays. Ils sont tous deux centrés sur la protection et la préservation des infrastructures critiques dans des conditions d'attaque simulées. Ces exercices ont considérablement gagné en profondeur et comportent à présent tous les deux des éléments de politique médiatique, juridique et financière afin de permettre aux acteurs de terrain de mieux apprécier les situations. Les exercices parallèles et coordonnés PACE (de type stratégique) servent à tester l'interaction UE-OTAN dans un scénario de menace hybride.

Ces exercices internationaux ne sont pas les seuls. L'ENISA organise chaque année un exercice appelé «Cyber challenge», dans le cadre duquel des équipes s'affrontent pour résoudre des problèmes liés à la sécurité, concernant par exemple la sécurité sur le web et celle des appareils mobiles, les puzzles mathématiques, la rétroingénierie, l'éthique et la criminalistique. Le premier exercice EU CYBRID, qui met les ministres à l'épreuve en testant la prise de décision stratégique, a eu lieu en septembre 2017. En 2018, l'OTAN a co-organisé un exercice nommé «Crossed Swords» afin d'améliorer les aspects offensifs de son exercice Locked Shields. L'OTAN organise en outre des exercices appelés «Cyber Coalition».

L'une des principales difficultés est d'assurer la participation active de tous les acteurs importants et de coordonner tous ces exercices, pour éviter les doubles emplois et pour partager de manière efficiente les enseignements tirés.

Sensibilisation

88 Parce qu'ils sont susceptibles d'être exposés à leur insu aux failles d'appareils et de logiciels bon marché et largement répandus, ou d'être victimes de piratage psychologique, les citoyens sont souvent utilisés comme vecteurs pour lancer des attaques et diffuser de fausses informations. La sensibilisation est donc un élément indispensable de toute cyberrésilience efficace, même si la tâche n'est pas du tout

aisée, la complexité de la cybersécurité et les risques qui y sont associés étant difficiles à appréhender pour les non-initiés.

89 Le mois de sensibilisation à la cybersécurité en Europe (ECSM - *European Cyber Security Month*) et la Journée pour un Internet plus sûr sont des exemples d'initiatives de sensibilisation. Sept États non-membres de l'UE participent aujourd'hui à l'ECSM[128]. La campagne *Say No!* d'Europol vise à réduire le risque que des enfants soient victimes de coercition et d'extorsion sexuelles sur internet. Il est important de réduire ce risque car, actuellement, peu de victimes d'attaques portent plainte auprès de la police[129]. La Commission admet que la stratégie de cybersécurité n'a permis que de manière «partiellement efficace» de sensibiliser les citoyens et les entreprises[130]. Cette situation s'explique par l'ampleur de la tâche, la pénurie de ressources, l'engagement variable des États membres et le manque de preuves scientifiques sur la meilleure manière d'accroître et de mesurer la prise de conscience.

90 Le défi pour la Commission et les agences concernées consiste à veiller à ce que les actions de sensibilisation soient correctement ciblées et diffusées, inclusives et adaptées à la nature des menaces, ainsi qu'à éviter les effets tels que la «fatigue sécuritaire»[131] et à mettre au point des méthodes et des paramètres permettant d'évaluer l'efficacité de ces actions. Cela vaut également pour les institutions européennes elles-mêmes, où la culture de la sensibilisation doit être développée[132].

Défi n° 8 – Améliorer l'échange d'informations et la coordination

91 La cybersécurité exige une coopération entre les secteurs public et privé, notamment en matière de partage d'informations et d'échange de bonnes pratiques. La confiance est essentielle à tous les niveaux afin de créer un environnement propice à l'échange d'informations sensibles par-delà les frontières. Une mauvaise coordination est source de fragmentation, de doubles emplois et de dispersion de l'expertise. Une coordination efficace peut amener des succès tangibles, comme la fermeture de marchés sur les réseaux clandestins en ligne (*dark web*)[133]. En dépit des progrès réalisés ces dernières années, les niveaux de confiance restent «insuffisants»[134] au niveau de l'UE et dans certains États membres[135].

Coordination entre les institutions de l'UE et avec les États membres

92 L'un des objectifs de la stratégie de cybersécurité, et des structures de coopération instituées par la directive SRI, est de renforcer la confiance entre les

parties prenantes. Dans l'évaluation de la stratégie, les services de la Commission reconnaissent que les bases d'une coopération stratégique et opérationnelle au niveau de l'UE ont été jetées[136]. Malgré cela, ils estiment que la coordination est, d'une manière générale, insuffisante[137]. Le défi consiste à s'assurer que l'échange d'informations est non seulement pertinent, mais qu'il permet également d'obtenir une vision d'ensemble. Pour ce faire, il importe de parvenir à une conception commune fondée sur une terminologie reconnue (voir ***encadré 5***).

93 L'évaluation de l'ENISA indiquait toutefois que l'approche de l'UE en matière de cybersécurité n'était pas suffisamment coordonnée et que cela entraînait un manque de synergies entre les activités de l'ENISA et celles des autres parties prenantes. Les mécanismes de coopération sont encore relativement peu développés[138]; le règlement sur la cybersécurité doit permettre d'apporter une solution en renforçant le rôle de coordination conféré à l'ENISA. La volonté de renforcer la coopération est à la base du protocole d'accord signé en 2018 entre l'ENISA, l'AED, le centre EC3 d'Europol et la CERT-UE[139]. Pour les années à venir, l'une des priorités de la Commission sera d'assurer une bonne correspondance entre les initiatives stratégiques, les besoins et les programmes d'investissement afin de remédier à la fragmentation et de dégager des synergies[140].

94 Des fonctions de coordination ont été confiées à plusieurs instances institutionnelles. La *task force* sur l'union de la sécurité a été créée pour jouer un rôle central dans la coordination des différentes directions générales de la Commission, et ce dans le but de soutenir le programme relatif à l'union de la sécurité[141]. La DG CNECT dirige le sous-groupe de travail de la *task force* sur la cybersécurité.

95 Au Conseil, la cybersécurité est confiée au groupe horizontal «Questions liées au cyberespace», qui coordonne les questions stratégiques et horizontales relatives au cyberespace, et contribue à la préparation des exercices et à leur évaluation. Le groupe horizontal travaille en étroite collaboration avec le Comité politique et de sécurité, qui joue un rôle décisionnel central pour toutes les mesures diplomatiques liées au cyberespace (voir ***encadré 6*** dans la prochaine section). Compte tenu du caractère transversal de la cybersécurité, la coordination de tous les intérêts concernés n'est pas évidente: pas moins de 24 groupes de travail et instances préparatoires ont récemment traité de thèmes liés au cyberespace[142].

96 Les deux dernières propositions législatives concernant l'ENISA (2017) et l'établissement d'un réseau de centres de compétences en cybersécurité et d'un centre de recherche et de compétences (2018) sont spécifiquement destinées à éviter les doubles emplois et la dispersion des efforts. La mise en place du réseau et du

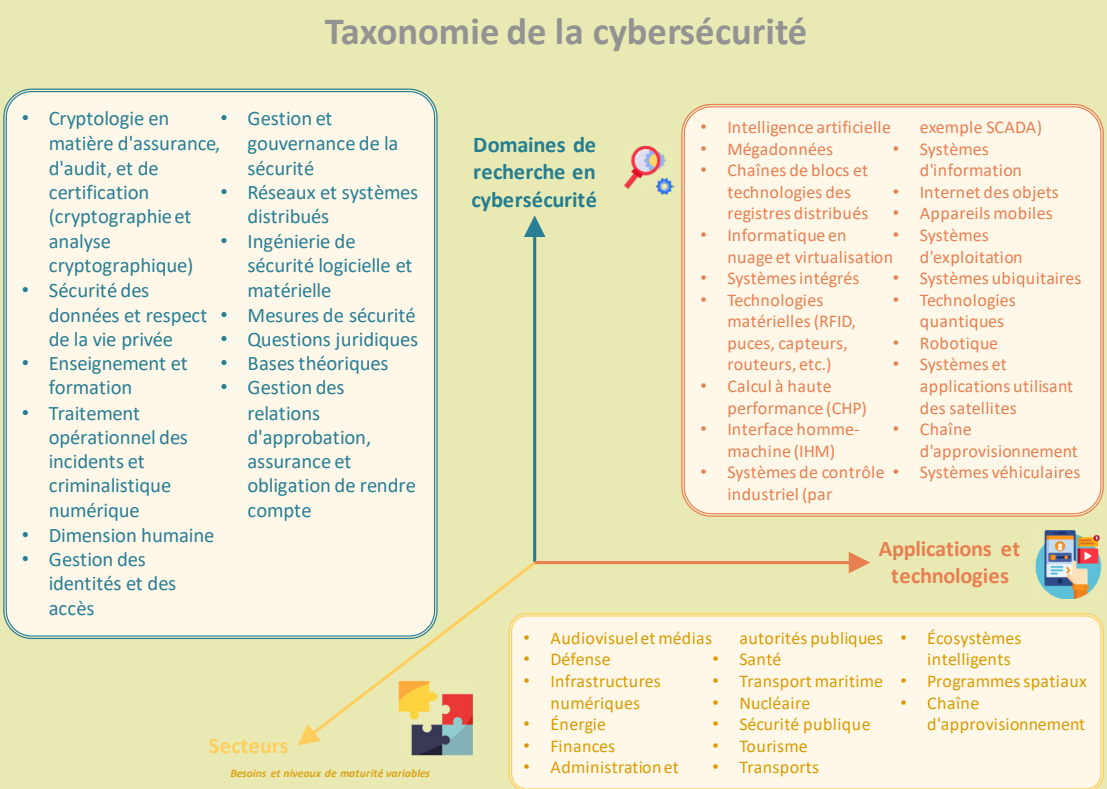
centre en question s'explique notamment par la nécessité de combler le vide laissé par les structures de coopération établies au titre de la directive SRI, lesquelles n'ont pas été conçues pour favoriser le développement de solutions de pointe.

Encadré 5

Pour un cyberlangage commun: *le souci de cohérence technologique*

La clarté terminologique permet de mieux apprécier les situations, d'améliorer la coordination[143] et de déterminer avec précision ce qui constitue une menace ou un risque.

Le Centre commun de recherche (JRC) de la Commission a récemment élaboré une taxonomie de recherche révisée, en se fondant sur différentes normes internationales[144]. L'idée est d'en faire un point de référence pour les entités de recherche dans toute l'Europe.



Source: Cour des comptes européenne, sur la base des informations communiquées par la Commission européenne.

Récemment encore, les institutions et agences de l'UE ne disposaient pas de définitions communes. Les choses sont en train de changer. Dans le cadre de son plan d'action, le groupe de coopération SRI a élaboré une taxonomie des incidents dans le but de favoriser une collaboration transfrontalière efficiente.

Coopération et échange d'informations avec le secteur privé

97 La coopération entre les autorités publiques et le secteur privé est essentielle pour renforcer les niveaux globaux de cybersécurité. Malgré cela, dans son évaluation 2017 de la stratégie de cybersécurité, la Commission a constaté que l'échange d'informations entre acteurs privés et entre les secteurs public et privé n'était pas encore optimal, en raison du manque de mécanismes de communication d'informations fiables et de mesures d'incitation au partage de l'information[145], et que cette situation entravait la réalisation des objectifs stratégiques. La Commission a en outre relevé l'absence d'un mécanisme de coopération efficace qui permettrait aux États membres d'œuvrer ensemble à renforcer durablement les capacités industrielles à grande échelle[146].

98 Les centres d'échange et d'analyse d'informations (ISAC) sont des organismes créés pour mettre en place des plateformes et fournir des ressources permettant de faciliter le partage d'informations entre les secteurs public et privé, ainsi que de recueillir des informations sur les cybermenaces. Ils visent à instaurer la confiance grâce au partage d'expériences, de connaissances et d'analyses, notamment en ce qui concerne les causes profondes, les incidents et les menaces. Il existe déjà des ISAC nationaux et sectoriels dans de nombreux États membres, mais leur nombre reste relativement limité au niveau européen[147]. Leur mise en place s'accompagne toutefois de nombreuses difficultés (contraintes en matière de ressources, difficulté à évaluer leur efficacité, établissement de structures appropriées pour associer à la fois le secteur public et le secteur privé, participation des autorités répressives) qu'il conviendra de surmonter pour que ces centres puissent contribuer à la mise en œuvre de la directive SRI et au développement des capacités en matière de sécurité à l'échelle de l'UE[148].

99 Une coopération étroite avec le secteur privé est capitale pour lutter contre les formes complexes de cybercriminalité, mais son efficacité varie d'un État membre à l'autre et dépend du climat de confiance[149]. Le centre EC3 d'Europol a néanmoins établi toute une série de groupes consultatifs constitués d'opérateurs du secteur privé, des institutions et agences de l'UE et d'autres organisations internationales, en vue d'améliorer la coopération grâce à la mise en réseau, au partage de renseignements stratégiques et à la coopération. Ces groupes consultatifs œuvrent à l'élaboration de plans conformes aux objectifs du cycle politique de l'UE[150]. Le recours au cryptage à des fins criminelles pose lui aussi de nombreuses difficultés et nécessite une coopération plus étroite avec le secteur privé. Le centre EC3 d'Europol examine actuellement différents moyens de faire détacher ponctuellement à la J-CAT (voir point ***62***) des experts universitaires et du secteur privé.

100 Les communautés civile et militaire, aussi bien publiques que privées, pâtissent de l'absence de mécanismes de coopération efficients. La cryptographie, les systèmes intégrés sécurisés, la détection de logiciels malveillants, les techniques de simulation, la protection des réseaux et des systèmes de communication et les technologies d'authentification figurent au nombre des domaines dans lesquels se posent des défis communs. Promouvoir la coopération entre civils et militaires et appuyer la recherche et la technologie (en particulier en soutenant les PME) sont deux des priorités du cadre stratégique de cyberdéfense de l'UE (dans sa version actualisée de 2018).

Éléments de réflexion – Renforcer la résilience

- Comment trouver le juste équilibre, au niveau de l'UE, entre la nécessité d'accorder une place importante à la politique de cybersécurité et celle d'assurer une coordination efficiente entre des acteurs variés aux responsabilités dispersées?
- Dans quelle mesure les institutions et agences de l'UE sont-elles prêtes à faire face à la prochaine attaque de grande envergure lancée directement contre elles?
- Comment rendre les agences de l'UE concernées par la cybersécurité plus attrayantes pour les talents?
- Quelles nouvelles mesures sont nécessaires pour garantir dans toutes les institutions et agences de l'UE des capacités suffisantes pour assurer un cadre d'évaluation des risques et des menaces qui soit cohérent?
- Comment les autorités européennes de surveillance (l'Autorité bancaire européenne, l'Autorité européenne des marchés financiers et l'Autorité européenne des assurances et des pensions professionnelles) traitent-elles les failles informatiques inhérentes au secteur financier, et quels enseignements peut-on en tirer pour les autres secteurs?
- Compte tenu du déficit général en expertise, comment utiliser au mieux l'assistance technique octroyée par l'UE aux autorités publiques pour assurer un impact global maximal sur le renforcement de la cyberrésilience?
- Comment assurer une participation significative de l'UE et des États membres à des discussions internationales qui façonnent la gouvernance et les normes du cyberespace, tout en promouvant les valeurs de l'UE?
- Aux niveaux de l'UE et des États membres, quelles mesures de sensibilisation (efforts de prévention compris) font vraiment la différence, et que peut faire l'UE pour les déployer à plus grande échelle?
- Quel rôle l'UE peut-elle jouer pour contribuer à assurer la mixité hommes-femmes dans le domaine de la cybersécurité?
- Que peuvent faire l'UE et les États membres pour améliorer les synergies entre les communautés civile et militaire, conformément au cadre stratégique de cyberdéfense de l'UE (dans sa version actualisée de 2018)?

Répondre efficacement aux cyberincidents

101 Il est essentiel d'élaborer une réponse efficace aux cyberattaques pour les arrêter le plus en amont possible. Il importe en particulier que les secteurs critiques, les États membres et les institutions de l'UE soient en mesure de réagir de manière rapide et coordonnée. Pour ce faire, une détection précoce est indispensable.

Défi n° 9 – Efficacité de la détection et de la réaction

Détection et signalement

102 Les outils de détection communs permettent de contrecarrer au quotidien la grande majorité des attaques[151]. Néanmoins, les systèmes numériques sont devenus si complexes qu'il est impossible de prévenir toutes les attaques. Leur degré de sophistication fait que les attaques échappent souvent à toute détection pendant de longues périodes. Selon les experts, l'accent devrait donc être mis sur la détection et la défense précoces[152]. Cependant, certains moyens de détection tels que l'automatisation, l'apprentissage automatique et l'analyse comportementale, qui ont pour objet de réduire les risques, d'analyser le comportement des systèmes et d'en tirer des enseignements, affichent de faibles taux d'adoption par les entreprises[153]. Cette situation s'explique en partie par l'existence de faux positifs, à savoir le fait que des activités non menaçantes soient considérées à tort comme malveillantes.

103 Dès qu'une violation est détectée et analysée, elle doit être rapidement signalée et notifiée afin que les autres entités publiques et privées puissent prendre des mesures préventives et que les autorités compétentes puissent aider ceux qui ont été touchés. De nombreuses organisations sont peu disposées à reconnaître et à signaler qu'elles ont fait l'objet de cyberincidents[154]. L'intervention précoce des autorités répressives dans la réaction initiale à des activités cybercriminelles présumées est également essentielle, de même que le partage préventif d'informations avec les CSIRT.

104 L'absence d'exigences communes au niveau de l'UE en matière de signalement des incidents qui prévalait autrefois risquait de retarder la communication des violations et de freiner leur traitement. L'introduction de la directive SRI visait à résoudre ce problème (voir point ***20***). À la suite des attaques *Wannacry* de 2017, la

Commission a conclu que le réseau des CSIRT «n'était pas encore pleinement opérationnel»[155]. Alors que la mise en application de cette directive se poursuit, il reste à voir si les orientations élaborées par le groupe de coopération SRI permettront effectivement de vaincre la réticence à signaler les incidents[156].

105 Dans certains secteurs, les opérateurs de services essentiels sont soumis à de multiples obligations de signalement (y compris aux consommateurs) découlant de la réglementation existante de l'UE, ce qui peut nuire à l'efficience du processus. Par exemple, dans les secteurs financier et bancaire, les opérateurs doivent respecter toute une série de critères, de normes, de seuils et de délais de signalement imposés par le RGPD, la directive SRI, la directive sur les services de paiement, la BCE et/ou le MSU, le système Target 2 et le règlement eIDAS[157]. Il importe donc de rationaliser ces obligations étant donné qu'une telle hétérogénéité alourdit inutilement la charge administrative et pourrait en outre entraîner une fragmentation de la communication d'informations.

Intervention coordonnée

106 La mise en place d'un cadre européen de coopération portant sur les crises de cybersécurité n'est pas encore achevée. Un plan d'action en ce sens[158] (voir point ***18***) a donc été mis sur pied pour introduire la dimension du cyberespace dans le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR), améliorer l'appréciation de la situation et assurer une meilleure intégration avec d'autres mécanismes de gestion de crise de l'UE[159]. Ce plan d'action associe les institutions, les agences et les États membres de l'UE. L'intégration harmonieuse de tous ces mécanismes de réaction en cas de crise est une gageure[160]. L'absence, pour l'heure, d'un réseau de communication sécurisé commun à l'ensemble des institutions de l'UE constitue également une lacune importante[161].

107 La capacité de l'UE à réagir aux cyberattaques sur les plans opérationnel et politique en cas d'incident transfrontière à grande échelle a été qualifiée de «limitée», notamment parce que la cybersécurité n'est pas encore intégrée dans les mécanismes de coordination de la réaction aux crises à l'échelle de l'UE[162]. La directive SRI ne règle pas ce problème.

108 La récente proposition de réforme de l'ENISA, qui prévoyait de lui conférer un rôle opérationnel plus important dans le traitement des incidents de cybersécurité majeurs, n'a pas été appuyée par les États membres, qui préfèrent que la mission de l'agence se limite à soutenir et à compléter leurs propres mesures opérationnelles[163]. Il

existe déjà de nombreux CERT/CSIRT au niveau des États membres, mais leurs capacités varient considérablement. Cette situation empêche toute coopération transfrontalière efficace, pourtant nécessaire pour faire face aux incidents majeurs[164].

109 En essayant de recenser tous les rôles confiés aux différents acteurs indiqués dans le plan d'action pour une réponse rapide et coordonnée à une cyberattaque majeure, nous avons relevé des lacunes qu'il conviendra de combler à mesure que la mise en œuvre progresse. Le maintien de l'ordre est un domaine qui n'a pas suffisamment été pris en compte au départ, même si le protocole de réaction d'urgence des services répressifs de l'UE a pris effet en décembre 2018[165]. Il est essentiel, pour la réussite de ce plan d'action, de veiller à ce qu'il soit pratique et à ce que toutes les parties sachent ce qu'elles ont à faire, ce qui nécessitera de procéder à des essais à grande échelle dans les années à venir.

110 Une réaction efficace ne se résume pas à la réduction des dommages; il est également essentiel d'établir les responsabilités en cas d'attaques. En raison de l'abus croissant des outils d'anonymisation, des cryptomonnaies et des systèmes de cryptage, il peut s'avérer très difficile de dépister et d'identifier les auteurs, en particulier dans le cas d'attaques hybrides. C'est ce que l'on appelle «le problème d'attribution des responsabilités». Il ne se pose pas uniquement sur le plan technique, mais également sur celui de la justice pénale. Les différences juridiques et procédurales entre les pays peuvent faire obstacle aux enquêtes pénales et aux poursuites à l'encontre des suspects. Pour trouver une solution au problème d'attribution des responsabilités, il sera nécessaire de formaliser davantage l'échange opérationnel d'informations, par exemple en mettant en place des procédures plus claires faisant intervenir Europol ou le réseau judiciaire européen en matière de cybercriminalité d'Eurojust.

111 Au niveau politique, une «boîte à outils cyberdiplomatique» (voir ***encadré 6***) a été élaborée pour faciliter le règlement pacifique des différends internationaux concernant le cyberespace. La création d'équipes d'intervention rapide en cas d'incident informatique et l'initiative d'assistance mutuelle dans le domaine de la cybersécurité sont deux projets favorisant un meilleur échange d'informations qui s'inscrivent dans le cadre de la CSP[166].

Encadré 6

La boîte à outils cyberdiplomatique

Le cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance[167], ou «boîte à outils cyberdiplomatique», est né des conclusions du Conseil de 2015 sur la diplomatie[168]. La cyberdiplomatie vise à élaborer et à appliquer une approche commune et globale du cyberespace, fondée sur les valeurs de l'UE, l'état de droit, le renforcement des capacités, les partenariats, la promotion du modèle de gouvernance multipartite de l'internet, la réduction des menaces qui pèsent sur la cybersécurité et une stabilité accrue des relations internationales.

La boîte à outils permet à l'UE et à ses États membres d'organiser une réponse diplomatique conjointe aux actes de cybermalveillance en tirant pleinement parti des mesures relevant de la politique étrangère et de sécurité commune. Il peut s'agir de mesures de prévention (sensibilisation, renforcement des capacités, etc.), de coopération, de stabilité ou de restriction (interdictions de voyager, embargos sur les armes, gels de fonds, etc.), ou encore de mesures de soutien aux réponses des États membres[169]. L'idée est qu'une coopération plus étroite en vue d'atténuer les menaces ainsi que l'envoi de signaux clairs sur les conséquences probables d'une réponse conjointe sont susceptibles de dissuader les comportements (potentiellement) agressifs.

Toute réponse diplomatique conjointe de l'UE face à des actes de cybermalveillance serait proportionnée à la portée, à l'ampleur, à la durée, à l'intensité, à la complexité, à la sophistication et à l'incidence de la cyberactivité.

Le succès de la boîte à outils sera aussi fonction de son imbrication avec le plan d'action pour une réponse rapide et coordonnée à une cyberattaque majeure et avec l'IPCR (voir point ***106***), de la mesure dans laquelle partage rapide et continu des informations (y compris sur les aspects liés à l'attribution des responsabilités) permet d'apprécier la situation[170] et, enfin, de l'efficacité de la coopération entre les différentes parties concernées. La réussite de son déploiement exigera également une communication efficace et coordonnée. Jusqu'ici, la boîte à outil a été utilisée à deux reprises: pour entamer un dialogue avec les États-Unis à la suite de l'attaque *Wannacry*[171], et pour élaborer les conclusions du Conseil condamnant l'utilisation malveillante des technologies de l'information et de la communication[172]. Sa mise en œuvre est en cours. Il reste à voir dans quelle mesure elle permettra d'atteindre efficacement les objectifs fixés.

Défi n° 10 – Protéger les infrastructures et fonctions sociétales critiques

Protéger les infrastructures

112 La plus grande partie des infrastructures critiques de l'UE fonctionnent grâce à des systèmes de contrôle industriel (SCI)[173]. Bon nombre de ces derniers ont été conçus en tant que systèmes autonomes, avec une connectivité limitée au monde extérieur. La connexion à internet de certains de leurs composants a rendu les SCI plus vulnérables aux interférences extérieures. Il n'est plus toujours possible d'assurer la maintenance des systèmes existants ou de leur appliquer des correctifs, mais leur modernisation ne peut se faire ni rapidement ni à moindre coût. Les efforts visant à renforcer la sécurité des infrastructures critiques doivent donc aussi consister à moderniser les SCI.

113 Alors que l'industrie continue à se numériser (sous l'appellation courante de «quatrième révolution industrielle»), l'impact d'un incident majeur dans un secteur industriel peut se répercuter ailleurs. L'ENISA a souligné l'importance de cartographier l'impact de l'interdépendance des secteurs critiques[174]. Une telle cartographie est essentielle pour comprendre la propagation potentielle d'un incident et sous-tend toute réponse bien coordonnée.

114 La directive SRI vise à améliorer la préparation dans les principaux secteurs responsables des infrastructures critiques. Cependant, tous les secteurs ne sont pas couverts (voir ***tableau 1***)[175], ce qui réduit l'efficacité de la stratégie[176]. L'une des grandes préoccupations à cet égard est la protection de l'intégrité des processus électoraux démocratiques contre toute atteinte aux infrastructures électorales et contre la désinformation (voir ***encadré 7***). Outre la révision de la législation existante, l'un des principaux défis consistera donc à associer ces secteurs à la mise en place de réponses efficaces à des incidents majeurs.

115 La vulnérabilité des infrastructures critiques ne s'arrête pas aux frontières de l'Europe. L'une des principales difficultés pour la Commission est d'encourager les pays candidats à adopter les mêmes normes que les États membres, par exemple dans des domaines tels que la législation relative au cyberespace ou la protection des infrastructures critiques.

Encadré 7

Protéger les fonctions sociétales critiques: *la lutte contre l'ingérence dans les élections*

En mai 2019, quelque 400 millions d'électeurs se rendront aux urnes pour les élections parlementaires européennes, les premières depuis l'entrée en vigueur du RGPD. Ces élections ont lieu au lendemain de scandales concernant l'utilisation abusive de données à caractère personnel à des fins de micro-ciblage politique et de campagnes de désinformation coordonnées sans précédent (phénomène dit des «fausses informations» ou «*fake news*» en anglais). La Commission a mis en garde contre de possibles ingérences dans ces élections[177], dont la prévention nécessitera une approche gouvernementale globale et une approche englobant l'ensemble de la société.

Infrastructures électorales

Organiser des élections est une tâche complexe, et la protection et l'intégrité du processus électoral relèvent de la responsabilité des États membres. L'ingérence dans les élections et les atteintes aux infrastructures électorales peuvent avoir pour but d'influer sur le choix des électeurs, sur leur participation ou sur le processus électoral lui-même, y compris le vote proprement dit, le dépouillement des bulletins ou la communication des résultats. Lors des élections du Parlement européen, la protection du «dernier kilomètre» (la communication des résultats depuis les capitales nationales vers Bruxelles) est un enjeu particulièrement important, étant donné qu'aucune approche commune en la matière n'a été adoptée ou testée[178].

Dans son dernier paquet électoral, la Commission a prévu des mesures pour renforcer la cybersécurité électorale, telles que la désignation de points de contact nationaux en charge de la coordination et de l'échange d'informations lors de la campagne précédant les élections. Le partage de bonnes pratiques et des enseignements tirés revêt une importance particulière à cet égard[179].

Les systèmes électoraux ne sont pas considérés comme faisant partie des infrastructures critiques[180], pas plus qu'ils ne sont couverts par la directive SRI. Malgré cela, le groupe de coopération SRI a élaboré des orientations pratiques sur la sécurité des technologies électorales à l'intention des autorités publiques. Les points de contact nationaux devraient se réunir début 2019[181]. Les États membres sont également encouragés à évaluer les risques de cybermenaces pesant sur leurs processus électoraux.

Désinformation

La désinformation est un élément de plus en plus important des attaques hybrides, qui associent cyberattaques et piratage des réseaux. Elle peut être utilisée pour diviser les sociétés, instiller la méfiance, saper la confiance dans les processus démocratiques ou semer le doute sur d'autres questions (par exemple la vaccination ou les changements climatiques). Elle a gagné en ampleur, en rapidité et en diversité et constitue une réelle menace sécuritaire pour l'UE.

L'Union a pris toute une série de mesures pour lutter contre la désinformation. Dès 2015, la *task force* «East StratCom» du SEAE a été mise en place pour contrer les campagnes de désinformation émanant de Russie[182]. Les experts ont salué son travail de promotion des politiques de l'UE, de soutien aux médias indépendants dans les pays du voisinage, ainsi que de prévision et de traçage de la désinformation et de lutte contre celle-ci[183]. Pourtant, les ressources de la *task force* sont limitées au regard de l'ampleur et de la complexité des campagnes de désinformation[184]. Une interaction plus systématique avec les structures de l'UE existantes et une meilleure coopération en matière de communication stratégique s'avèrent nécessaires[185]. Un nouveau plan d'action[186] a été adopté par le Conseil européen en décembre 2018.

Plus récemment, à la faveur de sa communication d'avril 2018 sur la lutte contre la désinformation en ligne[187], la Commission a élaboré, sur la base d'instruments stratégiques existants, un code volontaire de bonnes pratiques fondé sur l'autorégulation[188], auquel des plateformes en ligne et le secteur de la publicité ont adhéré[189]. L'idée est notamment d'aider à renforcer la fiabilité des contenus et de soutenir les efforts visant à améliorer l'éducation aux médias et aux informations. Un réseau européen indépendant de vérificateurs de faits a également été créé.

Selon la Commission, de nouvelles mesures réglementaires pourraient suivre si le code de pratiques n'est pas respecté. Il s'avérera crucial de déterminer l'efficacité des mesures, et plus particulièrement de décider comment évaluer les améliorations apportées sur les plans de la confiance, de la transparence et de l'obligation de rendre compte.

Un autre défi consistera à trouver des moyens d'améliorer la détection, l'analyse et la dénonciation des cas de désinformation[190]. Un suivi et une analyse dynamiques et stratégiques des sources de données ouvertes sont également nécessaires[191]. Les efforts visant à mieux appréhender les menaces dans leur contexte devraient également concerner les tendances émergentes, telles que les trucages vidéo élaborés (ou «*deepfakes*» en anglais, c'est-à-dire des vidéos truquées à l'aide de l'intelligence artificielle et de l'apprentissage automatique approfondi), ainsi que les outils nécessaires pour les détecter.

Renforcer l'autonomie

116 L'UE est un importateur net de produits et services de cybersécurité, ce qui augmente le risque de dépendance technologique et de vulnérabilité par rapport à des opérateurs de pays tiers[192]. Cette situation fragilise en particulier la sécurité des infrastructures critiques de l'UE, qui s'appuie également sur des chaînes d'approvisionnement mondiales complexes. Le risque s'accentue encore lorsque des opérateurs de pays tiers acquièrent des entreprises européennes de cybersécurité. Le filtrage des investissements directs étrangers (IDE) relève de la responsabilité des États membres et il n'existe actuellement aucun dispositif en la matière à l'échelle de l'UE[193].

117 Le renforcement de l'autonomie stratégique est un objectif de la stratégie globale de l'UE et de la communication de 2017 intitulée «Résilience, dissuasion et défense»[194]. Relever les multiples défis exposés dans le présent rapport contribuera au renforcement souhaité de cette autonomie. Aucune mesure ne permettra, à elle seule, d'atteindre cet objectif.

Éléments de réflexion – Réagir de manière efficace

- En quoi la directive SRI a-t-elle permis d'améliorer le signalement des cyberincidents dans les secteurs critiques et au-delà?
- Dans quelle mesure les institutions de l'UE internalisent-elles la coordination de la réaction aux crises en cas de cyberincident majeur?
- Comment la cyberdiplomatie peut-elle jouer un rôle plus éminent dans les actions extérieures de l'UE?
- Les structures et actions existantes, mises en place par l'UE pour lutter contre la désinformation, sont-elles adaptées à l'ampleur et à la complexité du problème?

Observations finales

118 Ces dernières années, l'UE et ses États membres ont érigé la cybersécurité en priorité, dans le but de renforcer la cyberrésilience. Assurer un degré plus élevé de cybersécurité dans l'UE reste toutefois une entreprise colossale. Dans le présent document d'information, nous avons cherché à mettre en évidence certains des grands défis que l'UE doit relever pour réaliser son ambition de disposer de l'environnement numérique le plus sûr au monde.

119 Notre examen montre qu'il est nécessaire de passer à une culture de la performance qui intègre des pratiques d'évaluation si l'on veut garantir **une réelle obligation de rendre compte et une véritable évaluation**. Certains **vides juridiques subsistent, et la législation existante n'est pas transposée uniformément par les États membres**. Cette situation pourrait empêcher la législation d'atteindre son plein potentiel. Un autre défi recensé concerne l'**alignement des niveaux d'investissement sur les objectifs stratégiques**, qui suppose d'accroître l'investissement global et d'en amplifier l'impact. La tâche est d'autant plus ardue que l'UE et ses États membres ne disposent pas d'une **vue claire des dépenses de l'UE** en matière de cybersécurité. Il est également fait état d'**obstacles rencontrés par les agences de l'UE concernées par la cybersécurité pour se doter de ressources adéquates,** y compris des difficultés à attirer et à retenir les talents.

120 Les études existantes concluent qu'il est **possible de renforcer la gouvernance de la cybersécurité** de manière à accroître la capacité de la communauté internationale à faire face aux cyberattaques et aux cyberincidents. Il est toutefois impossible de prévenir toutes les attaques. C'est pourquoi **la détection et la réaction rapides**, la **protection des infrastructures et fonctions sociétales critiques**, ainsi que l'amélioration de **l'échange d'informations et de la coordination** entre les secteurs public et privé sont des défis à relever en priorité. Enfin, compte tenu de la pénurie croissante de compétences en cybersécurité au niveau mondial, le **développement des compétences et de la prise de conscience** dans tous les secteurs et à tous les niveaux de la société représente également un défi de taille.

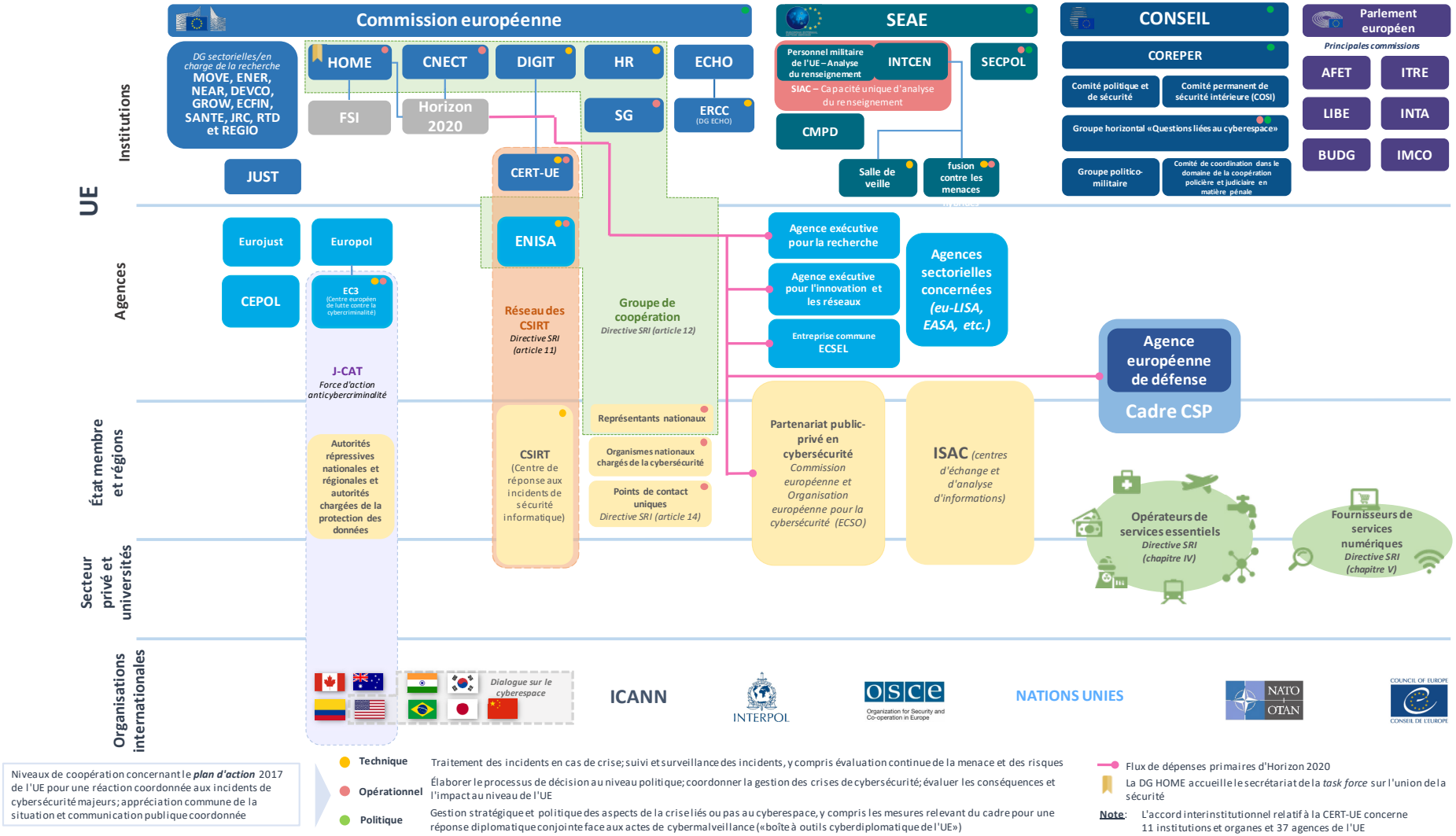
121 Relever les défis que représentent actuellement les cybermenaces pesant sur l'UE et sur le monde en général requiert un engagement continu et un attachement sans faille aux valeurs de l'Union.

Le présent document d'information a été adopté par la Chambre III en sa réunion du 14 février 2019.

Par la Cour des comptes

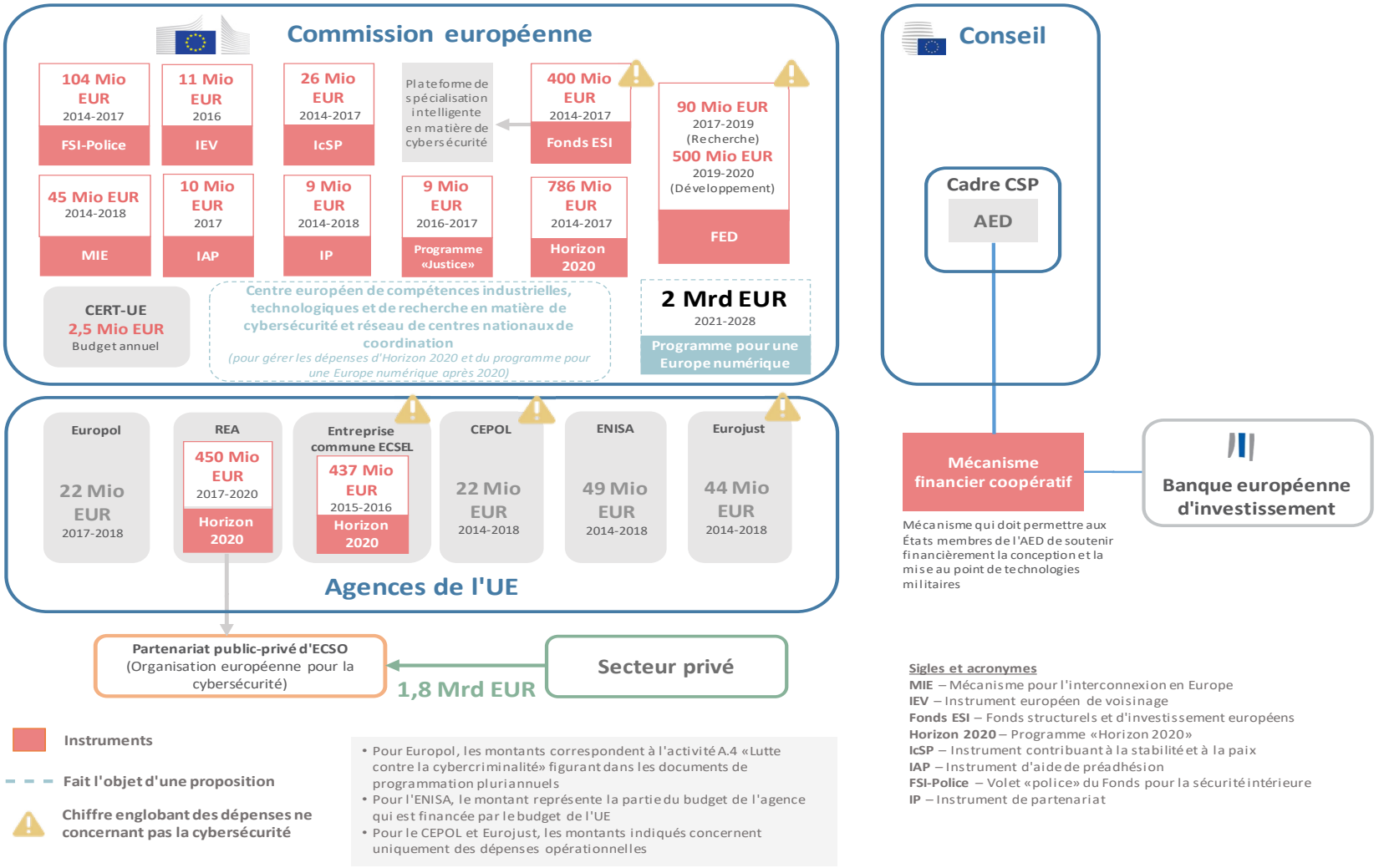
Klaus-Heiner Lehne
Président

Annexe I — Un paysage complexe et stratifié qui mobilise de nombreux acteurs



Source: Cour des comptes européenne.

Annexe II — Dépenses consacrées par l'UE à la cybersécurité depuis 2014



Source: Cour des comptes européenne, sur la base de documents de la Commission européenne et d'agences de l'UE.

Annexe III — Rapports des institutions supérieures de contrôle des États membres de l'UE

Type	Thème (et hyperlien vers le rapport)	Année	État membre
Audits de conformité	Note d'évaluation du contrôle interne	2014	FR
	Rapport de certification des comptes du régime général de la sécurité sociale (Défense et Affaires étrangères)	2016	FR
	Certification des comptes de l'État	2016	FR
	Assurer la sécurité et la préservation des bases de données nationales lituaniennes d'importance critique	Finalisé en 2018 / pas encore publié	EE
	Efficacité des contrôles internes dans la protection des données à caractère personnel contenues dans les bases de données nationales	2008	EE
Audits de la performance/de l'optimisation des ressources	Rapport sur l'atténuation des cyberattaques	2013	DK
	RiR 2014:23 Sécurité de l'information dans les administrations publiques civiles	2014	SE
	Rapport sur le traitement, par l'administration publique, des données confidentielles concernant les personnes et les entreprises	2014	DK
	Le programme national de cybersécurité	2014	UK
	Rapport présenté à la commission des budgets du Parlement fédéral allemand en application de l'article 88, paragraphe 2, du règlement financier fédéral (*Bundeshaushaltsordnung*) – Consolidation informatique au niveau du gouvernement fédéral	2015	DE
	Rapport sur l'accès aux systèmes informatiques utilisés pour fournir des services essentiels à la société danoise	2015	DK
	Établissement public d'aménagement de la Plaine de France	2015	FR
	L'environnement en matière de cybersécurité en Lituanie Version lituanienne Résumé traduit en anglais	2015	LT
	Exercice des missions de cybersécurité par les organismes publics en Pologne (en polonais)	2015	PL
	RiR 2015:21 Cybercriminalité – La police et le ministère public peuvent être plus efficients	2015	SE
	Enquête sur le déficit de compétences numériques dans l'administration publique	2015	UK
	Rapport au Parlement fédéral – Perception des droits de succession par le SPF Finances	2016	BE
	Rapport sur la gestion de la sécurité informatique des systèmes sous-traités à des prestataires externes	2016	DK
	Rapport d'audit sur les activités de prêt de l'Institut espagnol de crédit officiel pour l'exercice 2016	2016	ES

Type	Thème (et hyperlien vers le rapport)	Année	État membre
	Pilotage du réseau de sécurité de l'administration publique	2016	FI
	Assurer la sécurité des systèmes informatiques utilisés pour l'exercice des missions publiques	2016	PL
	Prévention et lutte contre le harcèlement en ligne chez les enfants et les jeunes	2016	PL
	Travaux en matière de sécurité de l'information au sein de neuf organismes - Nouvel audit sur la sécurité de l'information au niveau de l'État (RiR 2016:8)	2016	SE
	Protection de l'information aux différents niveaux de gouvernement	2016	UK
	Rapport sur la protection des systèmes informatiques et des données relatives à la santé dans trois régions danoises	2017	DK
	Note sur les résultats de l'audit parallèle international relatif à l'efficacité des contrôles internes dans la protection des données à caractère personnel contenues dans les bases de données nationales	2017	EE
	Dispositions en matière de protection contre les cyberattaques	2017	FI
	Orientation quant à la fiabilité opérationnelle des services électroniques	2017	FI
	Les chambres d'agriculture: façonner un réseau efficace (synthèse)	2017	FR
	Rapport sur la gestion de la chambre de commerce et d'industrie du Vaucluse (par la Chambre régionale des comptes - PACA)	2017	FR
	Assurer la sécurité et la préservation des bases de données nationales lituaniennes d'importance critique	Finalisé en 2018 / pas encore publié	EE
	Développement des infrastructures de communications électroniques de l'État Version lituanienne Résumé traduit en anglais	2017	LT
	Audit des technologie de l'information – La cybersécurité dans les entités de l'administration publique	2017	MT
	Le système des registres nationaux: sécurité, performance et facilité d'utilisation	2017	PL
	L'incident *WannaCry*	2017	UK
	La fraude en ligne	2017	UK
	Rapport sur la protection contre les attaques par logiciels rançonneurs	2018	DK
	Centre hospitalier d'Arpajon (par la Chambre régionale d'Île-de-France)	2018	FR
	Gestion des ressources en matière d'informations critiques de l'État	2018	LT
	Criminalité électronique	2019	LT
	Sécurité de l'information en Pologne	2019	PL
Divers	Bases de données des organismes publics	s.o.	BE
	Questionnaire sur la politique de sécurité et d'analyse des risques (en cours)	s.o.	BE

Acronymes et abréviations

AED – Agence européenne de défense

AES – Autorités européennes de surveillance

Cadre CSP – Cadre de coopération structurée permanente

CERT-UE – Équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne

CPSI – Comité de pilotage de la sécurité informatique

CSIRT – Centre de réponse aux incidents de sécurité informatique

DG HOME – Direction générale de la migration et des affaires intérieures

DG JUST – Direction générale de la justice et des consommateurs

DG CNECT – Direction générale des réseaux de communication, du contenu et des technologies

DIGIT – Direction générale de l'informatique

Directive SRI – Directive sur la sécurité des réseaux et de l'information

EC3 – Centre européen de lutte contre la cybercriminalité (Europol)

ECSEL — Composants et systèmes électroniques pour un leadership européen

ECSM – Mois de sensibilisation à la cybersécurité en Europe (*European Cyber-Security Month*)

ECSO – Organisation européenne pour la cybersécurité

ENISA – Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information

Fonds ESI – Fonds structurels et d'investissement européens

FSI - Police – Volet «police» du Fonds pour la sécurité intérieure

IDE – Investissements directs étrangers

ISC – Institution supérieure de contrôle

JRC – Centre commun de recherche

LISO – Responsable local de la sécurité informatique (*Local Information Security Officer*)

NCIRC – Capacité OTAN de réaction aux incidents informatiques

PME – Petites et moyennes entreprises

PPPc – Partenariat public-privé sur la cybersécurité

PSDC – Politique de sécurité et de défense commune

RGPD – Règlement général sur la protection des données

SEAE – Service européen pour l'action extérieure

UE – Union européenne

Glossaire

Clonage de carte – Vol de données de cartes de débit ou de crédit au moment de leur saisie en ligne.

Confidentialité – Protection des informations, des données et des avoirs contre tout accès non autorisé.

Contenu numérique – Toute donnée (telle que texte, son, image ou vidéo) stockée dans un format numérique.

Criminalité cyberdépendante – Infractions qui ne peuvent être commises qu'à l'aide de dispositifs informatiques.

Cryptage – Transformation d'informations lisibles en code indéchiffrable en vue de les protéger. Pour déchiffrer l'information, l'utilisateur doit avoir accès à une clé secrète ou à un mot de passe.

Cryptomonnaie – Actif numérique qui est émis et échangé au moyen de techniques de cryptage, indépendamment de toute banque centrale. Il est accepté comme moyen de paiement parmi les membres d'une communauté virtuelle.

Cyberattaque – Tentative de limiter ou de compromettre la confidentialité, l'intégrité et la disponibilité de données ou d'un système informatique via le cyberespace.

Cybercriminalité – Activités criminelles diverses impliquant des ordinateurs et des systèmes informatiques, en tant qu'outils ou cibles principaux. Il peut s'agir d'infractions classiques (fraude, établissement de faux, usurpation d'identité, etc.), d'infractions liées au contenu (comme la diffusion en ligne de matériel pédopornographique ou l'incitation à la haine raciale) et d'infractions spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service, logiciel malveillant, etc.).

Cyberdéfense – Volet de la cybersécurité visant à défendre le cyberespace par des moyens appropriés, militaires et autres, en vue d'atteindre des objectifs militaro-stratégiques.

Cyberécosystème – Désigne un ensemble complexe d'appareils, de données, de réseaux, de personnes, de processus et d'organisations qui interagissent, ainsi que l'environnement des processus et des technologies qui influent sur ces interactions et les rendent possibles.

Cyberespace – Environnement immatériel mondial dans lequel a lieu la communication en ligne entre les personnes, les logiciels et les services, par l'intermédiaire de réseaux informatiques et de dispositifs technologiques.

Cyberincident – Évènement qui compromet, ou menace de compromettre, directement ou indirectement, la résilience et la sécurité d'un système informatique et celles des données que ce système sert à traiter, à stocker ou à transmettre.

Cyberrésilience – Capacité à prévenir les cyberattaques et les cyberincidents, à s'y préparer, à y résister et à rétablir la situation.

Cybersécurité – Toutes les garanties et mesures adoptées pour défendre les systèmes informatiques et leurs données contre les accès non autorisés, les attaques et les dommages, de manière à assurer la confidentialité, l'intégrité et la disponibilité de ces dernières.

Déni de service distribué – Cyberattaque qui consiste à saturer de requêtes un service ou une ressource en ligne pour empêcher ses utilisateurs légitimes d'y accéder.

Désinformation – Informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public.

Disponibilité – Principe consistant à garantir que les informations sont accessibles et utilisables en temps utile et de manière fiable.

Donnée à caractère personnel – Toute information concernant une personne physique identifiable.

Données d'accès – Informations sur les connexions et les déconnexions d'un utilisateur à un service, telles que l'heure, la date et l'adresse IP.

Gestion des failles de sécurité – Partie intégrante de la sécurité des ordinateurs et des réseaux, elle vise, par la détection, la classification et la correction, à atténuer en amont ou à prévenir l'exploitation des vulnérabilités logicielles.

Hacktivistes: Individus ou groupes qui accèdent illégalement à des systèmes ou des réseaux informatiques dans le but de les utiliser à des fins politiques ou sociales.

Hameçonnage – Pratique consistant à envoyer des courriers électroniques supposés provenir d'une source fiable afin de tromper les destinataires pour qu'ils cliquent sur des liens malveillants ou qu'ils partagent des données à caractère personnel.

Informatique en nuage – Fourniture de ressources informatiques à la demande (par exemple stockage, puissance de calcul ou capacité de partage des données) sur internet, grâce à l'hébergement sur des serveurs distants.

Infraction facilitée par les TIC – Infraction classique commise à plus grande échelle à l'aide de systèmes informatiques.

Infrastructure électorale – Il s'agit notamment des systèmes informatiques et des bases de données servant aux campagnes électorales, ainsi que des informations sensibles concernant les candidats, l'inscription des électeurs et les systèmes de gestion.

Infrastructures critiques – Ressources physiques, services et installations dont l'arrêt ou la destruction aurait un impact grave sur le fonctionnement de l'économie et de la société.

Installation de correctifs – Introduction d'un ensemble de modifications dans un logiciel pour le mettre à jour, le réparer ou en améliorer le fonctionnement, y compris pour remédier aux failles de sécurité.

Intégrité – Principe consistant à prévenir la modification ou la destruction abusives de l'information et à en garantir l'authenticité.

Internet des objets – Réseau constitué d'objets de la vie quotidienne équipés de dispositifs électroniques, de logiciels et de capteurs qui leur permettent de communiquer et d'échanger des données via internet.

Kits d'exploitation – Sorte de boîte à outils utilisée par les cybercriminels pour exploiter les failles des réseaux et des systèmes d'information afin d'y introduire des logiciels malveillants ou de se livrer à d'autres activités malveillantes.

Logiciel malveillant d'effacement (*Wiper malware*) – Catégorie de logiciels malveillants destinés à effacer le contenu des disques durs des ordinateurs qu'ils contaminent.

Logiciel publicitaire – Logiciel malveillant qui affiche des bandeaux publicitaires ou des fenêtres contextuelles (*pop-ups*) comprenant des codes qui permettent de surveiller le comportement en ligne des victimes.

Logiciel rançonneur – Logiciel malveillant qui empêche les victimes d'accéder à un système informatique ou rend les fichiers illisibles, généralement par un procédé de cryptage. La plupart du temps, l'auteur fait ensuite chanter la victime en refusant de rétablir l'accès jusqu'à ce qu'une rançon soit versée.

Maliciel – Logiciel malveillant. Programme informatique conçu pour porter atteinte à un ordinateur, à un serveur ou à un réseau.

Menace hybride – Acte hostile commis par des adversaires au moyen d'une combinaison de techniques de guerre conventionnelles et non conventionnelles (à savoir des méthodes militaires, politiques, économiques et techniques), dans la poursuite acharnée de leurs objectifs.

Modèle *Crime-as-a-Service* – Modèle économique criminel de service en ligne à la demande qui sous-tend l'économie numérique souterraine en fournissant une vaste gamme de services commerciaux et d'outils permettant aux cybercriminels de base de commettre des méfaits.

Piratage psychologique – Dans le domaine de la sécurité de l'information, manipulation psychologique visant à tromper une personne pour l'amener à effectuer une action ou à divulguer des informations confidentielles.

Réseau zombie – Réseau d'ordinateurs contaminés par des logiciels malveillants et contrôlés à distance, à l'insu des utilisateurs, pour envoyer des courriers électroniques indésirables, voler des informations ou lancer des cyberattaques coordonnées.

Sécurité de l'information – L'ensemble des processus et outils de protection des données physiques et numériques contre tout accès, toute utilisation, toute divulgation, toute perturbation, toute altération, tout enregistrement ou toute destruction non autorisés.

Sécurité des réseaux – Volet de la cybersécurité consistant à protéger les données transmises au moyen d'appareils connectés à un même réseau, afin de garantir que les informations ne sont ni interceptées ni modifiées.

Services de confiance – Services qui renforcent la validité juridique d'une opération électronique, tels que les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, d'envoi recommandé électronique et d'authentification de site internet.

Système hérité – Système informatique, application ou langage de programmation obsolètes ou dépassés qui restent en usage, mais pour lesquels les mises à jour et le support fournisseur, y compris en matière de sécurité, peuvent ne plus être disponibles.

Vectorisation de texte – Procédé consistant à convertir des mots, des phrases ou des documents entiers en vecteurs numériques pouvant être utilisés par des algorithmes d'apprentissage automatique.

[1] Dans le projet de règlement de l'UE relatif à la cybersécurité, on entend par cybersécurité «toutes les activités nécessaires pour protéger les réseaux et les systèmes d'information, leurs utilisateurs et les personnes exposées contre les cybermenaces». Ce règlement devrait être adopté par le Parlement européen et le Conseil début 2019.

[2] Europol, *Internet Organised Crime Threat Assessment* (Évaluation de la menace que représente la criminalité organisée sur internet), 2017.

[3] Organisation européenne pour la cybersécurité (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, juin 2016.

[4] Parlement européen, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, étude réalisée pour la commission LIBE, septembre 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18 janvier 2018.

[6] Europol, *Internet Organised Crime Threat Assessment* (Évaluation de la menace que représente la criminalité organisée sur internet), 2018.

[7] Europol, *Ibid.*, 2018.

[8] Centre européen de politique économique internationale (ECIPE), *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, *Occasional Paper* n° 2/18, février 2018.

[9] Commission européenne, discours du président sur l'état de l'Union, 2017.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, communiqué de presse, 25 avril 2018.

[11] Europol, *Internet Organised Crime Threat Assessment* (Évaluation de la menace que représente la criminalité organisée sur internet), 2017.

[12] Commission européenne, Fiche d'information sur la cybersécurité, septembre 2017.

[13] Les coûts pourraient comprendre: le manque à gagner, les frais de réparation des systèmes endommagés, les responsabilités potentielles à supporter pour les avoirs et les informations volés, le coût des mesures de rétention de la clientèle, des primes d'assurance plus élevées, des coûts de protection plus élevés (nouveaux systèmes, nouveaux employés, nouvelles formations), ainsi que le règlement potentiel des frais de mise en conformité ou de litige.

[14] NTT Security, rapport *Risk:Value 2018*.

[15] Le logiciel rançonneur *Wannacry* exploitait les failles d'un protocole Microsoft Windows permettant la prise de contrôle à distance de tout ordinateur. Microsoft a déployé un correctif après la découverte de ces failles. Toutefois, des centaines de milliers d'ordinateurs n'avaient pas encore été mis à jour et un grand nombre d'entre eux ont été infectés. Source: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19 décembre 2017.

[16] Commission européenne, Eurobaromètre spécial 464a sur l'attitude des Européens à l'égard de la cybersécurité, septembre 2017. Une enquête de suivi devrait être publiée début 2019.

[17] La Convention de Budapest est un instrument international qui fournit des lignes directrices contraignantes pour tout pays élaborant une législation en matière de lutte contre la cybercriminalité. Elle établit un cadre pour la coopération internationale contre la cybercriminalité entre les États parties. Actuellement, l'UE y est représentée par la Commission, le Conseil de l'Union européenne, Europol, l'ENISA et Eurojust.

[18] Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure, *Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé*, JOIN(2013) 1 final du 7 février 2013.

[19] Commission européenne, *Le programme européen en matière de sécurité*, COM(2015) 185 final du 28 avril 2015.

[20] Commission européenne, *Stratégie pour un marché unique numérique en Europe*, COM(2015) 192 final du 6 mai 2015.

[21] SEAE, *Vision partagée, action commune: Une Europe plus forte. Une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne*, juin 2016.

[22] Centre d'études de la politique européenne, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, novembre 2018.

[23] Le logiciel malveillant utilisé pour perpétrer la cyberattaque *Wannacry*, attribuée à la Corée du Nord par les États-Unis, le Royaume-Uni et l'Australie, avait été initialement développé et stocké par l'Agence américaine de sécurité nationale pour exploiter les vulnérabilités de Windows. Source: A. Greenberg, ibid., WIRED, 19 décembre 2017. Au lendemain des attaques, Microsoft a dénoncé le fait que des gouvernements gardent le secret sur des failles logicielles et réitéré son appel à une convention de Genève numérique.

[24] Avec la terre, la mer, l'air et l'espace.

[25] Cadre stratégique de cyberdéfense de l'UE (version actualisée de 2018), document n° 14413/18 du 19 novembre 2018.

[26] Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure, *Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne*, JOIN(2016) 18 final du 6 avril 2016.

[27] Déclarations communes du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du traité de l'Atlantique Nord, 8 juillet 2016 et 10 juillet 2018.

[28] Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure, *Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide*, JOIN(2017) 450 final du 13 septembre 2017.

[29] 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).

[30] 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.

[31] Ces centres sont intégrés au sein de structures de coopération instituées par la directive, à savoir le réseau des CSIRT (composé des CSIRT désignés par les États membres et de la CERT-UE, l'ENISA accueillant le secrétariat) et le groupe de coopération SRI (qui soutient et facilite la coopération stratégique et l'échange d'informations entre les États membres, la Commission accueillant le secrétariat).

[32] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[33] Commission européenne, *Proposition de 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 (le «règlement sur la cybersécurité»)*, COM(2017) 477 final du 13 septembre 2017.

[34] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale*, COM(2018) 225 final, du 17 avril 2018.

[35] Commission européenne, *Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale*, COM(2018) 226 final du 17 avril 2018.

[36] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination,* COM(2018) 630 final du 12 septembre 2018.

[37] H. Carrapico et A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, volume 55, n° 6, 2017.

[38] Commission européenne, ibid., SWD (2017) 295 final du 13 septembre 2017.

[39] Service de recherche du Parlement européen, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, décembre 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27 novembre 2014.

[41] Sauf à l'article 14 («Suivi et statistiques») de la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

[42] Comité économique et social européen, *Cybersécurité: assurer la sensibilisation et la résilience du secteur privé à travers l'Europe face à la montée des risques cybernétiques*, mars 2018 (disponible uniquement en anglais). Task force du CEPS et de l'ECRI, *Cybersecurity in Finance: Getting the policy mix right!*, juin 2018.

[43] Sur 28 institutions supérieures de contrôle nationales, 24 ont répondu à notre enquête.

[44] À savoir fondé sur des principes et aussi technologiquement neutre que possible.

[45] Mécanisme de consultation scientifique de la Commission européenne, avis scientifique n° 2/2017, 24 mars 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, septembre 2018. Centre européen de politique économique internationale (ECIPE), ibid., *Occasional Paper No 2/18*, février 2018.

[47] Commission européenne, *Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique*, COM(2015) 634 final du 9 décembre 2015.

[48] Commission européenne, *Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de ventes en ligne et de toute autre vente à distance de biens* , COM(2015) 635 final du 9 décembre 2015.

[49] Cyber Security Raad (Pays-Bas), *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Centre d'études de la politique européenne, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force*, juin 2018.

[51] Commission européenne, *Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, COM(2017) 476 final/2 du 4 octobre 2017.

[52] Europol, Ibid., 2017.

[53] Conseil de l'Union européenne, *Rapport final sur la septième série d'évaluations mutuelles sur la mise en œuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci*, document n° 12711/1/17 REV 1 du 9 octobre 2017.

[54] Commission européenne, Analyse d'impact accompagnant la proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, SWD/2017/0298 final du 13 septembre 2017 (disponible uniquement en anglais). Un accord politique sur la nouvelle législation a été conclu en décembre 2018 et devrait être adopté début 2019.

[55] Europol, Ibid., 2017.

[56] Affaire C-362/14: Maximillian Schrems contre Data Protection Commissioner (Irlande), 6 octobre 2015.

[57] Europol et Eurojust, *Common challenges in combating cybercrime*, document n° 7021/17 du 13 mars 2017.

[58] Commission européenne, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD (2017) 295 final du 13 septembre 2017.

[59] Service de recherche du Parlement européen, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, *PE589.832*.

[60] Résolution du Parlement européen, *Droits de l'homme et technologies: incidences des systèmes de détection des intrusions et de surveillance sur les droits de l'homme dans les pays tiers* (2014/2232(INI)), 8 septembre 2015. Les biens et services à double usage, qui comprennent les logiciels et les technologies, peuvent avoir des applications aussi bien civiles que militaires.

[61] Les informations accessibles au public sont stockées dans la base de données WHOIS, gérée par l'ICANN (Société pour l'attribution des noms de domaine et des numéros sur internet). L'ICANN gère le système des noms de domaine. L'utilisation abusive des noms de domaine favorise la cybercriminalité.

[62] Directive SRI, article 3, ibid.

[63] Conseil de l'Atlantique, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10 septembre 2015.

[64] La Maison-Blanche, *Cybersecurity spending fiscal year 2019*.

[65] Commission européenne, *Document de travail des services de la Commission – Analyse d'impact accompagnant la «Proposition de règlement du Parlement européen et du Conseil établissant le programme pour une Europe numérique pour la période 2021-2027»*, SWD(2018) 305 final du 6 juin 2018 (disponible uniquement en anglais).

[66] Centre d'études stratégiques de La Haye, *Dutch investments in ICT and cybersecurity: putting it in perspective*, décembre 2016.

[67] Commission européenne, ibid., COM(2018) 630 final du 12 septembre 2018.

[68] Service de recherche du Parlement européen, Unité de la prospective scientifique, *Achieving a sovereign and trustworthy ICT industry in the EU*, décembre 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31 juillet 2017.

[70] Service de recherche du Parlement européen, Unité de la prospective scientifique, ibid., décembre 2017.

[71] Ibid.

[72] Commission européenne, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 final (partie 1/4) du 12 septembre 2018.

[73] Commission européenne, ibid., COM(2018) 630 final du 12 septembre 2018.

[74] Cour des comptes européenne, rapport spécial n° 13/2018 – «Lutte contre la radicalisation conduisant au terrorisme».

[75] Les chiffres cités dans cette section proviennent tous de documents de la Commission accessibles au public, sauf le montant de 42 millions d'euros cité au point ***51***, qui nous a été communiqué directement par la Commission.

[76] Horizon 2020 est le programme de recherche et d'innovation de l'UE. Doté de 80 milliards d'euros, il soutient la mise en œuvre de l'initiative phare «Union de l'innovation», qui vise à assurer la compétitivité de l'UE sur la scène mondiale.

[77] Défi de société n° 7 d'Horizon 2020, «Des sociétés sûres — protéger la liberté et la sécurité de l'Europe et de ses citoyens».

[78] Nous avons analysé les projets d'Horizon 2020 à l'aide de données extraites de CORDIS. Nous avons effectué une vectorisation de texte pour chaque description de projet, en suivant la taxonomie du JRC (voir ***encadré 5*** au prochain chapitre), pour déterminer quels projets étaient susceptibles d'être liés à la cybersécurité. Nous avons ensuite vérifié et analysé les résultats manuellement.

[79] Organisation européenne pour la cybersécurité, *ECS cPPP Progress Monitoring Report 2016-2017*, 29 octobre 2018.

[80] Directive SRI, article 9, paragraphe 2, ibid.

[81] Le projet GLACY+ (action globale sur la cybercriminalité élargie) est mené conjointement avec le Conseil de l'Europe. Il soutient 12 pays d'Afrique, d'Amérique latine, des Caraïbes et de la région Asie-Pacifique, qui pourraient ensuite servir de noyaux pour partager leur expérience au sein de leur région respective.

[82] Le Centre européen de stratégie politique (EPSC), groupe de réflexion au sein de la Commission européenne, a mis en garde contre le risque de voir apparaître un «angle mort numérique» si l'écart entre l'UE et ses voisins des Balkans occidentaux continue à se creuser. Des pays tels que la Chine et la Russie investissent des montants considérables dans la région, ce qui risque de marginaliser l'UE en tant qu'acteur du cyberespace dans la région. Source: EPSC, *Engaging with the Western Balkans: an investment in Europe's security*, 17 mai 2018.

[83] Banque européenne d'investissement, *Cadre opérationnel du Groupe BEI et Plan d'activité 2018*, 12 décembre 2017. Il n'y avait pas d'autres informations disponibles au moment de l'élaboration du présent document.

[84] Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant le programme pour une Europe numérique pour la période 2021-2027*, COM(2018) 434 final du 6 juin 2018.

[85] Commission européenne, *Règlement (UE) 2018/1092 du Parlement européen et du Conseil du 18 juillet 2018 établissant le programme européen de développement industriel dans le domaine de la défense visant à soutenir la compétitivité et la capacité d'innovation de l'industrie de la défense de l'Union* (JO L 200 du 7.8.2018, p. 30). En outre, une action préparatoire concernant la recherche en matière de défense a été mise en place en 2017. Dotée d'une enveloppe de 90 millions d'euros pour la période 2017-2019, elle est financée par Horizon 2020. Il est difficile de déterminer si ce montant comprend les dépenses liées au cyberespace.

[86] La Cour prévoit de publier un document d'information distinct sur la défense de l'UE courant 2019.

[87] Le centre EC3 d'Europol, l'ENISA, le SEAE, l'Agence européenne de défense et la CERT-UE disposent d'un effectif total de 159 personnes. Ce chiffre n'englobe pas le personnel chargé du cyberespace à la Commission européenne ou dans les États membres. Source: Centre d'études politiques européennes, ibid., novembre 2018.

[88] *Évaluation de l'ENISA*, 2017.

[89] Europol a demandé une augmentation annuelle des effectifs de 70 agents temporaires dans son plan pluriannuel 2018-2020, mais seuls 26 postes supplémentaires ont été approuvés pour 2018 Dans le prochain projet de plan pluriannuel, couvrant la période 2019-2021, Europol table sur une augmentation plus modeste, partant du principe qu'une demande de ressources plus conséquentes ne serait pas satisfaite. Source: Projet de programmation pluriannuelle 2019-2021 soumis au groupe de contrôle parlementaire conjoint d'Europol, document A000834 du 1er février 2018.

[90] *Évaluation de l'ENISA*, 2017. Entre 2014 et 2016, environ 80 % du budget opérationnel de l'ENISA a été utilisé pour commander des études.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, décembre 2017.

[92] ISACA (anciennement connue sous le nom d'Association des professionnels de la vérification et du contrôle des systèmes d'information), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, deuxième édition, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks.* 20ème enquête mondiale sur la sécurité de l'information, 2017, p. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy et H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, juillet 2017.

[95] Commission des valeurs mobilières des États-Unis, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21 février 2018.

[96] Forum de coopération entre l'Autorité bancaire européenne, l'Autorité européenne des marchés financiers et l'Autorité européenne des assurances et des pensions professionnelles.

[97] Autorité européenne des marchés financiers, *Joint Committee report on risks and vulnerabilities in the EU financial system*, avril 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, décembre 2015.

[99] En ce qui concerne les États membres de l'UE, le mécanisme de consultation scientifique de la Commission a relevé un degré élevé et unique de convergence quant aux principes et valeurs fondamentaux, ainsi qu'un intérêt stratégique partagé qui peut se retrouver au cœur d'une gouvernance de l'UE efficace en matière de cybersécurité. Source: Avis scientifique n° 2/2017 du 24 mars 2017.

[100] Avec les États-Unis, la Chine, le Japon, la Corée du Sud, l'Inde et le Brésil.

[101] Collège européen de sécurité et de défense (T. Renard et A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 23 novembre 2018.

[102] Conseil de l'Union européenne, *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'UE d'une cybersécurité solide*, document n° 15748/17 final du 12 décembre 2017.

[103] Commission européenne, *Stratégie numérique de la Commission européenne: Une Commission transformée numériquement, centrée sur l'utilisateur et fondée sur les données*, C(2018) 7118 final du 21 novembre 2018.

[104] Réponse de la commissaire Gabriel à une question parlementaire écrite (réf. E-004294-17), 28 juin 2017.

[105] Conseil de l'Union européenne, *Rapport annuel sur la mise en œuvre du cadre stratégique de cyberdéfense de l'UE*, 15870/17, 19 décembre 2017 (disponible uniquement en anglais).

[106] Les décisions 2015/443, 2015/444 et 2017/46 régissent la sécurité des systèmes de communication et d'information de la Commission. La décision C(2018) 7706 de la Commission du 21 novembre 2018 établit un comité chargé des technologies de l'information et de la cybersécurité, qui fusionne l'ancien comité chargé des technologies de l'information et le comité de pilotage de la sécurité informatique.

[107] Comité économique et social européen, ibid., mars 2018.

[108] Parlement européen, ibid., septembre 2015.

[109] La cellule de fusion contre les menaces hybrides a été mise en place en 2016 au sein du Centre de situation et du renseignement de l'UE, qui relève du SEAE. Elle reçoit et analyse des informations classifiées et de source ouverte sur les menaces hybrides, communiquées par différentes parties prenantes.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, novembre 2013.

[111] Commission européenne, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final du 13 septembre 2017 (partie 1 sur 6).

[112] Commission européenne, ibid., SWD(2018) 403 final du 12 septembre 2018.

[113] L'organisme «Réseaux IP Européens - Network Coordination Centre», registre internet régional pour l'Europe, est chargé de superviser l'attribution et l'enregistrement des ressources de numéros internet.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs*, novembre 2012.

[115] The Centre for Cyber Safety and Education, en partenariat avec Booz Allen Hamilton, Alta Associates et Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] Comité économique et social européen, ibid., mars 2018.

[117] Chambre des lords du Royaume-Uni, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19*, 16 juillet 2018.

[118] Europol et Eurojust, *Common challenges in combating cybercrime*, document n° 7021/17 du 13 mars 2017.

[119] Europol et Eurojust, ibid., document n° 7021/17 du 13 mars 2017.

[120] Commission européenne, ibid., SWD(2018) 403 final du 12 septembre 2018.

[121] CEPOL, *décision du conseil d'administration n° 33/2018/MB du 20 novembre 2018 relative au document de programmation unique du CEPOL pour la période 2020-2022* (disponible uniquement en anglais).

[122] Par exemple, une coopération entre le SEAE, les États membres et des agences et organes tels que le CEPOL, le groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG) ou le Collège européen de sécurité et de défense (CESD).

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, décembre 2017.

[124] Groupe européen de formation et d'enseignement sur la cybercriminalité.

[125] Commission européenne, *Treizième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective*, COM(2018) 46 final du 24 janvier 2018.

[126] Sur la base des observations du rapport spécial n° 14/2018, ibid.

[127] Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI)). Conseil de l'Union européenne, ibid., document n° 15870/17 du 19 décembre 2017.

[128] La Bosnie-Herzégovine, la Suisse, la Macédoine du Nord, le Kosovo (cette dénomination est sans préjudice des positions sur le statut et est conforme à la résolution 1244 du Conseil de sécurité des Nations unies ainsi qu'à l'avis de la CIJ sur la déclaration d'indépendance du Kosovo), la Turquie, l'Ukraine et les États-Unis.

[129] Europol, *Internet Organised Crime Threat Assessment* (Évaluation de la menace que représente la criminalité organisée sur internet), 2018.

[130] Commission européenne, ibid., SWD (2017) 295 final du 13 septembre 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman et S. Furman, *Security Fatigue*, IT Professional, volume 18, n° 5, 2016, p. 26 à 32. Voir également NIST.

[132] Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure, *Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides*, JOIN(2018) 16 final du 13 juin 2018.

[133] Par exemple, la fermeture d'AlphaBay et de Hansa dans le cadre d'opérations conjointes menées par le FBI et la police nationale néerlandaise avec l'appui d'Europol. Il s'agissait de deux des plus importants lieux d'échange de marchandises illicites telles des drogues, des armes à feu et des outils de cybercriminalité, comme les logiciels malveillants. Source: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, Communiqué de presse du 29 mai 2018.

[134] Commission européenne, ibid., SWD(2018) 403 final du 12 septembre 2018.

[135] Conseil de l'Union européenne, ibid., document n° 12711/17 REV 1 du 9 octobre 2017.

[136] Commission européenne, ibid., SWD (2017) 295 final du 13 septembre 2017.

[137] Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure, ibid., JOIN(2018) 16 du 13 juin 2018.

[138] Commission européenne, SWD (2017) 500 final du 13 septembre 2017.

[139] *Protocole d'accord entre l'ENISA, l'ADE, le centre EC3 d'EUROPOL et la CERT-EU*, 23 mai 2018.

[140] Appel d'offres de la Commission européenne – *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*, 27 octobre 2017.

[141] Jean-Claude Juncker, Lettre de mission adressée au commissaire chargé de l'union de la sécurité, 2 août 2016. Le domaine de la défense ne relève pas du mandat de la *task force*.

[142] Conseil de l'Union européenne, *EU Cybersecurity Strategy Roadmap – Finalisation*, document n° 8901/17 du 11 mai 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues, cinquième édition*, novembre 2017.

[144] Rapports techniques du JRC, *European Cybersecurity Centres of Expertise Map: Definitions and Taxonomy. Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres*, SWD(2018) 403 final du 12 septembre 2018.

[145] Commission européenne, ibid., SWD (2017) 295 final du 13 septembre 2017.

[146] Commission européenne, ibid., SWD(2018) 403 final du 12 septembre 2018.

[147] À titre d'exemple, le centre européen d'échange et d'analyse d'informations financières (*European FI-ISAC*) rassemble des représentants du secteur financier, des CERT nationales, des autorités répressives, de l'ENISA, d'Europol, de la Banque centrale européenne, du Conseil européen des paiements et de la Commission européenne.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14 février 2018.

[149] Conseil de l'Union européenne, ibid., document n° 12711/17 REV 1 du 9 octobre 2017.

[150] https://www.europol.europa.eu/empact.

[151] Une étude menée en 2018 par Accenture dans 15 pays a révélé que 87 % des cyberattaques ciblées étaient déjouées (*2018 State of Cyber Resilience*, 10 avril 2018).

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, Université d'Oxford, Politics Blog, 14 septembre 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14 juillet 2017.

[154] Comité économique et social européen, *ibid.*, mars 2018.

[155] Commission européenne, *Huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective*, COM(2017) 354 final du 29 juin 2017.

[156] Voir les différentes publications du groupe de coopération SRI.

[157] DSP2: directive sur les services de paiement 2; BCE/MSU: Banque centrale européenne/Mécanisme de surveillance unique; Target 2: système de transferts express automatisés transeuropéens à règlement brut en temps réel (de deuxième génération), règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Source: *task force* du CEPS et de l'ECRI, ibid., juin 2018.

[158] Commission européenne, *Recommandations sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs*, C(2017) 6100 final du 13 septembre 2017.

[159] Commission européenne, ibid., SWD (2017) 295 final du 13 septembre 2017. Il existe plusieurs mécanismes de gestion de crise, parmi lesquels le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR), Argus (le mécanisme de gestion de crise de la Commission), le mécanisme du SEAE de réaction en cas de crise, le mécanisme de protection civile de l'Union et le protocole de réaction d'urgence des services répressifs de l'UE.

[160] En outre, cela pourrait également entraîner le recours à l'article 42, paragraphe 7, du traité sur l'Union européenne (clause d'assistance mutuelle) et à l'article 222 du traité sur le fonctionnement de l'Union européenne (clause de solidarité).

[161] Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure, ibid., JOIN(2018) 16 du 13 juin 2018. En décembre 2018, la presse a fait état de cas de piratage présumé du réseau de communications diplomatiques du SEAE (source: *The New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*, 18 décembre 2018). Cette affaire fait actuellement l'objet d'une enquête.

[162] Il reste également des progrès à faire en ce qui concerne la coopération en matière d'alertes précoces et d'assistance mutuelle (voir *Projet de conclusions du Conseil sur la*

réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs, document n° 10085/18 du 26 juin 2018).

[163] Service de recherche du Parlement européen, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, septembre 2018.

[164] Comité économique et social européen, ibid., mars 2018.

[165] Conseil de l'Union européenne, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, document n° 14893/18, décembre 2018.

[166] Équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité; plateforme de partage d'informations en matière de réaction aux menaces et incidents informatiques. Source: Conseil de l'Union européenne, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*, 19 novembre 2018.

[167] Conseil de l'Union européenne, *Projet de conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance*, document n° 9916/17 du 7 juin 2017.

[168] Conseil de l'Union européenne, *Conclusions du Conseil sur la cyberdiplomatie*, document n° 6122/15 du 11 février 2015.

[169] Conseil de l'Union européenne, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, document n° 13007/17.

[170] L'établissement des responsabilités en cas d'incident reste une décision politique souveraine des États membres et n'est pas forcément requis pour toutes les mesures de la boîte à outils.

[171] La boîte à outils n'a pas permis d'agir de façon conjointe, différents États membres s'étant ralliés à la position des États-Unis.

[172] Conseil de l'Union européenne, *Conclusions du Conseil sur les actes de cybermalveillance*, document n° 7925/18 du 16 avril 2018.

[173] Systèmes informatiques utilisés pour contrôler les processus dans divers secteurs, tels que les services publics, la fabrication industrielle ou de produits chimiques, la transformation de denrées alimentaires, les systèmes et plateformes de transport et les services logistiques.

[174] ENISA, ibid., décembre 2017.

[175] Par exemple, les secteurs de l'administration publique, des industries chimique et nucléaire, de la manufacture, de la transformation de denrées alimentaires, du tourisme, de la logistique et de la protection civile.

[176] Commission européenne, ibid., SWD (2017) 295 final du 13 septembre 2017.

[177] Discours de la commissaire Jourová en session plénière du Parlement européen, *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign*, 14 novembre 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23 mai 2018.

[179] Centre européen de stratégie politique (Liisa Past), *Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses*, dans la publication intitulée «*Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats – A collection of think pieces of 35 leading practitioners and experts*», 2018.

[180] Au sens de la directive 2008/114/CE du Conseil concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

[181] Recommandation de la Commission sur les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité et la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen, C(2018) 5949 final du 12 septembre 2018.

[182] Conclusions du Conseil européen des 19 et 20 mars 2015 (EUCO 11/15). Deux *task forces* supplémentaires ont été mises en place depuis lors, sur les Balkans occidentaux et les pays du voisinage méridional.

[183] Dans un rapport, le Conseil de l'Atlantique a demandé à l'UE d'inviter tous les États membres à détacher des experts nationaux auprès de la *task force*. Voir: D. Fried and A. Polyakova, *Democratic Defense Against Disinformation*, 5 mars 2018.

[184] Dépourvue de budget propre au départ, elle s'est vu allouer 1,1 million d'euros en 2018 par le Parlement européen pour une action préparatoire «StratCom Plus».

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), ibid., 23 mai 2018.

[186] Communication conjointe de la Commission européenne et de la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, *Plan d'action contre la désinformation*, JOIN(2018) 36 final. Le plan d'action est axé sur: l'amélioration des capacités des institutions de l'UE à détecter, analyser et dénoncer les cas de désinformation; le renforcement des réponses coordonnées et conjointes; la mobilisation du secteur privé; la sensibilisation de la population et l'amélioration de la résilience de la société.

[187] Commission européenne, *Lutter contre la désinformation en ligne: une approche européenne*, COM(2018) 236 final du 26 avril 2018.

[188] À ne pas confondre avec le code de conduite pour lutter contre les discours haineux illégaux en ligne.

[189] Centre commun de recherche, *The digital transformation of news media and the rise of disinformation and fake news*, Rapports techniques du JRC, Document de travail du JRC sur l'économie numérique 2018-02, avril 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* avril 2018

[191] Centre européen de stratégie politique (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, dans: ibid, 2018.

[192] Commission européenne, ibid., SWD(2018) 403 final du 12 septembre 2018.

[193] La proposition de règlement (COM(2017) 487 final du 13 septembre 2018) établissant un cadre pour le filtrage des IDE, soumise en septembre 2017, suit actuellement le processus législatif. Elle concerne spécifiquement les technologies critiques, dont font partie l'intelligence artificielle et les applications à double usage.

[194] Communication conjointe de la Commission européenne et du Service européen pour l'action extérieure, ibid., JOIN(2017) 450 final du 13 septembre 2017.

Équipe de la Cour

Le document d'information «Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité» a été adopté par la Chambre III (Action extérieure/Sécurité et justice), présidée par M^{me} Bettina Jakobsen, Membre de la Cour. La mission a été effectuée sous la responsabilité de M. Baudilio Tomé Muguruza, Membre de la Cour, assisté de: M. Daniel Costa de Magalhaes, chef de cabinet; M. Ignacio Garcia de Parada, attaché de cabinet; M.°Alejandro Ballester-Gallardo, manager principal; M. Michiel Sweerts, chef de mission; M. Simon Dennett, M^{me} Aurelia Petliza, M. Mirko Iaconisi, M. Michele Scardone et M^{me} Silvia Monteiro Da Cunha, auditeurs; M. Johannes Bolkart, stagiaire. L'assistance linguistique a été assurée par M^{me} Hannah Critoph.

De gauche à droite: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph et Daniel Costa de Magalhaes.

COUR DES COMPTES EUROPÉENNE

Office des publications

COUR DES COMPTES EUROPÉENNE
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tél. +352 4398-1

Contact: eca.europa.eu/fr/Pages/ContactForm.aspx
Site web: eca.europa.eu
Twitter: @EUAuditors