COMMISSION
EUROPÉENNE

Bruxelles, le 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ANNEXE

de la

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

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

TABLE DES MATIÈRES

ANNEXE

1. Introduction

La présente annexe vise à contribuer à l'application, à la mise en œuvre et à l'exécution effectives de la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information dans l'Union européenne[1] (ci-après la «directive SRI» ou la «directive») et à aider les États membres à garantir une application efficace du droit de l'Union. Plus particulièrement, ses objectifs spécifiques sont triples: a) apporter davantage d'éclaircissements aux autorités nationales au sujet des obligations contenues dans la directive qui s'appliquent à ces autorités, b) assurer le respect effectif des obligations de la directive qui s'appliquent aux entités soumises à des obligations en matière d'exigences de sécurité et de notifications d'incidents, et c) contribuer globalement à créer une sécurité juridique pour tous les acteurs concernés.

À cette fin, la présente annexe fournit des orientations sur les aspects suivants, qui sont essentiels pour atteindre l'objectif de la directive SRI, à savoir garantir un niveau élevé commun de sécurité des réseaux et des systèmes d'information au sein de l'Union, qui sous-tendent le fonctionnement de notre société et de notre économie:

- l'obligation des États membres d'adopter une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information (section 2);
- la mise en place d'autorités nationales compétentes, de points de contact uniques et de centres de réponse aux incidents de sécurité informatique (CSIRT) (section 3);
- les exigences en matière de sécurité et de notification d'incidents applicables aux opérateurs de services essentiels et aux fournisseurs de service numérique (section 4); ainsi que
- la relation entre la directive SRI et d'autres textes législatifs (section 5).

Pour élaborer ces orientations, la Commission a utilisé les contributions et analyses recueillies lors de l'élaboration de la directive, ainsi que les informations fournies par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et le groupe de coopération. Elle s'est également appuyée sur les expériences de certains États membres. Le cas échéant, la Commission a tenu compte des principes directeurs pour l'interprétation du droit de l'Union: le libellé, le contexte et les objectifs de la directive SRI. Étant donné que la directive n'a pas encore été transposée, aucun arrêt de la Cour de justice de l'Union européenne (CJUE) ou des juridictions nationales n'a encore été rendu. Il n'est donc pas possible d'utiliser la jurisprudence comme guide.

[1] 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. La directive est entrée en vigueur le 8 août 2016.

La compilation de ces informations dans un document unique peut permettre aux États membres d'avoir une bonne vue d'ensemble de la directive et de tenir compte de ces informations lors de l'élaboration de leur législation nationale. Dans le même temps, la Commission souligne que la présente annexe n'a pas de caractère contraignant et n'a pas pour objet de créer de nouvelles règles. La compétence finale en matière d'interprétation du droit de l'Union incombe à la CJUE.

2. Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Conformément à l'article 7 de la directive SRI, les États membres sont tenus d'adopter une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui peut être considérée comme équivalente à une «stratégie nationale de cybersécurité» (SNCS). La fonction d'une stratégie nationale est de définir les objectifs stratégiques et les mesures politiques et réglementaires appropriées en matière de cybersécurité. Le concept de SNCS est largement utilisé au niveau international et en Europe, notamment dans le cadre des travaux menés par l'ENISA avec les États membres sur les stratégies nationales, qui ont récemment abouti à la mise à jour du guide des bonnes pratiques SNCS[2].

Dans cette section, la Commission précise comment la directive SRI renforce l'état de préparation des États membres en exigeant la mise en place de stratégies nationales solides en matière de sécurité des réseaux et des systèmes d'information (article 7). Cette section traite des aspects suivants: a) la portée de la stratégie, et b) le contenu et la procédure d'adoption.

Comme décrit plus en détail ci-dessous, la transposition correcte de l'article 7 de la directive SRI est fondamentale pour la réalisation des objectifs de la directive et nécessite l'allocation de ressources financières et humaines suffisantes à cette fin.

2.1. La portée de la stratégie nationale.

Conformément au libellé de l'article 7, l'obligation d'adopter une SNCS ne s'applique qu'aux secteurs visés à l'annexe II (c'est-à-dire l'énergie, les transports, les banques, le marché financier, le secteur de la santé, la fourniture et la distribution d'eau potable, et les infrastructures numériques) et aux services visés à l'annexe III (place de marché en ligne, moteurs de recherche en ligne et service d'informatique en nuage).

L'article 3 de la directive énonce expressément le principe d'harmonisation minimale, en vertu duquel les États membres peuvent adopter ou maintenir des dispositions en vue de parvenir à un niveau de sécurité plus élevé des réseaux de systèmes d'information. L'application de ce principe à l'obligation d'adopter une «SNCS» permet aux États membres d'inclure davantage de secteurs et de services que ceux couverts par les annexes II et III de la directive.

[2] ENISA, *National Cyber-Security Strategy Good Practice*, 2016. Disponible à l'adresse https://www.enisa.europa.eu/publications/ncss-good-practice-guide

De l'avis de la Commission et à la lumière de l'objectif de la directive SRI, à savoir assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information au sein de l'Union[3], il serait souhaitable d'élaborer une stratégie nationale qui englobe toutes les dimensions pertinentes de la société et de l'économie, et pas seulement les secteurs et les services numériques couverts respectivement par les annexes II et III de la directive SRI. Cela est conforme aux bonnes pratiques internationales (voir les orientations de l'UIT et l'analyse de l'OCDE mentionnées plus loin) et à la directive SRI.

Comme expliqué plus en détail ci-dessous, tel est notamment le cas des administrations publiques responsables de secteurs et de services autres que ceux énumérés dans les annexes II et III de la directive. Les administrations publiques peuvent traiter des informations sensibles, ce qui justifie la nécessité d'être couvertes par une SNCS et des plans de gestion qui permettent d'éviter les fuites et d'assurer une protection adéquate de ces informations.

2.2. Contenu et procédure d'adoption des stratégies nationales.

Conformément à l'article 7 de la directive SRI, une SNCS doit inclure au moins les éléments suivants:

i) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;
ii) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale;
iii) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé;
iv) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale;
v) un aperçu des plans de recherche et de développement;
vi) un plan d'évaluation des risques permettant d'identifier les risques; et
vii) une liste des différents acteurs concernés par la mise en œuvre de la stratégie.

Ni l'article 7 ni le considérant 29 correspondant ne précisent les exigences relatives à l'adoption d'une SNCS ou n'apportent plus de granularité au contenu de la SNCS. En ce qui concerne le processus et les éléments supplémentaires liés au contenu de la SNCS, la Commission considère l'approche exposée ci-après comme un moyen approprié d'adopter une SNCS. Elle se fonde sur l'analyse des expériences des États membres et des pays tiers quant à la manière dont les États membres ont élaboré leurs propres stratégies. Une autre source d'information est l'outil de formation SNCS de l'ENISA, disponible sous forme de clips vidéo et de supports téléchargeables sur son site internet[4].

2.3. Processus et questions à aborder.

Le processus d'élaboration et d'adoption ultérieure d'une stratégie nationale est complexe et comporte de multiples facettes. Il exige donc un engagement soutenu de la part des experts en

[3] Voir l'article 1er, paragraphe 1.
[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

matière de cybersécurité, de la société civile et de la sphère politique nationale, si l'on veut qu'il soit efficace et couronné de succès. Un soutien administratif de haut niveau, au moins au niveau du secrétaire d'État ou à un niveau équivalent dans le ministère de tutelle, ainsi qu'un parrainage politique sont des conditions indispensables à cet égard. Pour réussir l'adoption d'une SNCS, on peut envisager un processus en cinq étapes (voir l'illustration 1):

Première étape - **Établissement des principes directeurs et des objectifs stratégiques découlant de la stratégie.**

Tout d'abord, les autorités nationales compétentes devraient définir certains éléments clés à inclure dans la SNCS, à savoir les résultats souhaités [dans le libellé de la directive (article 7, paragraphe 1, point a), «*les objectifs et les priorités*»], la manière dont ces résultats complètent les politiques sociales et économiques nationales et la mesure dans laquelle ils sont compatibles avec les privilèges et obligations découlant de la qualité d'État membre de l'Union européenne. Les objectifs doivent être spécifiques, mesurables, atteignables, réalistes et limités dans le temps (SMART). Un exemple illustratif est le suivant: «*Nous veillerons à ce que cette stratégie [limitée dans le temps] soit fondée sur un ensemble solide et complet de paramètres de mesure par rapport auxquels nous mesurons les progrès accomplis en vue d'atteindre les résultats escomptés.*»[5].

Cette première étape inclut également une évaluation politique visant à déterminer s'il est possible d'obtenir un budget important pour financer la mise en œuvre de la stratégie. Elle comprend aussi une description de la portée prévue de la stratégie et des diverses catégories d'intervenants des secteurs public et privé qui devraient participer à la définition des divers objectifs et mesures.

Cette étape pourrait être accomplie par le biais d'ateliers ciblés destinés à de hauts fonctionnaires ministériels et responsables politiques, animés par des cyberspécialistes dotés de compétences professionnelles en communication et capables de mettre en lumière les implications d'une cybersécurité faible ou inexistante pour une économie et une société numériques modernes.

Deuxième étape - **Développement du contenu de la stratégie.**

La stratégie devrait prévoir des mesures habilitantes, des actions fondées sur le temps et des indicateurs de performance clés pour l'évaluation, le perfectionnement et l'amélioration qui en résultent, après une période de mise en œuvre définie. Ces mesures devraient appuyer l'objectif, les priorités et les résultats énoncés à titre de principes directeurs. La nécessité d'inclure des mesures habilitantes est énoncée à l'article 7, paragraphe 1, point c), de la directive SRI.

Il est recommandé qu'un groupe de pilotage présidé par le ministère responsable soit formé pour gérer le processus de rédaction et favoriser les contributions. Cela pourrait être réalisé par le biais d'un certain nombre de groupes de rédaction composés de fonctionnaires et

[5] Extrait de la stratégie nationale en matière de cybersécurité du Royaume-Uni, 2016-2021, page 67.

d'experts compétents sur des thèmes génériques clés, par exemple l'évaluation des risques, la planification d'urgence, la gestion des incidents, le développement des compétences, la sensibilisation, la recherche et le développement industriel, etc. Chaque secteur (par exemple, l'énergie, les transports, etc.) serait également invité à évaluer les implications de son inclusion, y compris en matière de ressources, et à associer les opérateurs désignés de services essentiels et les principaux fournisseurs de service numérique à la définition des priorités et à la soumission de propositions pour le processus de rédaction. La participation des parties prenantes sectorielles est également essentielle, compte tenu de la nécessité d'assurer une mise en œuvre harmonisée de la directive dans différents secteurs, tout en tenant compte des spécificités sectorielles.

Troisième étape - **Élaboration d'un cadre de gouvernance.**

Pour être efficace et efficient, le cadre de gouvernance doit reposer sur les principales parties prenantes, les priorités définies lors du processus de rédaction, ainsi que les contraintes et le contexte associés aux structures administratives et politiques nationales. Il serait souhaitable d'instaurer une relation directe avec le niveau politique, dans la mesure où le cadre implique une capacité de prise de décision et d'affectation des ressources, ainsi que la contribution d'experts en cybersécurité et d'intervenants de l'industrie. L'article 7, paragraphe 1, point b), de la directive SRI mentionne le cadre de gouvernance et prévoit spécifiquement «*les responsabilités des organismes publics et des autres acteurs pertinents*».

Quatrième étape - **Compilation et examen du projet de stratégie.**

À ce stade, le projet de stratégie devrait être compilé et examiné au moyen d'une analyse des forces, faiblesses, opportunités et menaces (SWOT), qui pourrait permettre de déterminer s'il convient de réviser le contenu. À la suite de l'examen interne, une consultation des parties prenantes devrait avoir lieu. Il serait également essentiel d'entreprendre une consultation publique afin de souligner l'importance de la stratégie proposée auprès du public, de recueillir les commentaires de toutes les sources possibles et de solliciter l'appui des ressources nécessaires à la mise en œuvre ultérieure de la stratégie.

Cinquième étape – **Adoption formelle.**

Cette dernière étape suppose une adoption formelle au niveau politique avec un budget habilitant qui reflète l'importance que l'État membre concerné accorde à la cybersécurité. Pour atteindre les objectifs de la directive SRI et, lors de la communication du document de stratégie nationale à la Commission conformément à l'article 7, paragraphe 3, la Commission encourage les États membres à fournir des informations sur le budget. Les engagements concernant le budget et les ressources humaines nécessaires sont absolument essentiels pour une mise en œuvre efficace de la stratégie et de la directive. Dans la mesure où la cybersécurité est un domaine des politiques publiques encore relativement nouveau et en pleine expansion, de nouveaux investissements sont nécessaires dans la plupart des cas, même si la situation générale des finances publiques exige des réductions et des économies.

Des conseils sur le processus d'élaboration et le contenu des stratégies nationales sont disponibles auprès de diverses sources publiques et universitaires, par exemple l'ENISA[6], l'UIT[7], l'OCDE[8], le Forum mondial sur la cyber-expertise et l'Université d'Oxford[9].

2.4. Mesures concrètes que les États membres doivent prendre avant la date limite de transposition.

Avant l'adoption de la directive, presque tous les États membres[10] avaient déjà publié des documents désignés comme constituant une SNCS. La section 6 de la présente annexe énumère les stratégies actuellement en place dans chaque État membre[11]. Elles comprennent généralement des principes, des lignes directrices, des objectifs stratégiques et, dans certains cas, des mesures spécifiques visant à atténuer les risques associés à la cybersécurité.

Étant donné que certaines de ces stratégies ont été mises en place avant l'adoption de la directive SRI, elles ne contiennent pas nécessairement tous les éléments énoncés à l'article 7. Afin d'assurer une transposition correcte, les États membres devront procéder à une analyse des lacunes en faisant correspondre le contenu de leur SNCS aux sept exigences distinctes énumérées à l'article 7 pour l'ensemble des secteurs visés à l'annexe II de la directive et des services visés à l'annexe III. Les lacunes recensées pourront ensuite être comblées par une révision de leur SNCS existante ou en décidant d'une révision complète des principes de leur stratégie nationale en matière de SRI. Les lignes directrices ci-dessus relatives au processus d'adoption d'une SNCS sont également pertinentes pour la révision et la mise à jour d'une SNCS existante.

---

[6] ENISA, *National Cyber-Security Strategy Good Practice*, 2016. Disponible à l'adresse https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] UIT, *National Cybersecurity Strategy Guide*, 2011. Disponible à l'adresse http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
L'UIT publiera également une boîte à outils sur la stratégie nationale en matière de cybersécurité en 2017 (voir la présentation à l'adresse http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

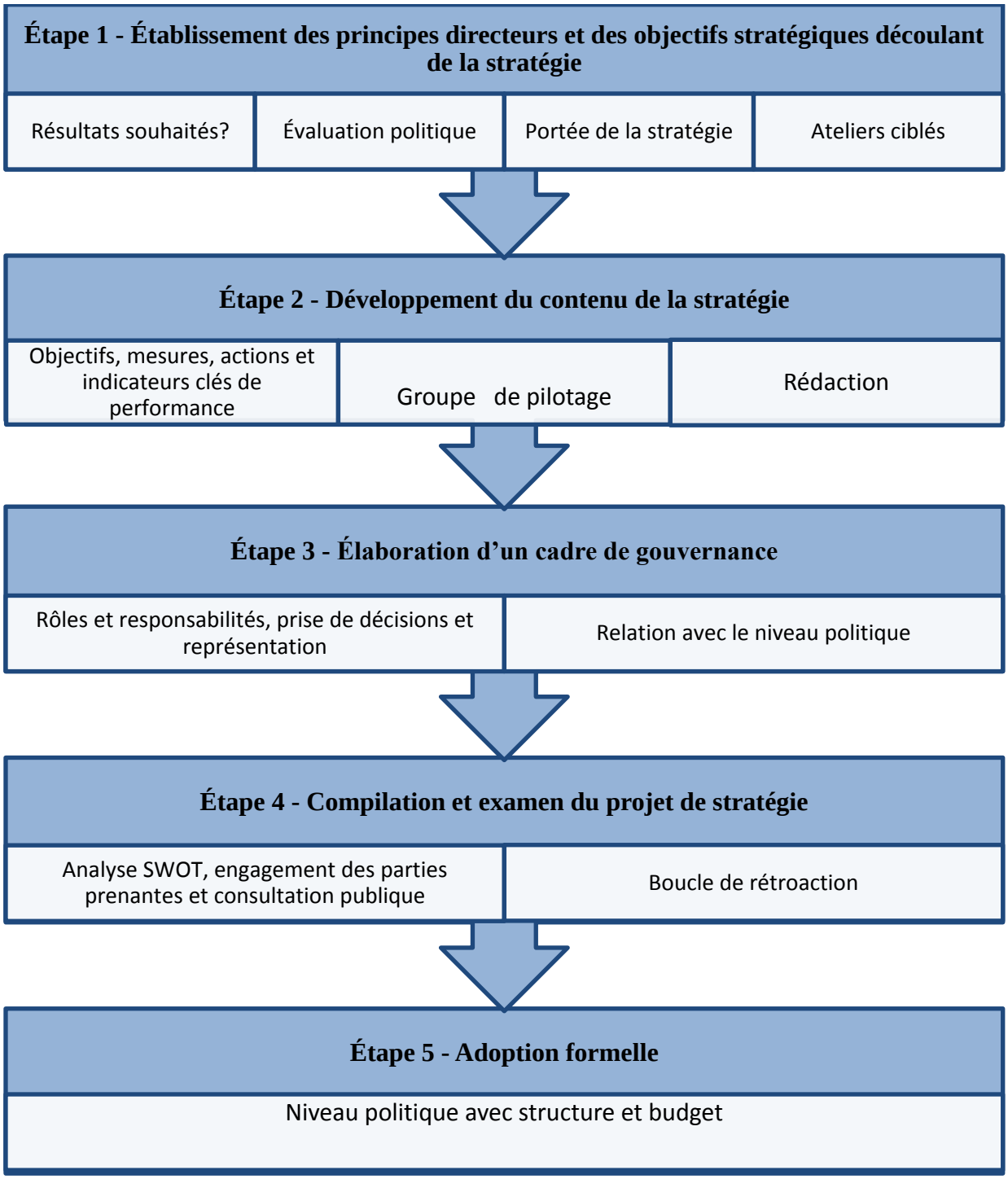
[8] OCDE, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies*, 2012. Disponible à l'adresse suivante: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Global Cyber Security Capacity Centre and University of Oxford, Global Cyber *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition*, 2016. Disponible à l'adresse suivante: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Hormis la Grèce, où une stratégie nationale en matière de cybersécurité est en cours d'élaboration depuis 2014 (voir à l'adresse https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] Ces informations sont fondées sur la vue d'ensemble des SNCS fournie par l'ENISA à l'adresse suivante https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Illustration nº 1: Processus en 5 étapes pour adopter une SNCS



3. Directive SRI: autorités nationales compétentes, points de contact uniques et centres de réponse aux incidents de sécurité informatique (CSIRT)

En vertu de l'article 8, paragraphe 1, les États membres sont tenus de désigner une ou plusieurs autorités nationales compétentes, couvrant au moins les secteurs visés à l'annexe II de la directive et les services visés à son annexe III, chargées de contrôler l'application de la directive. Les États membres peuvent attribuer cette mission à une ou des autorités existantes.

Cette section met l'accent sur la manière dont la directive SRI améliore l'état de préparation des États membres en exigeant la mise en place d'autorités nationales compétentes et de centres de réponse aux incidents de sécurité informatique (CSIRT). Plus précisément, elle couvre l'obligation de désigner des autorités nationales compétentes, ainsi que le rôle du point de contact unique. Il y est question de trois sujets: a) les structures de gouvernance nationales possibles (par exemple, modèles centralisés, décentralisés, etc.) et d'autres exigences; b) le rôle du point de contact unique et c) les centres de réponse aux incidents de sécurité informatique (CSIRT).

3.1. Type d'autorités.

L'article 8 de la directive SRI exige des États membres qu'ils désignent des autorités nationales compétentes en matière de sécurité des réseaux et des systèmes d'information, tout en reconnaissant explicitement la possibilité de désigner «*une ou plusieurs autorités nationales compétentes*». Le considérant 30 de la directive explique ce choix politique: «*Compte tenu des divergences entre les structures de gouvernance nationales et en vue de sauvegarder les accords existants au niveau sectoriel ou les autorités de surveillance et de régulation de l'Union et d'éviter les doubles emplois, les États membres devraient pouvoir désigner plusieurs autorités nationales compétentes chargées d'accomplir les tâches liées à la sécurité des réseaux et des systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique dans le cadre de la présente directive*».

En conséquence, les États membres sont libres de désigner une seule autorité centrale traitant de tous les secteurs et services couverts par la directive ou plusieurs autorités, en fonction du type de secteur, par exemple.

Lorsqu'ils décident de cette approche, les États membres peuvent s'inspirer de l'expérience tirée des approches nationales utilisées dans le contexte de la législation en vigueur sur la protection des infrastructures d'information critiques (PIIC). Comme indiqué dans le tableau 1, dans le cas de la PIIC, les États membres ont décidé d'adopter une approche centralisée ou décentralisée lors de l'attribution des compétences au niveau national. Les exemples nationaux ne sont utilisés ici qu'à titre indicatif et en vue de porter les cadres organisationnels existants à l'attention des États membres. Par conséquent, la Commission n'insinue pas que le modèle utilisé par chaque pays pour la PIIC devrait nécessairement être appliqué aux fins de la transposition de la directive SRI.

Les États membres peuvent également opter pour diverses formules hybrides comportant des éléments d'approches centralisées et décentralisées. Les choix peuvent être opérés en conformité avec les dispositions nationales antérieures en matière de gouvernance pour les différents secteurs et services couverts par la directive, ou être nouvellement déterminés par les autorités concernées et par les parties intéressées identifiées comme opérateurs de services essentiels et fournisseurs de service numérique. L'existence de compétences spécialisées en matière de cybersécurité, les considérations de ressources, les relations entre les parties prenantes et les intérêts nationaux (par exemple, le développement économique, la sécurité publique, etc.) peuvent également constituer des facteurs importants qui orientent les choix des États membres.

3.2 Information du public et autres aspects pertinents.

Conformément à l'article 8, paragraphe 7, les États membres doivent informer la Commission de la désignation des autorités nationales compétentes et des tâches qui leur sont confiées. Cette démarche doit être effectuée avant la date limite de transposition.

Les articles 15 et 17 de la directive SRI exigent des États membres qu'ils veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour accomplir les tâches énoncées dans lesdits articles.

En outre, la désignation d'entités spécifiques en tant qu'autorités nationales compétentes doit être rendue publique. La directive ne précise pas les modalités de cette information du public. Étant donné que l'objectif de cette exigence est d'atteindre un niveau élevé de sensibilisation des acteurs couverts par les SRI et du grand public, et sur la base des expériences tirées d'autres secteurs (télécommunications, banques, médicaments), la Commission considère que cette démarche pourrait être réalisée, par exemple, au moyen d'un portail jouissant d'une bonne publicité.

L'article 8, paragraphe 5, de la directive SRI exige que ces autorités disposent de «ressources suffisantes» pour pouvoir s'acquitter des tâches qui leur sont confiées au titre de la directive.

Tableau 1: Approches nationales en matière de protection des infrastructures d'information critiques (PIIC).

En 2016, l'ENISA a publié une étude[12] sur les différentes approches suivies par les États membres pour protéger leurs infrastructures d'information critiques. Deux profils sont décrits en ce qui concerne la gouvernance de la PIIC dans les États membres et ceux-ci peuvent être appliqués dans le cadre de la transposition de la directive SRI.

Profil 1: Approche décentralisée – avec des autorités multisectorielles compétentes pour des secteurs et services spécifiques visés aux annexes II et III de la directive.

L'approche décentralisée se caractérise par:

(i) le principe de subsidiarité;
(ii) une coopération étroite entre les organismes publics;
(iii)une législation propre au secteur.

Le principe de subsidiarité.

Plutôt que d'établir ou de désigner un organisme unique doté d'une responsabilité globale, l'approche décentralisée suit le principe de subsidiarité. Cela signifie que la responsabilité de la mise en œuvre incombe à une autorité sectorielle, qui comprend le mieux le secteur local et a déjà établi des relations avec les parties prenantes. En vertu de ce principe, les décisions sont prises par les personnes les plus proches de celles qui sont concernées.

Coopération étroite entre les organismes publics.

En raison de la diversité des organismes publics associés à la PIIC, de nombreux États membres ont développé des programmes de coopération afin de coordonner le travail et les efforts des différentes autorités. Ces programmes de coopération peuvent prendre la forme de réseaux informels ou de forums ou d'arrangements plus institutionnalisés. Toutefois, ils ne servent qu'à l'échange d'informations et à la coordination entre les différents organismes publics, mais n'ont aucune autorité sur eux.

Législation propre au secteur.

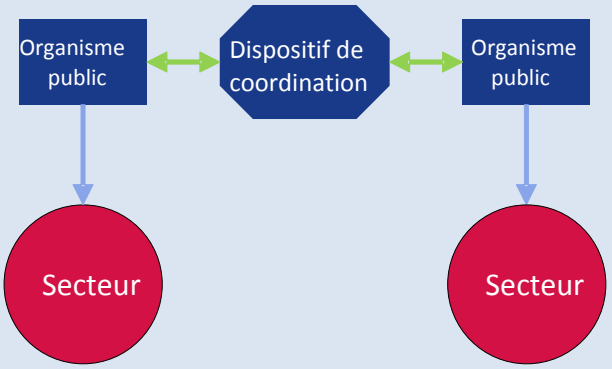
Les pays qui suivent l'approche décentralisée à travers les secteurs critiques s'abstiennent souvent de légiférer aux fins de la PIIC. Au contraire, l'adoption de législations et de réglementations demeure sectorielle et peut donc varier considérablement d'un secteur à l'autre. Cette approche aurait l'avantage d'aligner les mesures liées aux SRI sur les réglementations sectorielles existantes afin d'améliorer l'acceptation par le secteur et l'efficacité de l'application par l'autorité concernée.

L'adoption d'une approche purement décentralisée dans de multiples secteurs et services peut entraîner un manque de cohérence substantiel dans l'application de la directive. Dans ce cas, la directive prévoit un point de contact national unique pour assurer la

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs*, 2016. Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

liaison sur les questions transfrontalières, et cette entité pourrait également être chargée par l'État membre concerné de la coordination et de la coopération internes entre plusieurs autorités nationales compétentes, conformément à l'article 10 de la directive.

Illustration nº 2 – Approche décentralisée.



Exemples d'approche décentralisée.

La Suède est un bon exemple de pays qui suit une approche décentralisée dans le cadre de la PIIC. Le pays utilise une «perspective systémique», ce qui signifie que les principales tâches associées à la PIIC, telles que l'identification des services vitaux et des infrastructures critiques, la coordination et le soutien des opérateurs, les tâches réglementaires, ainsi que les mesures de préparation aux situations d'urgence, relèvent de la responsabilité des différents organismes et municipalités. Parmi ces agences figurent l'Agence suédoise pour les contingences civiles (MSB), l'Agence suédoise des postes et télécommunications (PTS) et plusieurs agences suédoises, militaires de défense et de maintien de l'ordre.

Afin de coordonner les actions entre les différentes agences et entités publiques, le gouvernement suédois a mis en place un réseau coopératif composé d'autorités «dotées de responsabilités sociétales spécifiques en matière de sécurité de l'information». Ce groupe de coopération pour la sécurité de l'information (SAMFI) est composé de représentants des différentes autorités et se réunit plusieurs fois par an pour discuter des questions liées à la sécurité nationale de l'information. Les domaines d'intervention de la SAMFI se situent principalement dans des domaines politico-stratégiques et couvrent des thèmes tels que les questions techniques et la normalisation, le développement national et international dans le domaine de la sécurité de l'information ou la gestion et la prévention des incidents informatiques. [Agence suédoise pour les contingences civiles (MSB) 2015].

La Suède n'a pas publié de loi centrale relative à la PIIC applicable aux opérateurs d'infrastructures d'information critiques (IIC) dans tous les secteurs. Au lieu de cela, la

promulgation d'une législation assortie d'obligations pour les entreprises de secteurs spécifiques relève de la responsabilité des autorités publiques respectives. Par exemple, la MSB a le droit d'édicter des règlements à l'intention des autorités gouvernementales dans le domaine de la sécurité de l'information, tandis que la PTS peut exiger des opérateurs qu'ils mettent en œuvre certaines mesures de sécurité techniques ou organisationnelles fondées sur le droit dérivé.

L'Irlande est un autre exemple de pays qui affiche les caractéristiques de ce profil. Elle applique une «doctrine de la subsidiarité» selon laquelle chaque ministère est responsable de l'identification des IIC et de l'évaluation des risques dans son propre secteur. En outre, aucune réglementation spécifique au niveau national n'a été adoptée en ce qui concerne la PIIC. La législation reste sectorielle et existe principalement dans le secteur de l'énergie et des télécommunications (2015). D'autres exemples sont l'Autriche, Chypre et la Finlande.

Profil 2: Approche centralisée – avec une autorité centrale compétente pour tous les secteurs et services spécifiques visés aux annexes II et III de la directive.

L'approche centralisée se caractérise par:

i) une autorité centrale pour tous les secteurs;
ii) une législation globale.

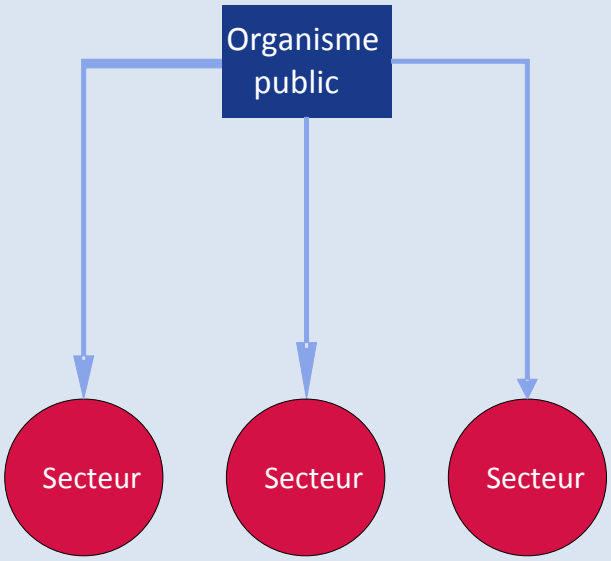
Autorité centrale pour tous les secteurs.

Les États membres qui suivent une approche centralisée ont mis en place des autorités dotées de responsabilités et de compétences étendues dans plusieurs ou dans tous les secteurs critiques, ou ont étendu les pouvoirs des autorités existantes. Ces autorités principales en matière de PIIC combinent plusieurs tâches telles que la planification d'urgence, la gestion des urgences, les tâches réglementaires et le soutien aux opérateurs privés. Dans de nombreux cas, le CSIRT national ou gouvernemental fait partie de l'autorité principale en matière de PIIC. Une autorité centrale est susceptible de disposer d'une plus forte concentration de compétences en cybersécurité que plusieurs autorités sectorielles, étant donné la pénurie générale de compétences en la matière.

Une législation globale.

Une législation globale impose des obligations et des exigences à l'ensemble des exploitants d'IIC dans tous les secteurs. Cela peut se faire au moyen de nouvelles législations exhaustives ou en complétant les réglementations sectorielles existantes. Cette approche favoriserait une application cohérente de la directive SRI dans tous les secteurs et services couverts. Elle contribuerait à éviter le risque de lacunes dans la mise en œuvre qui pourraient se produire dans le cas d'autorités multiples ayant des attributions spécifiques.

Illustration nº 3 – Approche centralisée.



Exemples d'approche centralisée

La France est un bon exemple d'État membre de l'Union doté d'une approche centralisée. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été désignée comme la principale autorité nationale de défense des systèmes d'information en 2011. Elle joue un rôle de supervision fort à l'égard des «opérateurs d'importance vitale» (OIV): l'agence peut ordonner aux OIV de se conformer aux mesures de sécurité et est habilitée à effectuer des audits de sécurité à leur égard. En outre, il s'agit du principal point de contact unique pour les OIV, qui sont tenus de signaler les incidents de sécurité à l'agence.

En cas d'incidents de sécurité, l'ANSSI agit en tant qu'agence de secours pour la PIIC et décide des mesures que les opérateurs doivent prendre pour répondre à la crise. Les actions gouvernementales sont coordonnées au sein du centre opérationnel de l'ANSSI. La détection des menaces et la réponse aux incidents au niveau opérationnel sont effectuées par le CERT-FR, qui fait partie de l'ANSSI.

La France a mis en place un cadre juridique complet pour la PIIC. En 2006, le premier ministre a ordonné l'établissement d'une liste de secteurs d'infrastructures critiques. Sur la base de cette liste, qui recense douze secteurs vitaux, le gouvernement a défini environ 250 OIV. En 2013, la loi de programmation militaire (LPM)[13] a été promulguée. Elle fixe différentes obligations pour les OIV, telles que le signalement des incidents ou la mise en œuvre de mesures de sécurité. Ces exigences sont obligatoires pour tous les OIV, tous secteurs confondus (Sénat français, 2013).

[13] La loi de programmation militaire

3.3. Directive SRI – article 9: Centres de réponse aux incidents de sécurité informatique (CSIRT).

En vertu de l'article 9, les États membres sont tenus de désigner un ou plusieurs CSIRT chargés de la gestion des incidents et des risques pour les secteurs visés à l'annexe II de la directive SRI et les services visés à l'annexe III. Compte tenu de l'exigence d'harmonisation minimale énoncée à l'article 3 de la directive, les États membres sont libres d'utiliser les CSIRT également pour d'autres secteurs non couverts par la directive, tels que l'administration publique.

Les États membres peuvent opter pour l'établissement d'un CSIRT au sein de l'autorité nationale compétente[14].

3.4. Tâches et obligations.

Les tâches des CSIRT désignés, définies à l'annexe I de la directive SRI, sont notamment les suivantes:

- suivi des incidents au niveau national;
- activation du mécanisme d'alerte précoce, diffusion de messages d'alerte, annonces et diffusion d'informations sur les risques et incidents auprès des parties intéressées;
- intervention en cas d'incident;
- analyse dynamique des risques et incidents et conscience situationnelle; et
- participation au réseau des CSIRT nationaux (réseau des CSIRT) établi au titre de l'article 12.

Des tâches spécifiques supplémentaires sont prévues à l'article 14, paragraphes 3, 5 et 6, ainsi qu'à l'article 16, paragraphes 3, 6 et 7, en ce qui concerne les notifications d'incidents lorsqu'un État membre décide que les CSIRT peuvent assumer ces rôles en plus ou en lieu et place des autorités nationales compétentes.

En transposant la directive, les États membres disposent de différentes options en ce qui concerne le rôle des CSIRT soumis à des obligations de notification d'incidents. La notification obligatoire directe aux CSIRT est possible avec des avantages d'efficacité administrative, mais les États membres peuvent opter pour une notification directe aux autorités nationales compétentes, les CSIRT ayant alors un droit d'accès aux informations notifiées. Les CSIRT s'intéressent en fin de compte à la résolution de problèmes à des fins de dissuasion, de détection, de réponse et d'atténuation de l'impact des cyberincidents (y compris ceux qui ne sont pas essentiels à la notification obligatoire) pour leurs parties prenantes, le respect des dispositions réglementaires incombant aux autorités nationales compétentes.

[14] Voir l'article 9, paragraphe 1, dernière phrase.

Conformément à l'article 9, paragraphe 3, de la directive, les États membres doivent également veiller à ce que ces CSIRT aient accès à une infrastructure d'information et de communication sécurisée et résiliente.

L'article 9, paragraphe 4, de la directive exige des États membres qu'ils informent la Commission des missions de leurs CSIRT ainsi que des principaux éléments de leurs processus de gestion des incidents.

Les obligations qui incombent aux CSIRT désignés par les États membres figurent à l'annexe I de la directive SRI. Un CSIRT doit veiller à un niveau élevé de disponibilité de ses services de communication. Ses locaux et les systèmes d'information utilisés doivent se trouver sur des sites sécurisés et être en mesure de garantir la continuité des opérations. De plus, les CSIRT devraient avoir la possibilité de participer aux réseaux de coopération internationale.

3.5. Assistance pour le développement de CSIRT.

Le programme du mécanisme pour l'interconnexion en Europe (MIE) relatif aux infrastructures de services numériques (DSI) dans le domaine de la cybersécurité peut fournir un financement européen important pour aider les CSIRT des États membres à améliorer leurs capacités et à coopérer entre eux par le biais d'un mécanisme de coopération en matière d'échange d'informations. Le mécanisme de coopération en cours d'élaboration dans le cadre du projet SMART 2015/1089 vise à favoriser une coopération opérationnelle rapide et efficace sur une base volontaire entre les CSIRT des États membres, notamment à l'appui des tâches confiées au réseau des CSIRT en vertu de l'article 12 de la directive.

Des informations détaillées sur les appels à propositions pertinents pour le renforcement des capacités des CSIRT des États membres sont disponibles sur le site web de l'Agence exécutive pour l'innovation et les réseaux (INEA) de la Commission européenne[15].

Le conseil de gouvernance DSI pour la cybersécurité du MIE fournit une structure informelle d'orientation et d'assistance au niveau politique à l'attention des CSIRT des États membres à des fins de renforcement des capacités et en vue de la mise en œuvre du mécanisme de coopération volontaire.

Un CSIRT nouvellement créé ou désigné pour remplir les tâches visées à l'annexe I de la directive SRI peut compter sur les conseils et l'expertise de l'ENISA pour améliorer ses performances et mener à bien ses travaux de manière efficace[16]. À cet égard, il convient de souligner que les CSIRT des États membres pourraient prendre comme référence une partie des travaux récemment menés par l'ENISA. En particulier, comme indiqué à la section 7 de la présente annexe, l'Agence a publié un certain nombre de documents et d'études décrivant les bonnes pratiques et formulant des recommandations au niveau technique, y compris pour ce qui est des évaluations du niveau de maturité des CSIRT, pour diverses capacités et services

[15] Disponible à l'adresse suivante: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Voir l'article 9, paragraphe 5, de la directive SRI.

des CSIRT. En outre, les conseils et les bonnes pratiques ont également été partagés par des réseaux de CSIRT tant au niveau mondial (FIRST[17]) qu'européen (Trusted Introducer, TI[18]).

3.6. Le rôle du point de contact unique.

Conformément à l'article 8, paragraphe 3, de la directive SRI, chaque État membre doit désigner un point de contact national unique, qui exercera une fonction de liaison pour assurer une coopération transfrontalière avec les autorités compétentes des autres États membres, ainsi qu'avec le groupe de coopération et le réseau des CSIRT[19] créés au titre de la directive elle-même. Le considérant 31 et l'article 8, paragraphe 4, expliquent la raison d'être de cette exigence, à savoir faciliter la coopération et la communication transfrontalières. Cet élément est particulièrement nécessaire dans la mesure où les États membres peuvent décider d'avoir plus d'une autorité nationale. Ainsi, un point de contact unique faciliterait l'identification et la coopération des autorités de différents États membres.

Le rôle de liaison du point de contact unique est susceptible d'impliquer une interaction avec les secrétariats du groupe de coopération et du réseau des CSIRT dans les cas où le point de contact national unique n'est ni un CSIRT ni un membre du groupe de coopération. En outre, les États membres doivent veiller à ce que le point de contact unique soit informé des notifications reçues des opérateurs de services essentiels et des fournisseurs de service numérique[20].

L'article 8, paragraphe 3, de la directive précise que, dans le cas où un État membre adopte une approche centralisée, c'est-à-dire ne désignant qu'une seule autorité compétente, cette dernière fait aussi fonction de point de contact unique. Si un État membre opte pour une approche décentralisée, il pourrait choisir l'une des différentes autorités compétentes pour agir en tant que point de contact unique. Indépendamment du modèle institutionnel choisi, lorsqu'ils sont distincts, l'autorité compétente, le point de contact unique et le CSIRT d'un même État membre ont l'obligation de coopérer aux fins du respect des obligations énoncées dans ladite directive[21].

Au plus tard le 9 août 2018, puis tous les ans, le point de contact unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises par les autorités, telles que l'information des autres États membres touchés sur l'incident ou la fourniture à la société à l'origine de la notification d'informations pertinentes pour la gestion de l'incident[22]. À la demande de l'autorité compétente ou du CSIRT, le point de contact

[17] Forum des centres de réponse aux incidents de sécurité (*Forum of Incident Response and Security Teams*, https://www.first.org/)
[18] https://www.trusted-introducer.org/
[19] Un réseau de CSIRT nationaux pour la coopération opérationnelle entre les États membres au titre de l'article 12.
[20] Voir l'article 10, paragraphe 3.
[21] Voir l'article 10, paragraphe 1.
[22] Idem

unique doit transmettre les notifications d'opérateurs de services essentiels aux points de contact uniques des autres États membres touchés par les incidents[23].

Les États membres doivent informer la Commission de la désignation du point de contact unique et de ses tâches avant la date limite de transposition. La désignation du point de contact unique doit être rendue publique, au même titre que celle des autorités nationales compétentes. La Commission publie la liste des points de contact uniques désignés.

3.7. Sanctions.

L'article 21 laisse aux États membres une marge de manœuvre pour décider du type et de la nature des sanctions applicables, pour autant qu'elles soient effectives, proportionnées et dissuasives. En d'autres termes, les États membres sont en principe libres de décider du montant maximal des sanctions prévues par leur législation nationale, mais le montant ou le pourcentage choisi devrait permettre aux autorités nationales d'imposer, dans chaque cas concret, des sanctions effectives, proportionnées et dissuasives, en tenant compte de différents facteurs tels que la gravité ou la fréquence de l'infraction.

4. Entités soumises à des obligations concernant les exigences de sécurité et les notifications d'incidents.

Les entités qui jouent un rôle important pour la société et l'économie visées à l'article 4, paragraphes 4 et 5, de la directive, en tant qu'opérateurs de services essentiels (OSE) et fournisseurs de service numérique (FSN), sont tenues de prendre des mesures de sécurité appropriées et de notifier les incidents graves aux autorités nationales compétentes. La raison en est que les incidents de sécurité dans ces services peuvent représenter une menace considérable pour leur fonctionnement, ce qui peut nuire gravement à l'exercice d'activités économiques et à la société au sens large, entamer la confiance des utilisateurs et porter un grand préjudice à l'économie de l'Union[24].

La présente section donne un aperçu des entités relevant du champ d'application des annexes II et III de la directive SRI et énumère leurs obligations. L'identification des opérateurs de services essentiels est largement couverte, compte tenu de l'importance que ce processus revêt pour la mise en œuvre harmonisée de la directive SRI dans l'ensemble de l'Union européenne. Elle fournit également des explications détaillées sur les définitions des infrastructures numériques et des fournisseurs de service numérique. Elle examine également la possibilité d'inclure d'autres secteurs et explique plus en détail l'approche spécifique en ce qui concerne les FSN.

4.1. Opérateurs de services essentiels (OSE).

La directive SRI ne définit pas explicitement quelles entités particulières seront considérées comme des OSE relevant de son champ d'application. Au lieu de cela, elle établit des critères

[23] Voir l'article 14, paragraphe 5.
[24] Voir le considérant 2.

que les États membres devront appliquer pour mettre en œuvre un processus d'identification qui déterminera, en définitive, les entreprises individuelles appartenant au type d'entités énumérées à l'annexe II qui seront considérées comme des opérateurs de services essentiels, et seront donc soumises aux obligations prévues par la directive.

4.1.1. Type d'entités figurant à l'annexe II de la directive SRI.

L'article 4, paragraphe 4, définit les OSE comme des entités publiques ou privées dont le type figure à l'annexe II de la directive et qui répondent aux critères énoncés à l'article 5, paragraphe 2. L'annexe II énumère les secteurs, sous-secteurs et types d'entités pour lesquels chaque État membre doit procéder à la procédure d'identification prévue à l'article 5, paragraphe 2[25]. Ces secteurs comprennent l'énergie, les transports, les banques, les infrastructures de marchés financiers, le secteur de la santé, l'eau et les infrastructures numériques.

Pour la plupart des entités qui appartiennent aux «secteurs traditionnels», la législation de l'Union contient des définitions bien développées auxquelles l'annexe II renvoie. Toutefois, ce n'est pas le cas pour le secteur des infrastructures numériques, figurant au point 7 de l'annexe II, y compris les points d'échange internet, les systèmes de noms de domaine et les registres de noms de domaine de haut niveau. C'est pourquoi, dans le but de clarifier ces définitions, une explication détaillée est donnée ci-après:

1) Point d'échange internet (*Internet Exchange Point* – IXP).

Le terme «point d'échange Internet» est défini à l'article 4, paragraphe 13, et clarifié plus en détail au considérant 18, et peut être décrit comme une structure de réseau qui permet l'interconnexion de plus de deux systèmes indépendants techniquement autonomes, essentiellement aux fins de faciliter l'échange de trafic internet. Le point d'échange internet peut également être décrit comme un lieu physique où un certain nombre de réseaux peuvent échanger du trafic internet entre eux par l'intermédiaire d'un commutateur. L'objectif premier d'un IXP est de permettre aux réseaux de s'interconnecter directement, via l'échange, plutôt que via un ou plusieurs réseaux tiers. Le fournisseur IXP n'est normalement pas responsable de l'acheminement du trafic internet. L'acheminement du trafic est effectué par les fournisseurs de réseau. Les avantages de l'interconnexion directe sont nombreux, mais les principales raisons en sont le coût, la latence et la largeur de bande. Le trafic passant par un échange n'est généralement pas facturé par une tierce partie, contrairement au trafic vers un fournisseur d'accès internet (FAI) en amont. L'interconnexion directe, souvent située dans la même ville que les deux réseaux, évite aux données de parcourir de longues distances pour se rendre d'un réseau à l'autre, réduisant ainsi la latence.

Il convient de noter que la définition de l'IXP ne couvre pas les points physiques où seuls deux réseaux physiques sont interconnectés entre eux (c'est-à-dire les fournisseurs de réseaux

[25] Pour plus de détails sur le processus d'identification, voir la section 4.1.6 ci-dessous.

tels que BASE et PROXIMUS). Par conséquent, lors de la transposition de la directive, les États membres doivent établir une distinction entre les opérateurs qui facilitent l'échange de trafic internet agrégé entre plusieurs opérateurs de réseau et ceux qui sont des opérateurs de réseau unique, qui interconnectent physiquement leurs réseaux sur la base d'un accord d'interconnexion. Dans ce dernier cas, les fournisseurs de réseau ne sont pas couverts par la définition figurant à l'article 4, paragraphe 13. Un éclaircissement à ce sujet figure au considérant 18, qui indique que l'IXP ne fournit pas d'accès à un réseau et n'agit pas en tant que fournisseur ou opérateur de transit. La dernière catégorie de fournisseurs est constituée par les entreprises fournissant des réseaux et/ou des services de communications publics qui sont soumises aux obligations de sécurité et de notification prévues à l'article 13, points a) et b), de la directive 2002/21/CE et qui sont donc exclues du champ d'application de la directive SRI[26].

2) Système de noms de domaines (DNS)

Le terme «système de noms de domaine» (DNS) est défini à l'article 4, paragraphe 14 comme «*un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines*». Plus précisément, le DNS peut être décrit comme un système hiérarchique et distribué d'affectation de noms pour les ordinateurs, les services ou toute autre ressource connectée à internet qui permet l'encodage des noms de domaine en adresses IP (*Internet Protocol*). Le rôle principal du système est de traduire les noms de domaine assignés en adresses IP. À cet effet, le DNS exploite une base de données et utilise des serveurs de noms et un résolveur pour permettre ce type de «traduction» des noms de domaine en adresses IP opérationnelles. Bien que l'encodage des noms de domaine ne soit pas la seule responsabilité du DNS, c'est une tâche essentielle du système. La définition juridique donnée à l'article 4, paragraphe 14, se concentre sur le rôle principal du système du point de vue de l'utilisateur sans entrer dans les détails plus techniques, comme par exemple l'exploitation de l'espace de noms de domaine, des serveurs de noms, des résolveurs, etc. Enfin, l'article 4, paragraphe 15, donne une définition plus précise du fournisseur de services DNS.

3) Registre de noms de domaine de haut niveau (TLD).

Le «registre de noms de domaine de haut niveau» est défini à l'article 4, paragraphe 16, comme une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné. L'administration et la gestion des noms de domaine comprennent l'encodage des noms de domaines de haut niveau en adresses IP.

L'IANA (*Internet Assigned Numbers Authority*) est responsable de la coordination globale des serveurs racines du DNS, de l'adressage du protocole internet et d'autres ressources de protocole internet. En particulier, l'IANA est responsable de l'attribution des domaines de haut niveau génériques, par exemple «.com», et des domaines nationaux de haut niveau (code pays), par exemple «.be», aux opérateurs (registres) ainsi que du maintien de leurs détails

[26] Voir la section 5.2. pour plus de détails sur la relation entre la directive SRI et la directive 2002/21/CE.

techniques et administratifs. L'IANA tient un registre mondial des domaines de haut niveau attribués et joue un rôle dans la diffusion de cette liste auprès des utilisateurs d'internet du monde entier ainsi que dans l'introduction de nouveaux domaines de haut niveau.

Une tâche importante des registres consiste à attribuer des noms de deuxième niveau aux titulaires sous leurs domaines de haut niveau respectifs. Ces titulaires peuvent également, s'ils le souhaitent, attribuer eux-mêmes des noms de domaine de troisième niveau. Les noms de domaines nationaux de haut niveau sont désignés pour représenter un pays ou un territoire selon la norme ISO 3166-1. Les noms de domaines de haut niveau «génériques» n'ont normalement pas de désignation géographique ou de pays.

Il convient de noter que l'exploitation d'un registre de noms de domaine de haut niveau peut supposer la fourniture de DNS. Par exemple, conformément aux règles de délégation de l'IANA, l'entité désignée traitant des noms de domaines nationaux de haut niveau doit – entre autres – superviser les noms de domaine et exploiter le DNS de ce pays[27]. Ces circonstances doivent être prises en considération par les États membres lors de la mise en œuvre du processus d'identification des opérateurs de services essentiels prévue à l'article 5, paragraphe 2.

4.1.2. Identification des opérateurs de services essentiels

Conformément aux exigences de l'article 5 de la directive, chaque État membre est tenu de procéder à une identification de toutes les entités des types énumérés à l'annexe II qui ont un établissement juridique sur son territoire. À l'issue de cette évaluation, toutes les entités qui satisfont aux critères énoncés à l'article 5, paragraphe 2, sont identifiées comme des OSE et sont soumises aux obligations de sécurité et de notification prévues à l'article 14.

Les États membres ont jusqu'au 9 novembre 2018 pour identifier les opérateurs de chaque secteur et sous-secteur. Afin d'aider les États membres tout au long de ce processus, le groupe de coopération élabore actuellement un document d'orientation contenant des informations pertinentes sur les étapes nécessaires à suivre et sur les bonnes pratiques en matière d'identification des OSE.

En outre, conformément à l'article 24, paragraphe 2, le groupe de coopération doit discuter du processus, ainsi que du contenu et du type des mesures nationales visant à identifier les opérateurs de services essentiels dans un secteur spécifique. Un État membre peut, avant le 9 novembre 2018, demander à ce que le groupe de coopération discute de son projet de mesures nationales en vue d'identifier les opérateurs de services essentiels.

4.1.3. Inclusion de secteurs supplémentaires.

Compte tenu de l'exigence d'harmonisation minimale prévue à l'article 3, les États membres peuvent adopter ou maintenir une législation garantissant un niveau de sécurité plus élevé des réseaux et des systèmes d'information. À cet égard, les États membres sont généralement libres d'étendre les obligations de sécurité et de notification prévues à l'article 14 aux entités

[27] Informations disponibles à l'adresse: https://www.icann.org/resources/pages/delegation-2012-02-25-en

appartenant à d'autres secteurs et sous-secteurs que ceux énumérés à l'annexe II de la directive SRI. Plusieurs États membres ont décidé ou envisagent actuellement d'inclure certains des secteurs supplémentaires suivants dans la liste.

i) Administrations publiques

Les administrations publiques peuvent proposer des services essentiels, au-delà de ceux visés à l'annexe II de la directive, qui satisfont aux exigences de l'article 5, paragraphe 2. Dans de tels cas, les administrations publiques offrant ces services seraient couvertes par les exigences de sécurité et les obligations de notification applicables. En revanche, lorsque des administrations publiques offrent des services qui ne relèvent pas du champ d'application ci-dessus, ces services ne seraient pas couverts par les obligations applicables.

Les administrations publiques sont responsables de la bonne prestation des services publics fournis par les organismes gouvernementaux, les autorités régionales et locales, les agences et les entreprises associées. Ces services impliquent souvent la création et la gestion de données personnelles et corporatives sur des particuliers et organisations, qui peuvent être partagées et mises à la disposition de multiples entités publiques. D'une manière plus générale, un niveau élevé de sécurité des réseaux et des systèmes d'information utilisés par les administrations publiques revêt un intérêt important pour la société et l'économie dans son ensemble. La Commission estime donc qu'il serait judicieux que les États membres envisagent d'inclure l'administration publique dans le champ d'application de la législation nationale transposant la directive, au-delà de la prestation de services essentiels visés aux annexes II et à l'article 5, paragraphe 2.

ii) Secteur postal

Le secteur postal englobe la fourniture de services postaux tels que la collecte, le tri, le transport et la distribution des envois postaux.

iii) Secteur alimentaire

Le secteur alimentaire couvre la production de produits agricoles et d'autres produits alimentaires et pourrait inclure des services essentiels tels que la sécurité alimentaire et l'assurance de la qualité et de la salubrité des aliments.

iv) Industrie chimique et nucléaire

L'industrie chimique et nucléaire concerne en particulier le stockage, la production et le traitement de produits chimiques et pétrochimiques ou de matières nucléaires.

v) Secteur de l'environnement

Les activités environnementales englobent la fourniture des biens et services nécessaires pour protéger l'environnement et gérer les ressources. Ainsi, les activités visent à prévenir, réduire et éliminer la pollution et à préserver le stock de ressources naturelles disponibles. Dans ce secteur, les services essentiels pourraient consister en la surveillance et le contrôle de la pollution (par exemple de l'air et de l'eau) et des phénomènes météorologiques.

vi) Protection civile

L'objectif du secteur de la protection civile est de prévenir les catastrophes naturelles et anthropiques, de s'y préparer et d'y faire face. Les services fournis à cette fin peuvent être l'activation de numéros d'urgence et la mise en œuvre d'actions d'information, de confinement et de réponse aux situations d'urgence.

4.1.4. Compétence.

En vertu de l'article 5, paragraphe 1, chaque État membre doit identifier les OSE ayant un établissement sur son territoire. La disposition ne précise pas le type d'établissement juridique, mais le considérant 21 dispose que cet établissement suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable, alors que la forme juridique retenue pour un tel établissement ne devrait pas être déterminante à cet égard. Cela signifie qu'un État membre peut être compétent à l'égard d'un opérateur de services essentiels non seulement dans les cas où l'opérateur a son siège social sur son territoire, mais aussi dans les cas où l'opérateur a, par exemple, une succursale ou un autre type d'établissement juridique.

Cela a pour conséquence que plusieurs États membres en parallèle pourraient avoir compétence sur la même entité.

4.1.5. Informations à transmettre à la Commission.

Aux fins du réexamen que la Commission doit effectuer conformément à l'article 23, paragraphe 1, de la directive SRI, les États membres sont tenus de transmettre à la Commission, au plus tard le 9 novembre 2018, puis tous les deux ans, les informations suivantes:

- les mesures nationales permettant l'identification des opérateurs de services essentiels;
- la liste des services essentiels;
- le nombre d'opérateurs de services essentiels identifiés pour chaque secteur visé à l'annexe II et une indication de leur importance pour ce secteur; et
- les seuils, pour autant qu'ils existent, permettant de déterminer le niveau de l'offre pertinent en fonction du nombre d'utilisateurs tributaires de ce service visé à l'article 6, paragraphe 1, point a), ou de l'importance de cet opérateur de services essentiels particulier visée à l'article 6, paragraphe 1, point f).

Le réexamen prévu à l'article 23, paragraphe 1, qui précède le réexamen complet de la directive, reflète l'importance que les colégislateurs attachent à la transposition correcte de la directive en ce qui concerne l'identification des opérateurs de services essentiels afin d'éviter la fragmentation du marché.

Afin de mener à bien ce processus de la meilleure manière possible, la Commission encourage les États membres à discuter de ce sujet, ainsi qu'à échanger les expériences pertinentes au sein du groupe de coopération. En outre, la Commission encourage les États membres à communiquer à la Commission, si nécessaire sur une base confidentielle, les listes des opérateurs de services essentiels identifiés (qui ont finalement été sélectionnés) ainsi que toutes les informations que les États membres sont tenus de lui fournir en vertu de la directive.

La mise à disposition de ces listes favoriserait et améliorerait la qualité de l'évaluation que la Commission doit réaliser sur la cohérence du processus d'identification et garantirait une meilleure comparaison des approches adoptées par les États membres, ce qui contribuerait à une meilleure réalisation des objectifs de la directive.

4.1.6. Comment réaliser le processus d'identification?

Comme le montre l'illustration nº 4, une autorité nationale devrait examiner six questions clés lorsqu'elle procède à l'identification d'une entité particulière. Dans la partie suivante, chaque question correspond à une étape à entreprendre conformément à l'article 5 en liaison avec l'article 6, et compte tenu également de l'applicabilité de l'article 1er, paragraphe 7.

Étape 1 – **L'entité appartient-elle à un secteur/sous-secteur et correspond-elle au type visé à l'annexe II de la directive?**

Une autorité nationale devrait évaluer si une entité établie sur son territoire appartient aux secteurs et sous-secteurs visés à l'annexe II de la directive. L'annexe II couvre divers secteurs économiques considérés comme essentiels au bon fonctionnement du marché intérieur. En particulier, l'annexe II se réfère aux secteurs et sous-secteurs suivants:

- Énergie: électricité, pétrole et gaz,
- Transports: aérien, ferroviaire, par voie d'eau et routier,
- Banques: établissements de crédit,
- Infrastructures de marchés financiers: plateformes de négociation, contreparties centrales,
- Secteur de la santé: établissements de soins de santé (y compris les hôpitaux et les cliniques privées),
- Eau: fourniture et distribution d'eau potable,
- Infrastructures numériques: points d'échange internet, fournisseurs de services relatifs au système des noms de domaine, registres de noms de domaine de haut niveau[28].

Étape 2 – **Une lex specialis est-elle applicable?**

Dans un deuxième temps, l'autorité nationale doit évaluer si la disposition de la lex specialis prévue à l'article 1er, paragraphe 7, s'applique. En particulier, la disposition prévoit que s'il existe un acte juridique de l'Union imposant aux fournisseurs de service numérique ou aux opérateurs de services essentiels des exigences en matière de sécurité et/ou de notification au moins équivalentes aux exigences correspondantes de la directive SRI, les obligations prévues par l'acte juridique spécial devraient s'appliquer. En outre, le considérant 9 précise que si les exigences de l'article 1er, paragraphe 7, sont remplies, les États membres devraient appliquer les dispositions de l'acte sectoriel de l'Union, notamment celles relatives à la compétence. Dans le cas contraire, les dispositions pertinentes de la directive SRI ne s'appliqueraient pas.

[28]Ces entités sont expliquées plus en détail à la section 4.1.1.

Dans ce cas, l'autorité compétente ne devrait pas poursuivre la procédure d'identification prévue à l'article 5, paragraphe 2[29].

Étape 3 – **L'opérateur fournit-il un service essentiel au sens de la directive?**

En vertu de l'article 5, paragraphe 2, point a), l'entité soumise à l'identification doit fournir un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques. Lorsqu'ils procèdent à cette évaluation, les États membres devraient tenir compte du fait qu'une seule entité peut fournir à la fois des services essentiels et non essentiels. Cela signifie que les exigences de sécurité et de notification prévues par la directive SRI ne s'appliqueront à un opérateur donné que dans la mesure où il fournit des services essentiels.

Conformément à l'article 5, paragraphe 3, un État membre devrait établir une liste de tous les services essentiels fournis par OSE sur son territoire. Cette liste devra être soumise à la Commission au plus tard le 9 novembre 2018, et tous les deux ans par la suite[30].

Étape 4 - **Le service est-il tributaire d'un réseau et d'un système d'information?**

En outre, il convient de préciser si ce service satisfait au deuxième critère de l'article 5, paragraphe 2, point b), et notamment si la fourniture du service essentiel est tributaire des réseaux et des systèmes d'information définis à l'article 4, paragraphe 1.

Étape 5 – **Un incident de sécurité aurait-il un effet disruptif important?**

L'article 5, paragraphe 2, point c), exige que l'autorité nationale évalue si un incident aurait un effet disruptif important sur la fourniture dudit service. Dans ce contexte, l'article 6, paragraphe 1, énonce plusieurs facteurs transsectoriels dont il convient de tenir compte dans l'évaluation. En outre, l'article 6, paragraphe 2, dispose que, le cas échéant, l'évaluation doit également tenir compte des facteurs sectoriels.

Les **facteurs transsectoriels** énumérés à l'article 6, paragraphe 1, sont les suivants:

- le nombre d'utilisateurs tributaires du service fourni par l'entité concernée;
- la dépendance des autres secteurs visés à l'annexe II à l'égard du service fourni par cette entité;
- les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique;
- la part de marché de cette entité;
- la portée géographique eu égard à la zone susceptible d'être touchée par un incident;
- l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

[29] Pour plus de détails sur l'applicabilité de la lex specialis, voir la section 5.1.
[30] Voir l'article 5, paragraphe 7, point b).

En ce qui concerne les **facteurs sectoriels**, le considérant 28 donne quelques exemples (voir tableau 4) qui pourraient être utiles aux autorités nationales.

Tableau 4: Exemples de facteurs sectoriels à prendre en considération pour déterminer l'effet disruptif important en cas d'incident.

Secteur	Exemples de facteurs sectoriels
Fournisseurs d'énergie	volume ou proportion d'énergie produite au niveau national
Fournisseurs de pétrole	volume journalier
Transport aérien (y compris les aéroports et les transporteurs aériens) **Transport ferroviaire** **Ports maritimes**	proportion du volume de trafic national nombre de passagers ou d'opérations de fret par an
Infrastructures bancaires ou des marchés financiers	importance systémique sur la base de leurs actifs totaux ratio entre ces actifs totaux et le PIB
Secteur de la santé	nombre annuel de patients pris en charge par le prestataire
Production, traitement et distribution d'eau	volume d'eau, nombre et types d'utilisateurs servis (y compris, par exemple, des hôpitaux, des organismes de service public ou des particuliers) existence d'autres sources d'approvisionnement en eau couvrant la même zone géographique

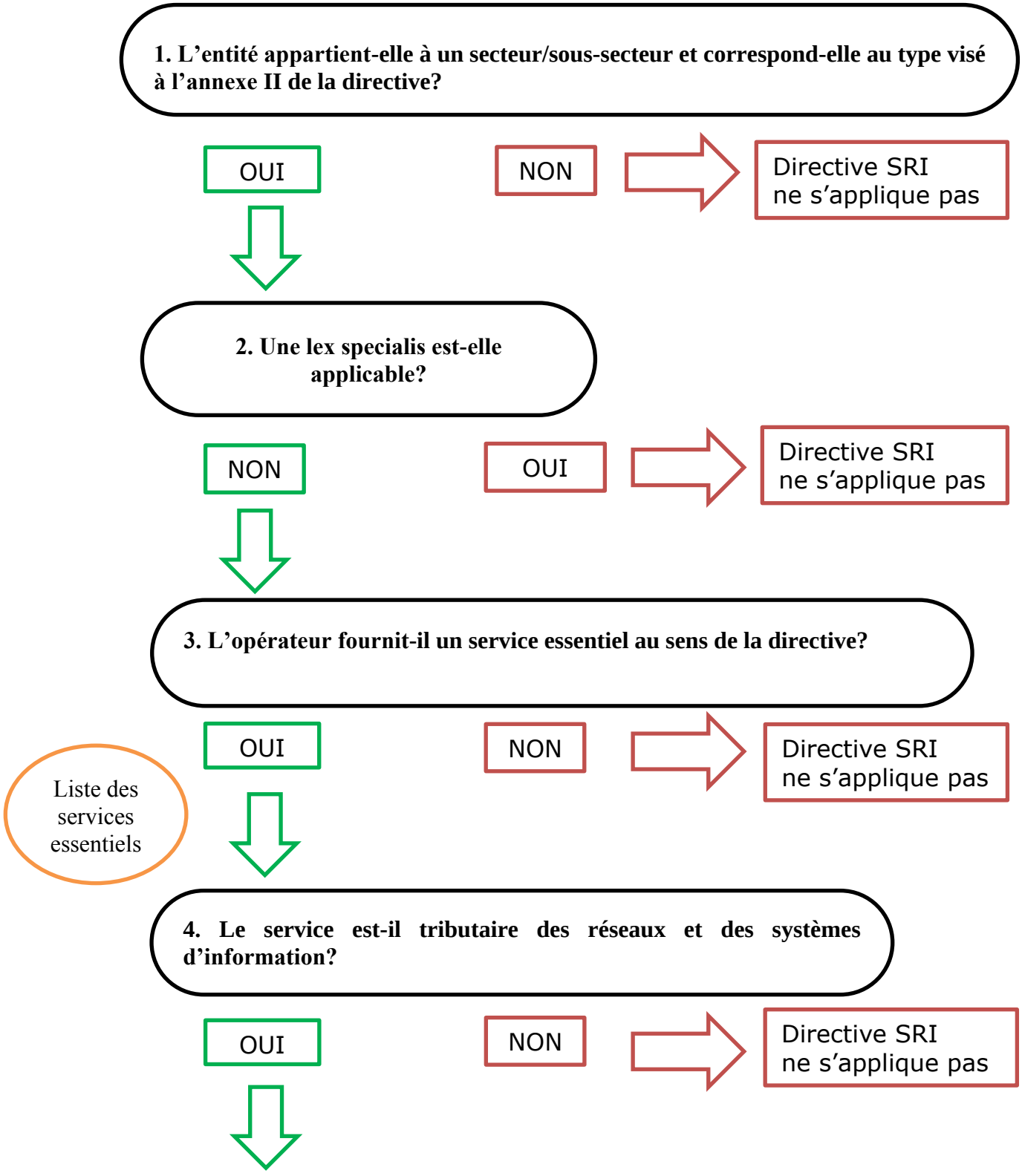
Il convient de souligner que, lors de l'évaluation effectuée conformément à l'article 5, paragraphe 2, les États membres ne devraient pas ajouter de critères supplémentaires à ceux qui sont énumérés dans cette disposition, car cela pourrait réduire le nombre d'OSE identifiés et compromettre l'harmonisation minimale pour les OSE prévue à l'article 3 de la directive.

Étape 6 - **L'opérateur concerné fournit-il des services essentiels dans d'autres États membres?**

L'étape 6 concerne les cas où un opérateur fournit ses services essentiels dans deux États membres ou plus. Avant l'achèvement du processus d'identification, l'article 5, paragraphe 4, exige des États membres concernés qu'ils engagent un processus de consultation[31].

[31] Pour plus de détails sur le processus de consultation, voir la section 4.1.7.

Illustration nº 4: Processus d'identification en 6 étapes.



5. Un incident de sécurité aurait-il un effet disruptif important?

Facteurs transsectoriels (article 6, paragraphe 1)

- **Nombre d'utilisateurs** tributaires des services
- **Dépendance** des autres secteurs essentiels à l'égard du service
- Conséquences que des incidents pourraient avoir sur les **fonctions économiques ou sociétales** ou sur la **sûreté publique**
- **Portée géographique** possible

Facteurs sectoriels (exemples mentionnés au considérant 28)

- **Énergie**: volume ou proportion d'énergie produite au niveau national
- **Transports**: proportion du volume de trafic national et nombre d'opération par an
- **Secteur de la santé**: nombre annuel de patients pris en charge par le prestataire

OUI

NON → Directive SRI ne s'applique pas

6. L'opérateur concerné fournit-il des services essentiels dans d'autres États membres?

OUI

NON → Directive SRI ne s'applique pas

Consultation obligatoire avec le ou les État(s)

Adoption de mesures nationales (liste des opérateurs de services essentiels, mesures politiques et juridiques, par exemple).

4.1.7. Processus de consultation transfrontalière.

Lorsqu'un opérateur fournit des services essentiels dans deux États membres ou plus, l'article 5, paragraphe 4, exige que ces États membres se consultent mutuellement avant l'achèvement du processus d'identification. Ce processus de consultation est destiné à les aider à évaluer le caractère critique de l'opérateur en termes d'incidence transfrontalière.

Le résultat souhaité de la consultation est que les autorités nationales concernées échangent des arguments et des points de vue et, idéalement, aboutissent au même résultat en ce qui concerne l'identification de l'opérateur concerné. Toutefois, la directive SRI n'empêche pas les États membres de parvenir à des conclusions divergentes, qu'une entité donnée soit ou non identifiée comme un OSE. Le considérant 24 mentionne la possibilité pour les États membres de solliciter l'assistance du groupe de coopération à cet égard.

De l'avis de la Commission, les États membres devraient s'efforcer de parvenir à un consensus sur ces questions afin d'éviter que la même entreprise ne soit soumise à un statut juridique différent dans différents États membres. Les divergences devraient être vraiment exceptionnelles, par exemple lorsqu'une entité déterminée comme OSE dans un État membre exerce une activité marginale et insignifiante dans un autre État membre.

4.2. Exigences de sécurité.

En vertu de l'article 14, paragraphe 1, les États membres sont tenus de veiller à ce que les OSE, compte tenu de l'état des connaissances, prennent des mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que les organismes utilisent pour la fourniture de leurs services. Conformément à l'article 14, paragraphe 2, les mesures appropriées doivent contribuer à prévenir un incident et en limiter l'impact.

Un groupe de travail spécialisé du groupe de coopération travaille actuellement sur des lignes directrices non contraignantes concernant les mesures de sécurité applicables aux OSE[32]. Le document d'orientation devrait être finalisé par le groupe au quatrième trimestre 2017. La Commission encourage les États membres à respecter minutieusement le document d'orientation qui sera élaboré par le groupe de coopération afin d'aligner autant que possible les dispositions nationales relatives aux exigences de sécurité. L'harmonisation de ces exigences favoriserait grandement le respect par les OSE qui fournissent souvent des services essentiels dans plus d'un État membre, et faciliterait les tâches de surveillance des autorités nationales compétentes et des CSIRT.

[32] Aux fins des activités menées par ce groupe de travail, des listes de normes internationales, de bonnes pratiques et de méthodologies d'évaluation et de gestion des risques pour tous les secteurs couverts par la directive SRI ont été diffusées et ont servi aux discussions sur les domaines de sécurité et les mesures de sécurité proposés.

4.3 Exigences en matière de notification.

Conformément à l'article 14, paragraphe 3, les États membres doivent veiller à ce que les OSE notifient «*les incidents qui ont un impact significatif sur la continuité des services essentiels*». Par conséquent, les OSE ne doivent pas notifier d'incidents mineurs, mais uniquement des incidents graves qui affectent la continuité du service essentiel. L'article 4, paragraphe 7, désigne par «incident» «*tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information*». Le terme «sécurité des réseaux et des systèmes d'information» est défini à l'article 4, paragraphe 2, comme «*la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles*». En conséquence, tout événement ayant un impact négatif non seulement sur la disponibilité, mais aussi sur l'authenticité, l'intégrité ou la confidentialité des données ou des services connexes pourrait potentiellement déclencher l'obligation de notification. En effet, la continuité du service telle que visée à l'article 14, paragraphe 3, peut être compromise non seulement dans les cas où la disponibilité matérielle est en jeu, mais aussi par tout autre incident de sécurité affectant la bonne fourniture du service[33].

Un groupe de travail spécialisé au sein du groupe de coopération élabore actuellement des lignes directrices non contraignantes en matière de notification concernant les circonstances dans lesquelles les opérateurs de services essentiels sont tenus de notifier les incidents conformément à l'article 14, paragraphe 7, ainsi que le format et la procédure des notifications nationales. Les lignes directrices devraient être finalisées d'ici le quatrième trimestre de 2017.

La diversité des exigences nationales en la matière peut être un facteur d'insécurité juridique, entraîner des procédures plus complexes et plus lourdes ainsi que des frais administratifs importants pour les fournisseurs ayant une activité transnationale. La Commission se félicite donc des travaux menés par le groupe de coopération. Comme pour les exigences en matière de sécurité, la Commission encourage les États membres à respecter minutieusement le document d'orientation qui sera élaboré par le groupe de coopération afin d'aligner autant que possible les dispositions nationales relatives à la notification des incidents.

4.4. Directive SRI, annexe III: fournisseurs de service numérique.

Les fournisseurs de service numérique (FSN) constituent la deuxième catégorie d'entités incluses dans le champ d'application de la directive SRI. Ces entités sont considérées comme des acteurs économiques importants du fait qu'elles sont utilisées par de nombreuses entreprises pour la fourniture de leurs propres services, et qu'une perturbation du service numérique pourrait avoir une incidence sur des fonctions économiques et sociétales clés.

[33] Il en va de même pour les FSN.

4.4.1. Catégories de FSN.

L'article 4, paragraphe 5, qui définit le service numérique renvoie à la définition juridique de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 en limitant le champ d'application aux types de services visés à l'annexe III. En particulier, l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 définit ces services comme «*tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services*» et l'annexe III de la directive énumère trois types spécifiques de services: place de marché en ligne, moteurs de recherche en ligne et service d'informatique en nuage. Par rapport aux opérateurs de services essentiels, la directive n'oblige pas les États membres à identifier les fournisseurs de service numérique, qui seraient alors soumis aux obligations correspondantes. Par conséquent, les obligations applicables de la directive, à savoir les exigences en matière de sécurité et de notification énoncées à l'article 16, s'appliqueront à tous les FSN relevant de son champ d'application.

Les sections suivantes fournissent des explications supplémentaires concernant trois types de services numériques relevant du champ d'application de la directive.

1. Fournisseur de place de marché en ligne.

Une place de marché en ligne permet à un grand nombre et à une grande variété d'entreprises d'exercer leurs activités commerciales vis-à-vis des consommateurs et de s'engager dans des relations interentreprises. Elle fournit aux entreprises l'infrastructure de base pour le commerce en ligne et transfrontalier. Elle joue un rôle important dans l'économie, notamment en permettant aux PME d'accéder au marché unique numérique de l'Union au sens large. La fourniture de services informatiques à distance facilitant l'activité économique de ses clients, y compris le traitement des transactions et l'agrégation d'informations sur les acheteurs, les fournisseurs et les produits peut également faire partie des activités d'un fournisseur de place de marché en ligne, au même titre que la facilitation de la recherche de produits appropriés, la fourniture de produits, l'expertise transactionnelle et la mise en relation des acheteurs et des vendeurs.

Le terme «place de marché en ligne» est défini à l'article 4, paragraphe 17, et précisé au considérant 15. Il est décrit comme un service qui permet aux consommateurs et aux professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels, et comme la destination finale pour la conclusion desdits contrats. Par exemple, un fournisseur tel qu'*E-bay* peut être considéré comme une place de marché en ligne car il permet à d'autres fournisseurs de créer des boutiques sur sa plate-forme afin de mettre leurs produits et services en ligne à la disposition des consommateurs ou des entreprises. En outre, les magasins d'applications en ligne destinés à la distribution d'applications et de logiciels sont considérés comme relevant de la définition de la place de marché en ligne parce qu'ils permettent aux développeurs d'applications de vendre ou de distribuer leurs services aux consommateurs ou à d'autres entreprises. En revanche, les intermédiaires de services tiers tels que *Skyscanner* et les services de comparaison de prix, qui redirigent l'utilisateur vers le site internet du professionnel où le contrat de service ou de produit est effectivement conclu, ne sont pas couverts par la définition de l'article 4, paragraphe 17.

2. Fournisseur de moteur de recherche en ligne.

Le terme «moteur de recherche en ligne» est défini à l'article 4, paragraphe 18, et précisé au considérant 16. Il est décrit comme un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet. Les fonctionnalités de recherche limitées aux sites internet de recherche sur site et de comparaison des prix ne sont pas couvertes. Par exemple, un type de moteur de recherche tel que celui qui est fourni par EUR LEX[34] ne peut pas être considéré comme un moteur de recherche au sens de la directive, car sa fonction de recherche est limitée au contenu de ce site internet en particulier.

3. Fournisseur de service d'informatique en nuage.

L'article 4, paragraphe 19, définit un service d'informatique en nuage comme «un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagée» et le considérant 17 apporte des éclaircissements supplémentaires sur les termes «ressources informatiques», «modulable» et «ensemble variable».

En résumé, l'informatique en nuage peut être décrite comme un type particulier de service informatique qui utilise des ressources partagées pour traiter des données à la demande, les ressources partagées désignant tout type de composants matériels ou logiciels (réseaux, serveurs ou autres infrastructures, stockage, applications et services) mis à la disposition des utilisateurs à la demande pour le traitement des données. Le terme «pouvant être partagée» définit les ressources informatiques dans lesquelles de nombreux utilisateurs utilisent la même infrastructure physique pour le traitement des données. La ressource informatique peut être définie comme «pouvant être partagée» si l'ensemble de ressources utilisées par le prestataire peut être étendu ou réduit à tout moment, en fonction des besoins de l'utilisateur. Ainsi, des centres de données ou des composants individuels au sein d'un même centre de données pourraient éventuellement être ajoutés ou supprimés si la quantité totale de capacité de calcul ou de stockage nécessite une mise à jour. Le terme «ensemble variable» peut être décrit comme une modification de la charge de travail par l'approvisionnement et le désapprovisionnement automatique des ressources, de telle sorte qu'à chaque instant les ressources disponibles correspondent le plus possible à la demande actuelle[35].

Il existe actuellement trois principaux types de modèles de service en nuage qu'un fournisseur peut proposer:

- Infrastructure à la demande (*Infrastructure as a Service* – IaaS): Une catégorie de services en nuage dans laquelle le type de services fournis au client est une infrastructure. Il comprend la livraison virtuelle de ressources informatiques sous forme de matériel, de

[34] Disponible à l'adresse suivante: http://eur-lex.europa.eu/homepage.html

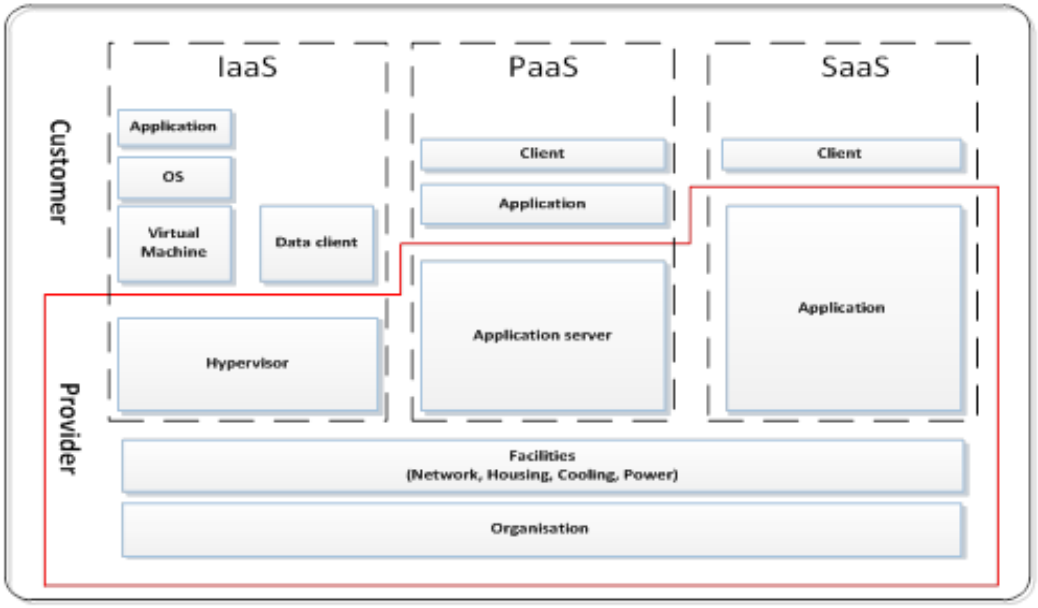
[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, «Elasticity in Cloud Computing: What It Is, and What It Is Not», disponible à l'adresse: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Voir également les pages 2 à 5 du document COM (2012)529.

réseaux et de services de stockage. L'IaaS alimente les serveurs, le stockage, les réseaux et les systèmes d'exploitation. Il fournit une infrastructure d'entreprise dans laquelle une entreprise peut stocker ses données et exécuter les applications nécessaires à son fonctionnement quotidien.

- Plateforme à la demande (*Platform as a Service* – PaaS): Une catégorie de services en nuage dans laquelle le type de services fournis au client est une plateforme. Il comprend des plateformes informatiques en ligne qui permettent aux entreprises d'exécuter des applications existantes ou de développer et tester de nouvelles applications.

- Logiciel à la demande (*Software as a service* – SaaS): Une catégorie de services en nuage dans laquelle le type de services fournis au client est une application ou un logiciel déployé sur internet. Ce type de services en nuage supprime la nécessité pour l'utilisateur final d'acheter, d'installer et de gérer des logiciels et présente l'avantage de rendre le logiciel accessible depuis n'importe quel endroit avec une connexion internet.

Illustration n° 5: Modèles de services et ressources dans l'informatique en nuage



L'ENISA a produit des lignes directrices détaillées sur des sujets spécifiques dans le domaine de l'informatique en nuage[36], ainsi qu'un document d'orientation sur les fondamentaux de l'informatique en nuage[37].

[36] Elles sont disponibles à l'adresse: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs*, 2015. Disponible à l'adresse: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

4.4.2. Exigences de sécurité.

En vertu de l'article 16, paragraphe 1, les États membres sont tenus de veiller à ce que les FSN, prennent des mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que les entreprises utilisent pour la fourniture de leurs services. Ces mesures de sécurité devraient tenir compte de l'état des connaissances et des cinq éléments suivants: i) la sécurité des systèmes et des installations; ii) la gestion des incidents; iii) la gestion de la continuité des activités; iv) le suivi, l'audit et le contrôle; v) le respect des normes internationales.

À cet égard, la Commission est habilitée, en vertu de l'article 16, paragraphe 8, à adopter des actes d'exécution afin de compléter ces éléments et d'assurer un niveau élevé d'harmonisation pour ces prestataires de services. L'acte d'exécution devrait être adopté par la Commission à l'automne 2017. En outre, les États membres sont tenus de veiller à ce que les fournisseurs de service numérique prennent les mesures nécessaires pour prévenir les incidents et en limiter l'impact en vue d'assurer la continuité de leurs services.

4.4.3. Exigences en matière de notification.

Les FSN devraient être tenus de notifier les incidents graves aux autorités compétentes ou aux CSIRT. Conformément à l'article 16, paragraphe 3, de la directive SRI, l'obligation de notification pour les fournisseurs de service numérique sera déclenchée dans les cas où l'incident de sécurité a un impact significatif sur la fourniture du service. Afin de déterminer l'importance de l'impact d'un incident, l'article 16, paragraphe 4, énumère en particulier cinq paramètres qui doivent être pris en considération par les fournisseurs de service numérique. À cet égard, la Commission est habilitée, en vertu de l'article 16, paragraphe 8, à adopter des actes d'exécution fournissant une description plus détaillée des paramètres. La spécification de ces paramètres fera partie intégrante de l'acte d'exécution précisant les éléments de sécurité mentionnés au point 4.4.2, que la Commission a l'intention d'adopter à l'automne.

4.4.4. Approche réglementaire fondée sur le risque.

L'article 17 dispose que les FSN sont soumis au contrôle a posteriori des autorités nationales compétentes. Les États membres doivent veiller à ce que les autorités compétentes prennent des mesures lorsque, selon les éléments communiqués, un FSN ne satisfait pas aux exigences énoncées à l'article 16 de la directive.

En outre, en vertu de l'article 16, paragraphes 8 et 9, la Commission est habilitée à adopter des actes d'exécution relatifs aux exigences de notification et de sécurité qui renforceront le niveau d'harmonisation pour les FSN. De plus, en vertu de l'article 16, paragraphe 10, les États membres ne sont pas autorisés à imposer aux FSN des exigences liées à la sécurité et aux notifications plus strictes que celles prévues par la directive, sauf dans les cas où de telles mesures sont nécessaires pour préserver leurs fonctions étatiques essentielles, en particulier dans le but de préserver la sécurité nationale, et permettre la recherche, la détection et la poursuite d'infractions pénales.

Enfin, compte tenu du caractère transfrontalier des FSN, la directive ne suit pas le modèle des juridictions parallèles multiples, mais une approche fondée sur le critère de l'établissement principal de la société au sein de l'Union[38]. Cette approche permet d'appliquer un ensemble unique de règles aux FSN, avec une autorité compétente responsable de la surveillance, ce qui est particulièrement important dans la mesure où de nombreux FSN offrent leurs services simultanément dans de nombreux États membres. L'application de cette approche réduit au minimum la charge imposée aux fournisseurs de service numérique et garantit le bon fonctionnement du marché unique numérique.

4.4.5. Compétence.

Comme expliqué ci-dessus, conformément à l'article 18, paragraphe 1, de la directive SRI, un FSN est considéré comme relevant de la compétence de l'État membre dans lequel il a son établissement principal. Dans les cas où le FSN concerné n'est pas établi dans l'Union mais fournit des services à l'intérieur de l'Union, l'article 18, paragraphe 2, impose au FSN l'obligation de désigner un représentant dans l'Union. Dans ce cas, le FSN est considéré comme relevant de la compétence de l'État membre dans lequel le représentant est établi. Dans les cas où un FSN fournit des services dans un État membre mais n'a pas désigné de représentant dans l'Union, l'État membre peut en principe prendre des mesures à l'encontre du FSN, car il enfreint les obligations qui lui incombent en vertu de la directive.

4.4.6. Exemption des fournisseurs de service numérique à échelle limitée concernant les exigences en matière de sécurité et de notification

Conformément à l'article 16, paragraphe 11, les fournisseurs de service numérique qui sont des microentreprises ou des petites entreprises au sens de la recommandation 2003/361/CE[39] de la Commission sont exclus du champ d'application des exigences en matière de sécurité et de notification visées à l'article 16. Cela signifie que les entreprises qui emploient moins de 50 personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel ne dépasse pas 10 millions d'EUR ne sont pas liées par ces exigences. Pour déterminer la taille de l'entité, il importe peu de savoir si la société concernée ne fournit que des services numériques au sens de la directive SRI ou d'autres services.

5. La relation entre la directive SRI et d'autres textes législatifs.

La présente section se concentre sur les dispositions de lex specialis figurant à l'article 1er, paragraphe 7, de la directive SRI, illustrant les trois exemples de lex specialis évalués jusqu'à présent par la Commission et clarifiant les exigences de sécurité et de notification appliquées aux fournisseurs de services de télécommunications et aux prestataires de services de confiance.

[38] Voir en particulier l'article 18 de la directive.
[39] JO L 24 du 20.5.2003, p. 36.

5.1. Directive SRI – article premier, paragraphe 7: La disposition de lex specialis.

Conformément à l'article 1er, paragraphe 7, de la directive SRI, les dispositions relatives aux exigences de sécurité et/ou de notification applicables aux fournisseurs de service numérique ou aux opérateurs de services essentiels en vertu de la directive ne sont pas applicables si une législation sectorielle de l'Union prévoit des exigences de sécurité et/ou de notification qui ont un effet au moins équivalent à celui des obligations correspondantes de la directive SRI. Les États membres doivent tenir compte de l'article 1er, paragraphe 7, dans la transposition globale de la directive et fournir à la Commission des informations sur l'application des dispositions de lex specialis.

Méthode.

Lors de l'évaluation de l'équivalence d'une législation sectorielle de l'Union avec les dispositions pertinentes de la directive SRI, il convient d'accorder une importance particulière à la question de savoir si les obligations en matière de sécurité prévues par la législation sectorielle comprennent des mesures garantissant la sécurité des réseaux et des systèmes d'information au sens de l'article 4, paragraphe 2, de la directive.

En ce qui concerne les obligations de notification, l'article 14, paragraphe 3 et l'article 16, paragraphe 3, de la directive SRI disposent que les opérateurs de services essentiels et les fournisseurs de service numérique doivent notifier aux autorités compétentes ou au CSIRT, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services. À cet égard, il convient d'accorder une attention particulière aux obligations qui incombent à l'opérateur/au fournisseur de service numérique d'inclure dans la notification des informations permettant à l'autorité compétente ou au CSIRT d'évaluer l'ampleur de l'éventuel impact au niveau transfrontalier.

Actuellement, aucune législation sectorielle spécifique pour la catégorie des fournisseurs de service numérique ne prévoit des exigences de sécurité et de notification comparables à celles énoncées à l'article 16 de la directive SRI, qui peuvent être prises en considération dans l'application de l'article 1er, paragraphe 7, de la directive SRI[40].

En ce qui concerne les opérateurs de services essentiels, le secteur financier, et notamment les infrastructures bancaires et des marchés financiers visées aux points 3 et 4 de l'annexe II, est actuellement soumis à des obligations de sécurité et/ou de notification découlant de la législation sectorielle de l'Union. Cela s'explique par le fait que la sécurité et la solidité des systèmes informatiques et des systèmes de réseau et d'information utilisés par les institutions financières constituent un élément essentiel des exigences de risque opérationnel imposées aux institutions financières en vertu de la législation de l'Union.

Exemples.

i) Directive sur les services de paiement 2

[40] Ceci est sans préjudice de la notification à l'autorité de contrôle d'une violation de données à caractère personnel, visée à l'article 33 du règlement général sur la protection des données.

En ce qui concerne le secteur bancaire, et en particulier la prestation de services de paiement par les établissements de crédit tels que définis à l'article 4, point 1), du règlement (UE) nº 575/2013, la deuxième directive sur les services de paiement (DSP 2)[41] prévoit des exigences en matière de sécurité et de notification qui sont énoncées aux articles 95 et 96 de cette directive.

Plus précisément, l'article 95, paragraphe 1, exige des prestataires de services de paiement qu'ils adoptent des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent. Ces mesures devraient prévoir l'établissement et le maintien de procédures efficaces de gestion des incidents, y compris des procédures de détection et de classification des incidents opérationnels et de sécurité majeurs. Les considérants 95 et 96 de la DSP 2 clarifient davantage la nature de ces mesures de sûreté. Il ressort de ces dispositions que les mesures prescrites visent à gérer les risques de sécurité liés au réseau et aux systèmes d'information utilisés pour la fourniture de services de paiement. Par conséquent, ces exigences en matière de sécurité peuvent être considérées comme ayant un effet au moins équivalent à celui des dispositions correspondantes de l'article 14, paragraphes 1 et 2, de la directive SRI.

En ce qui concerne les obligations de notification, l'article 96, paragraphe 1, de la DSP 2 prévoit l'obligation pour les prestataires de services de paiement d'informer sans retard injustifié l'autorité compétente en cas d'incidents de sécurité majeurs. En outre, dans la mesure où il est comparable à l'article 14, paragraphe 5, de la directive SRI, l'article 96, paragraphe 2, de la DSP 2 impose à l'autorité compétente d'informer les autorités compétentes des autres États membres si un incident les concerne. Cette obligation suppose dans le même temps que le signalement des incidents de sécurité doit inclure des informations permettant aux autorités d'évaluer l'impact d'un incident au niveau transfrontalier. L'article 96, paragraphe 3, point a), de la DSP 2 habilite à cet égard l'ABE, en coopération avec la BCE, à élaborer des orientations sur le contenu exact et le format de la notification.

Par conséquent, on peut conclure qu'en vertu de l'article 1er, paragraphe 7, de la directive SRI, les exigences en matière de sécurité et de notification énoncées aux articles 95 et 96 de la DSP 2 devraient s'appliquer à la place des dispositions correspondantes de l'article 14 de la directive SRI en ce qui concerne la prestation de services de paiement par les établissements de crédit.

ii) Règlement (UE) nº 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux.

En ce qui concerne l'infrastructure des marchés financiers, le règlement (UE) nº 648/2012, en liaison avec le règlement délégué (UE) nº 153/2013 de la Commission, contient des dispositions relatives aux exigences de sécurité pour les contreparties centrales, qui peuvent

[41] Directive (UE) 2015/2366, JO L 337 du 23.12.2015, p. 35.

être considérées comme la lex specialis. En particulier, les actes juridiques prévoient des mesures techniques et organisationnelles liées à la sécurité des réseaux et des systèmes d'information qui, en termes de détail, vont même au-delà des exigences de l'article 14, paragraphes 1 et 2, de la directive SRI et peuvent donc être considérées comme satisfaisant aux exigences de l'article 1er, paragraphe 7, de la directive SRI en ce qui concerne les exigences de sécurité.

Plus précisément, l'article 26, paragraphe 1, du règlement (UE) nº 648/2012 dispose que l'entité doit disposer d'un «*solide dispositif de gouvernement d'entreprise, comprenant notamment une structure organisationnelle claire avec un partage des responsabilités qui soit bien défini, transparent et cohérent, des procédures efficaces de détection, de gestion, de contrôle et de déclaration des risques auquel il est ou pourrait être exposé et des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines*». L'article 26, paragraphe 3, dispose que la structure organisationnelle doit assurer la continuité et le bon fonctionnement de la fourniture des services et de l'exercice des activités en utilisant des systèmes, des ressources et des procédures appropriés et proportionnés.

En outre, l'article 26, paragraphe 6, précise que les contreparties centrales doivent maintenir «*des systèmes informatiques appropriés pour gérer la complexité, la diversité et le type des services fournis et des activités exercées, de manière à garantir des normes de sécurité élevées et l'intégrité et la confidentialité des informations conservées*». De plus, l'article 34, paragraphe 1, impose aux contreparties centrales d'établir, de mettre en œuvre et d'entretenir une politique adéquate de continuité des activités et un plan de rétablissement après sinistre visant à assurer la reprise des activités en temps opportun.

Ces obligations sont précisées dans le règlement délégué (UE) nº 153/2013 de la Commission du 19 décembre 2012 complétant le règlement (UE) nº 648/2012 du Parlement européen et du Conseil en ce qui concerne les normes techniques de réglementation régissant les exigences applicables aux contreparties centrales[42]. En particulier, l'article 4 impose aux contreparties centrales de mettre au point des outils de gestion des risques appropriés leur permettant de gérer tous les risques pertinents et précise le type de mesures (notamment, utilisation de systèmes d'information et de maîtrise des risques solides, disponibilité des ressources et de l'expertise et accès à toutes les informations pertinentes pour la fonction de gestion des risques, disponibilité de mécanismes de contrôle interne adéquats tels que des procédures administratives et comptables saines pour aider leur conseil d'administration à suivre et à vérifier l'adéquation et l'efficacité de leurs politiques, procédures et systèmes de gestion des risques).

En outre, l'article 9 fait explicitement référence à la sécurité des systèmes informatiques et impose des mesures techniques et organisationnelles concrètes liées au maintien d'un cadre solide de sécurisation de l'information pour la gestion des risques en matière de sécurité informatique. Ces mesures devraient inclure des mécanismes et des procédures garantissant la

[42] JO L 52 du 23.2.2013, p. 41.

disponibilité des services et la protection de l'authenticité, de l'intégrité et de la confidentialité des données.

iii) Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE[43].

En ce qui concerne les plates-formes de négociation, l'article 48, paragraphe 1, de la directive 2014/65/UE impose aux opérateurs d'assurer le maintien de leurs services en cas de défaillance de leur système de négociation. Cette obligation générale a été récemment précisée et complétée par le règlement délégué (UE) 2017/584[44] de la Commission du 14 juillet 2016 complétant la directive 2014/65/UE du Parlement européen et du Conseil par des normes techniques de réglementation précisant les exigences organisationnelles applicables aux plates-formes de négociation[45]. En particulier, l'article 23, paragraphe 1, de ce règlement précise que les plates-formes de négociation disposent de procédures et de mécanismes de sécurité physique et électronique conçus pour protéger leurs systèmes de toute utilisation abusive ou de tout accès non autorisé et pour garantir l'intégrité des données. Ces mesures devraient permettre de prévenir ou de minimiser les risques d'attaques contre les systèmes d'information.

L'article 23, paragraphe 2, dispose en outre que les mesures et les mécanismes mis en place par les opérateurs devraient permettre une identification et une gestion rapides du risque lié à tout accès non autorisé, à toute interférence avec le système ayant pour effet d'entraver gravement ou d'interrompre le fonctionnement des systèmes d'information et à toute interférence avec les données ayant pour effet de compromettre la disponibilité, l'intégrité ou l'authenticité des données. En outre, l'article 15 du règlement impose aux plates-formes de négociation l'obligation de mettre en place des mécanismes efficaces de continuité des activités afin d'assurer une stabilité suffisante du système et de faire face aux incidents perturbateurs. En particulier, ces mesures devraient garantir qu'après un incident perturbateur, la négociation peut reprendre dans les deux heures, ou dans un délai proche de deux heures, et que la quantité maximale de données susceptibles d'être perdues par un service informatique de la plate-forme de négociation est proche de zéro.

L'article 16 dispose en outre que les mesures identifiées pour traiter et gérer les incidents perturbateurs devraient faire partie du plan de continuité des activités des plates-formes de négociation et prévoit des éléments particuliers dont l'opérateur doit tenir compte lorsqu'il adopte le plan de continuité des activités (par exemple, la mise en place d'une équipe spécifique chargée des activités de sécurité, la réalisation d'une analyse d'impact recensant les risques qui est réexaminée périodiquement).

[43] JO L 173 du 12.6.2014, p. 349.
[44] JO L 87 du 31.3.2017, p. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_fr.pdf

Compte tenu du contenu de ces mesures de sécurité, il apparaît qu'elles visent à gérer et à traiter le risque lié à la disponibilité, à l'authenticité, à l'intégrité et à la confidentialité des données ou des services fournis et, par conséquent, il peut être conclu que la législation sectorielle de l'Union susmentionnée contient des obligations en matière de sécurité qui ont de fait un effet au moins équivalent à celui des obligations correspondantes de l'article 14, paragraphes 1 et 2, de la directive SRI.

5.2 Directive SRI – article premier, paragraphe 3: Fournisseurs de télécommunications et prestataires de services de confiance.

Conformément à l'article 1er, paragraphe 3, les exigences en matière de sécurité et de notification prévues par la directive ne s'appliquent pas aux prestataires qui sont soumis aux exigences énoncées aux articles 13 bis et 13 ter de la directive 2002/21/CE. Les articles 13 bis et 13 ter de la directive 2002/21/CE s'appliquent aux entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public. Par conséquent, en ce qui concerne la fourniture de réseaux de communications publics ou de services de communications électroniques accessibles au public, l'entreprise doit se conformer aux exigences en matière de sécurité et de notification prévues par la directive 2002/21/CE.

Toutefois, si la même société fournit également d'autres services tels que des services numériques (par exemple, informatique en nuage ou place de marché en ligne) énumérés à l'annexe III de la directive SRI ou des services tels que le DNS ou l'IXP conformément à l'annexe II, point 7, de la directive SRI, elle sera soumise aux exigences de sécurité et de notification prévues par la directive SRI pour la fourniture de ces services particuliers. Il convient de noter qu'en raison du fait que les prestataires de services énumérés à l'annexe II, point 7, appartiennent à la catégorie des opérateurs de services essentiels, les États membres sont tenus de procéder à une procédure d'identification conformément à l'article 5, paragraphe 2, et d'identifier les fournisseurs individuels de services DNS, IXP ou TLD qui devraient satisfaire aux exigences de la directive SRI. Cela signifie qu'après une telle évaluation, seuls les fournisseurs DNS, IXP ou TLD qui remplissent les critères de l'article 5, paragraphe 2, de la directive SRI seront tenus de se conformer aux exigences de la directive SRI.

L'article 1er, paragraphe 3, précise en outre que les exigences en matière de sécurité et de notification prévues par la directive ne s'appliquent pas non plus aux prestataires de services de confiance qui sont soumis à des exigences similaires en vertu de l'article 19 du règlement (UE) nº 910/2014.

6. Documents publiés sur la stratégie nationale en matière de cybersécurité

	État membre	Titre de la stratégie et liens disponibles
1	Autriche	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgique	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgarie	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Croatie	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	République tchèque	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Chypre	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Danemark	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estonie	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finlande	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	France	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irlande	*National Cyber Security Strategy 2015-2017* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italie	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Allemagne	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Hongrie	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Lettonie	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Lituanie	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxembourg	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malte	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Pays-Bas	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Pologne	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Roumanie	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugal	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view

		(EN)
23	République slovaque	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovénie	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Espagne	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Suède	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Royaume-Uni	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Liste des bonnes pratiques et recommandations de l'ENISA.

Réponse en cas d'incident

- ✓ Procédure de réponse aux incidents et coopération en cas de cybercrise[46]

Gestion des incidents

- ✓ Projet d'automatisation de la gestion des incidents[47]
- ✓ Guide de bonnes pratiques pour la gestion des incidents[48]

Classification et taxonomie des incidents

- ✓ Aperçu des taxonomies existantes[49]
- ✓ Guide de bonnes pratiques sur l'utilisation des taxonomies dans la prévention et la détection des incidents[50]

Maturité des CSIRT

- ✓ Défis pour les CSIRT nationaux en Europe en 2016: étude sur la maturité des CSIRT[51]
- ✓ Étude sur la maturité des CSIRT – Processus d'évaluation[52]
- ✓ Lignes directrices pour les CSIRT nationaux et gouvernementaux sur la manière d'évaluer la maturité[53]

Renforcement des capacités et formation des CSIRT

- ✓ Guide des bonnes pratiques sur les méthodologies de formation[54]

Pour trouver des informations sur les CSIRT existants en Europe - Aperçu des CSIRT par pays[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Disponible à l'adresse:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Pour en savoir plus: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Disponible à l'adresse:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Pour en savoir plus: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Disponible à l'adresse:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Disponible à l'adresse:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Disponible à l'adresse:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Disponible à l'adresse: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Disponible à l'adresse:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Pour en savoir plus: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map