RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2

UNE INTRODUCTION AUX ENJEUX DE LA DIRECTIVE POUR LE SECTEUR DES TÉLÉCOMMUNICATIONS

Ionathan NOBLINS
Coordinateur pour la sécurité des télécommunications et des infrastructures du numérique
ANSSI

NIS2 : introduction aux enjeux pour le secteur des télécommunications

Objectifs de l'intervention

1. Faire connaître le nouveau cadre apporté par la directive NIS2
2. Permettre aux membres du FRnOG de :

- Se repérer

Anticiper

- Gagner du temps

Préambule

- La présente introduction n'a pas vocation à être exhaustive ;
- Les travaux relatifs à la transposition nationale de la directive sont en cours ;
- Les éclairages apportés ne sauraient remplacer les analyses juridiques internes nécessaires à l'appréciation des situations particulières à chaque entité.

Introduction

Genèse

Illustration : publications ANSSI

2016 : adoption par le Parlement européen de la 1ère directive NIS

- **N**etwork and **I**nformation system **S**ecurity /
  Sécurité des Réseaux et des systèmes d'Information
- Ciblage de certains **grands acteurs** économiques du marché intérieur et de leurs systèmes d'information (OSE, SIE)
- Renforcement du cadre de **coopération** entre états membres de l'UE en matière de cybersécurité (ex. GC NIS, EU-CyCLONe)

Depuis (8 ans) : évolution des menaces cyber

- Niveaux de menace et de **cybercriminalité** en augmentation
- Nouvelles **victimes** (ex. collectivités territoriales, ETI, PME)
- Amélioration des **capacités** offensives (ex. attaques à grande échelle)
- Ciblage soutenu d'**intermédiaires** (dont les télécoms)

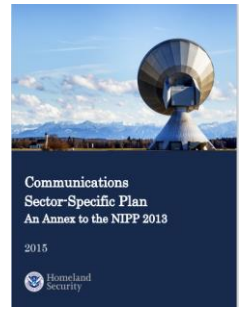
La menace cyber aujourd'hui

Une menace protéiforme à laquelle NIS2 répond de façon ciblée

La dernière édition du panorama de la menace distingue 3 principales **finalités** des attaquants, et met en évidence différents modes opératoires mis en œuvre :

	Gain financier	Déstabilisation	Espionnage
En général	• Augmentation de 30% des attaques par **rançongiciel** (ex. LockBit, Black Cat) • Chantage au DDoS	• **DDoS** par des groupes hacktivistes pro-russes (ex. NoName057, Anonymous Sudan)	• La menace qui a le plus mobilisé l'ANSSI • Ciblage d'instituts de recherche et de la **BITD**
Dans le secteur	• **Fuite de données** puis revente (ex. DCP) • Compromission de PABX pour mener des activités frauduleuses (ex. appels vers numéros surtaxés, services d'appels à bas prix)	• Le secteur est considéré comme particulièrement exposé à cette menace, notamment en temps de guerre (cf. diapositive suivante)	• Attaquants réputés liés aux intérêts chinois (ex. **Gallium**) • De plus en plus d'attaques réalisées au moyen de MOA associés publiquement au gouvernement russe (ex. **Turla**, **Sandworm**)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité



Une menace sectorielle bien réelle

Des entités de toutes tailles ciblées massivement, avec d'importants impacts métier

En moyenne, pour le secteur, et sur les dernières années, 1 événement de sécurité significatif par semaine a été porté à la connaissance de l'ANSSI, pouvant aller jusqu'à l'**interruption complète de l'activité** des opérateurs, accompagnée des inévitables **pertes financières** et impacts sur l'image associés.

En temps de paix	• Attaques par **rançongiciel** ciblant principalement des **entités de taille moyenne** • Compromission d'un **opérateur national** dans un but probable d'**espionnage** par le biais d'un MOA réputé chinois
En temps de guerre	• Réseau **KA-SAT** : mise hors service de dizaines de milliers de modems satellites • **Kyivstar** : mise hors service du cœur de réseau • **Infamous Chisel** : infection de terminaux de l'armée UKR
Dans l'actualité	• Panne massive chez **Vodafone Portugal** à la suite d'une cyberattaque • Fuites de données massives chez les opérateurs **AT&T**, **Telefónica**, **T-Mobile** • Attaque par rançongiciel sur un **FAI ultramarin**

De premières généralités sur NIS2

Une hygiène informatique de base pour faire face à la cybercriminalité de masse

Objectifs & grands principes

- Élever **le niveau** de cybersécurité dans l'UE **face à la cybercriminalité** de masse
- ➢ Étendre le périmètre assujetti à de plus **petites structures**
- ➢ Introduire des obligations, notamment de **gestion des risques**
- ➢ Continuer de renforcer la **coopération** entre états membres

Quelques concepts clés

- **Champ d'application** : sur qui, sur quoi
  - *Nature d'activité = secteurs et types d'entités*
  - *Volume d'activité = statut important ou essentiel*
  - *Portée = tous SI et réseaux*
- **Proportionnalité** EI/EE : obligations, sanctions

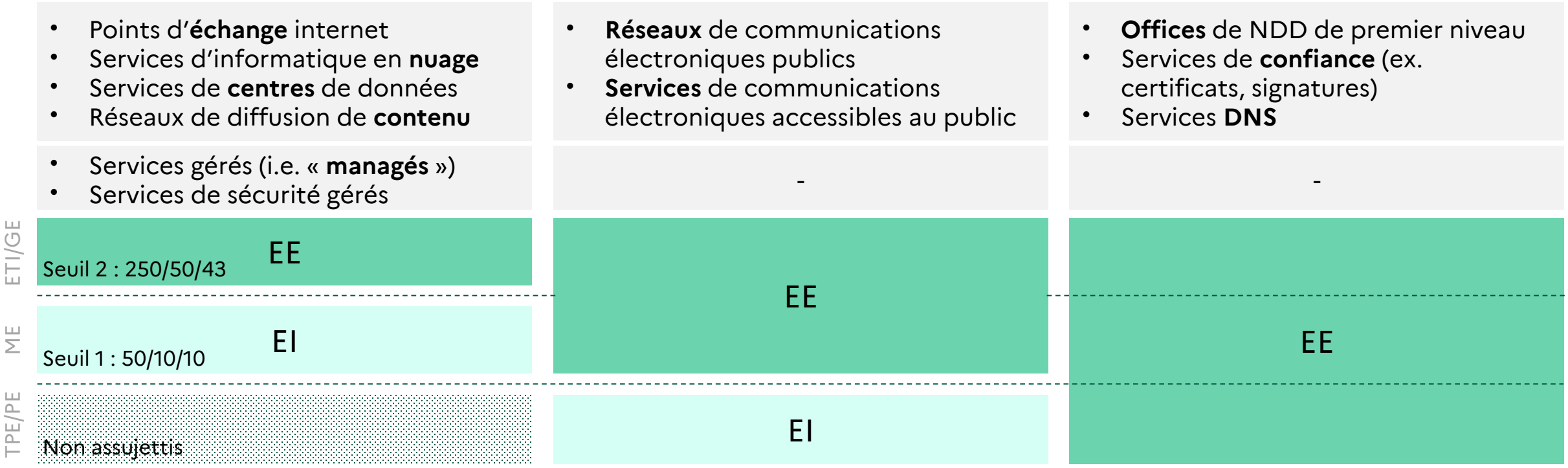
Illustration : chapitres et orientation (25 p. /72)

Section	p.
Considérations	28
Chapitre I - Dispositions générales	**4**
Chapitre II - Cadres coordonnés	6
Chapitre III - Coopération UE/Int	6
Chapitre IV - Mesures de gestion des risques	**6**
Chapitre V - Compétence et enregistrement	**2**
Chapitre VI - Partage d'informations	2
Chapitre VII - Supervision et exécution	**7**
Chapitre VIII - Actes délégués et d'exécution	**1**
Chapitre IX - Dispositions finales	1
Annexes I - Secteurs hautement critiques	**4**
Annexe II - Autres secteurs critiques	3
Tableau de correspondance	3

Caractérisation des entités du secteur

Entités importantes et essentielles (EI/EE) : cas général, cas particuliers

Selon leur **nature et volume d'activité**, exprimés en effectif/CA/bilan, les 11 types d'entités des secteurs 8 (infrastructures numériques) et 9 (gestion de services TIC) se répartissent selon leur statut EI ou EE.



Proportionnalité : Obligations, Sanctions

Une hygiène informatique de base pour faire face à la cybercriminalité de masse

Obligations

- Les **thématiques habituelles** de la cybersécurité, ex. cartographie, analyse des risques, MCS, sauvegardes, gestion des prestataires, des incidents, etc.
- Un référentiel national **souple** et **proportionné** articulé sur la notion d'**objectifs**, toujours en co-construction (ex. avec un ensemble d'organisations professionnelles et de ministères).

Sanctions

- Notamment financières, de façon simplifiée : jusqu'à **2% du CA** mondial pour les EE ; 1,4% pour les EI.

Autres informations choisies

- L'**enregistrement** et la notification des **incidents**
- La **territorialité** et le **règlement d'exécution** (référentiel européen)
- Le traitement particulier des fournisseurs de **services d'enregistrement** DNS (ex. BE).

En (presque) conclusion pour les membres du FRnOG 

Quelques clés pour une bonne préparation

1. Consulter le site **MonEspaceNIS2** (en version beta), la première pierre du dispositif d'accompagnement

- https://monespacenis2.cyber.gouv.fr/

2. Familiariser vos entités avec la **directive**, opérationnels notamment, équipes juridiques et SSI le cas échéant

- https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555

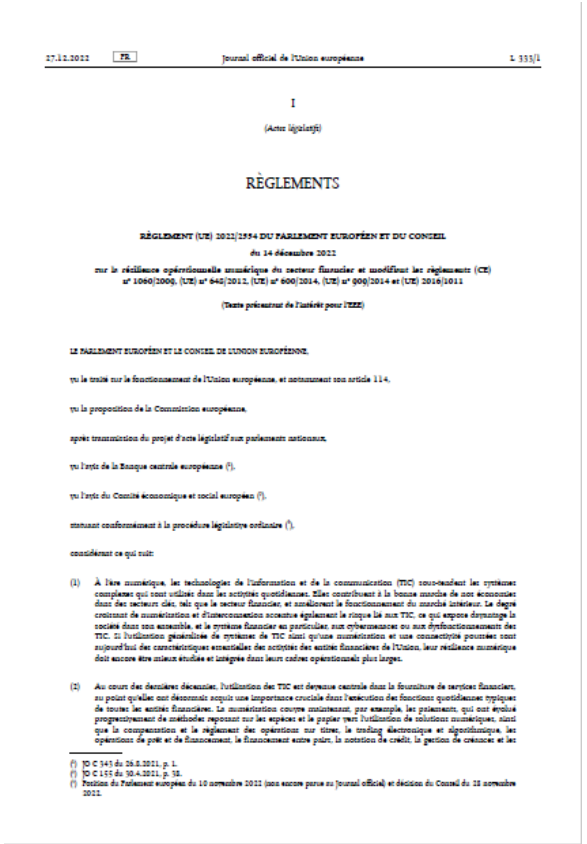
3. Prendre connaissance de l'esprit de **la doctrine de l'ANSSI**, pour estimer l'effort nécessaire à la future mise en conformité

- https://cyber.gouv.fr/
- Ex. guide d'admin, guide Linux, guide d'hygiène informatique, guide TPE/PME.

Quelques mots sur le règlement DORA

Une introduction aux enjeux cyber du règlement pour le secteur (1/2)

Illustration : 1ère page du règlement



27.12.2022 FR Journal officiel de l'Union européenne L 333/1

I

(Actes législatifs)

RÈGLEMENTS

RÈGLEMENT (UE) 2022/2554 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 14 décembre 2022

sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis de la Banque centrale européenne (1),

vu l'avis du Comité économique et social européen (2),

statuant conformément à la procédure législative ordinaire (3),

considérant ce qui suit:

(1) À l'ère numérique, les technologies de l'information et de la communication (TIC) sous-tendent les systèmes complexes qui sont utilisés dans les activités quotidiennes. Elles contribuent à la bonne marche de nos économies dans des secteurs clés, tels que le secteur financier, et améliorent le fonctionnement du marché intérieur. Le degré croissant de numérisation et d'interconnexion accentue également le risque lié aux TIC, ce qui expose davantage la société dans son ensemble, et le système financier en particulier, aux cybermenaces ou aux dysfonctionnements des TIC. Si l'utilisation généralisée de systèmes de TIC ainsi qu'une numérisation et une connectivité poussées sont aujourd'hui des caractéristiques essentielles des activités des entités financières de l'Union, leur résilience numérique doit encore être mieux étudiée et intégrée dans leurs cadres opérationnels plus larges.

(2) Au cours des dernières décennies, l'utilisation des TIC est devenue centrale dans la fourniture de services financiers, au point qu'elles ont désormais acquis une importance cruciale dans l'exécution des fonctions quotidiennes typiques de toutes les entités financières. La numérisation couvre notamment, par exemple, les paiements, qui ont évolué progressivement de méthodes reposant sur les espèces et le papier vers l'utilisation de solutions numériques, ainsi que la compensation et le règlement des opérations sur titres, le trading électronique et algorithmique, les opérations de prêt et de financement, le financement entre pairs, la notation de crédit, la gestion de créances et les

(1) JO C 343 du 26.8.2021, p. 1.
(2) JO C 155 du 30.4.2021, p. 38.
(3) Position du Parlement européen du 10 novembre 2022 (non encore parue au Journal officiel) et décision du Conseil du 28 novembre 2022.

Introduction

- Règlement applicable aux **entités financières** (EF, article 2) qui sera supervisé en France par l'ACPR, l'AMF, et la Banque de France
- Niveau 1 : dispositions de **gestion des risques liés aux TIC**, comprenant notamment i) des mesures générales destinées aux EF (chap. II), et des mesures spécifiques à la gestion des **prestataires tiers** (chap. V sec. 1)
- Niveau 2 : déclinaison en cours sous la forme de **RTS** (« Regulatory Technical Standards »)

Exemples de questions à se poser pour les membres du FRnOG

- Des services TIC sont-ils fournis à des EF ? Soutiennent-ils des fonctions considérées par les EF comme « critiques » ou « importantes » ?
- Si oui : se familiariser avec le texte, prendre connaissance des obligations portées par les EF, anticiper les évolutions dans la relation

Quelques mots sur le règlement DORA

Une introduction aux enjeux cyber du règlement pour le secteur (2/2)

Liens utiles

- Texte du règlement :
  - https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R2554
- Texte du projet de RTS JC 2023 86 (gestion des risques en général, 42 articles, 43 p.) :
  - https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_and_on_simplified_ICT_Risk_Management_Framework.pdf
- Texte du projet de RTS JC 2023 84 (sécurité des prestataires en particulier, 11 articles, 10 p.) :
  - https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_84_-_Final_report_on_draft_RTS_to_specify_the_policy_on_ICT_services_supporting_critical_or_important_functions.pdf

MERCI

RENDEZ-VOUS SUR LE SITE
MONESPACENIS2.CYBER.GOUV.FR

ÉCRIVEZ-NOUS À L'ADRESSE
RELATIONS_TELECOM_INFRANUM@SSI.GOUV.FR

Annexe 1

Glossaire

ACPR : Autorité de Contrôle Prudentiel et de Résolution

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

BITD : Base Industrielle et Technologique de Défense

BE : Bureau d'Enregistrement

CA : Chiffre d'Affaires

CE : Communications électroniques

DCP : Données à Caractère Personnel

DNS : Domain Name System

EdM : Etat de la Menace

EE : Entité Essentielle

EF : Entité Financière

EI : Entité Importante

EM-ET : état membre où une entité est établie

EM-EP : état membre où l'entité a son établissement principal

EM-SF : état(s) membre(s) où les services sont fournis

ETI : Entreprises de Taille Intermédiaire

ETP : Equivalent Temps Plein

EU-CyCLOne : European cyber crisis liaison organisation network

GC NIS : Groupe de Coopération NIS

MCS : Maintien en Conditions de Sécurité

MOA : Mode Opératoire d'Attaque

NDD : noms de domaine

NIS : Network and Information system Security

OSE : Opérateur de Services Essentiels

PME : Petites et Moyennes Entreprises

RAT : Remote Access Tool (i.e. outil d'accès à distance)

RTS : Regulatory Technical Standards

SIE : Système d'Information Essentiel

TIC : Technologies de l'Information et de la Communication

UE : Union Européenne

Annexe 2

Définitions issues de l'article 6 (1/2)

Concept	Définition
Point d'échange internet	Une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet, qui n'assure l'interconnexion que pour des systèmes autonomes et qui n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic.
Services DNS	Des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet; ou des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines.
Registres de NDD de premier niveau	Une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage.
Services d'informatique en nuage	Un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits.
Services de centres de données	Un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental.
Réseaux de diffusion de contenu	Un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services.

Annexe 2

Définitions issues de l'article 6 (2/2)

Concept	Définition
Services de confiance	Un service de confiance au sens de l'article 3, point 16 du règlement (UE) n°910/2014 dit « eIDAS », à savoir un service électronique normalement fourni contre rémunération qui consiste: • a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou • b) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou • c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services.
Réseaux de communications électroniques (CE) publics	Un réseau de communications électroniques public au sens de l'article 2, point 8), de la directive (UE) 2018/1972 établissant code des communications électroniques européen, à savoir un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau.
Services de CE accessibles au public	Un service de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972 établissant code des communications électroniques européen, à savoir le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus, comprend les types de services suivants : • a) un «service d'accès à l'internet» défini à l'article 2, deuxième alinéa, point 2, du règlement (UE) 2015/2120 (à savoir un service de communications électroniques accessible au public, qui fournit un accès à l'internet et, partant, une connectivité entre la quasi-totalité des points terminaux de l'internet, quels que soient la technologie de réseau ou les équipements terminaux utilisés) ; • b) un service de communications interpersonnelles ; et • c) des services consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion.
Services gérés	Services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance.
Services de sécurité gérés	Assistance pour des activités liées à la gestion des risques en matière de cybersécurité.

Annexe 3

Autres liens utiles

Liens

- Projet de règlement d'exécution, le référentiel européen qui sera *a priori* applicable à certains types d'entités du secteur :
  - https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en