INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INHESJ

TRAVAUX DES AUDITEURS

LA LOI DE PROGRAMMATION MILITAIRE APPLIQUÉE À LA CYBERSÉCURITÉ

Cycle « Sécurité des usages numériques »
Travaux de la 5e promotion (2014-2015)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

en partenariat avec le
cigref Réseau de Grandes Entreprises

JUILLET 2015
ISSN 2265-447X

Les **AUTEURS**

Les auteurs de ce travail intitulé : « **La Loi de Programmation Militaire appliquée à la Cybersécurité** » sont :

- **M. Gilles BERTHELOT,** Responsable de la sécurité des systèmes d'information, Réseau ferré de France
- **M. Juan-Carlos CERON ARANA,** Président, Createch sas
- **M. Bruno DELPHIN,** Responsable de la sécurité des systèmes d'information, Vetech (Veolia)
- **M. Bertrand de FOURNAS,** Responsable de la sûreté du patrimoine informationnel, Total
- **M. Ramesh PAVADEPOULLE,** Engagement manager, Dell

Sous la direction de **Nicolas Arpagian**, *directeur scientifique du cycle « Sécurité des usages numériques ».*

Directeur de la publication : M. Cyrille SCHOTT, directeur de l'INHESJ

LA LOI DE PROGRAMMATION MILITAIRE APPLIQUÉE À LA CYBERSÉCURITÉ

Travaux de la 5e promotion (2014-2015) du Cycle « Sécurité des usages numériques »

Sommaire

PRÉAMBULE 5

PRÉSENTATION ET ANALYSE DE LA LPM 6

CONTEXTE ET HISTORIQUE 6
FOCUS SUR LES ARTICLES AYANT UN IMPACT SUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION 8
LES OBJECTIFS, LES MOYENS ET LES ACTEURS 10
- Les objectifs 10
- Les moyens 11
- Les acteurs/périmètre 12

PÉRIMÈTRE D'APPLICATION DE LA LPM 13
- Synoptique général 13
- Notions d'organisation associées à la DNS et à la LPM 14
  - OIV 14
  - PIV 15
  - SIIV 15
  - Non OIV 16

ANALYSE DE LA MISE EN ŒUVRE DE LA LPM 17
- Défense de la Nation 17
- Soutenabilité de la LPM 17
- Planning de mise en œuvre 17

CONTEXTE EUROPÉEN 18
- Cybercriminalité et Conseil de l'Europe 18
- Cybercriminalité et Union européenne 19

DIRECTIVE NIS 20

LA LPM DÉCLINÉE DE MANIÈRE PRATIQUE 21
- Fiche Pratique et Plan Projet 21

ANALYSE DES IMPACTS DE LA LPM 24
- Les impacts légaux 25
- Les impacts organisationnels 26
- Les impacts technologiques 27
- Les impacts financiers 28

ANALYSE DES OPPORTUNITÉS, MENACES, FORCES ET FAIBLESSES 29
MISE EN ŒUVRE DES MESURES DE PROTECTION DES SIIV 31

LA LPM ET LE SECTEUR FRANÇAIS DE LA CYBER-SÉCURITÉ 32
SÉCURITÉ NATIONALE ET SOUVERAINETÉ 32
ANALYSE DES IMPACTS DE LA LPM SUR L'INDUSTRIE 32
Impacts organisationnels, technologiques, financiers 32
Impacts légaux..... 33
Une bulle économique ? 33

ACRONYMES ET GLOSSAIRE 34

ANNEXES 38
Annexe 1 : LE DISPOSITIF DNS 38
Annexe 2 : LPM – ARTICLE 20 40
Annexe 3 : LPM – ARTICLE 21 À 24 42
Annexe 4 : ARTICLE 20 - ANALYSE 48
Annexe 5 : DÉCRET RELATIF À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DES OIV. 49
Annexe 6 : DÉCRET RELATIF À LA QUALIFICATION DES PRODUITS ET PRESTATAIRES DE SERVICE DE CONFIANCE 56

PRÉAMBULE

Ce document a pour ambition de présenter les implications de la Loi de Programmation Militaire 2014-2019 pour son volet relatif à la Cybersécurité et en particulier pour les Opérateurs d'Importance Vitale.

Nous essayons de répondre aux questions que se pose un responsable. Comment ce sujet se situe dans le contexte réglementaire français et européen ? Quel est le contenu de la loi ? Quelles sont ses incidences, obligations ou contraintes pour les entreprises concernées ? Que faut-il faire pour se conformer à la loi ? Qu'est-ce qu'un système d'information d'importance vitale (SIIV) ? Qui sont les acteurs autour de ce sujet ?

Ce point de « l'état de l'art » est partiel ou temporaire car, d'une part, comme on le verra, une partie du volet réglementaire n'est, aujourd'hui, pas finalisé : les arrêtés sectoriels qui eux-mêmes sont porteurs des exigences ; d'autre part, aucune entreprise n'ayant encore mis en œuvre les règles et principes édictés par la loi, il n'est pas possible de s'appuyer sur un retour d'expérience.

Il convient donc de considérer ce document comme une version transitoire.

Attention : comme les éléments de mise en œuvre de la DNS dans l'entreprise, les informations relatives à la LPM font l'objet de restriction de diffusion.

Ainsi :

- **La liste des SIIV d'un OIV et les informations qui leurs sont rattachées, sont du niveau Confidentiel Défense.**
- **Les règles de sécurité LPM contenues dans les arrêtés sectoriels sont en Diffusion Restreinte.**

Leur contenu ne doit donc être diffusé qu'aux personnes habilitées.

PRÉSENTATION ET ANALYSE DE LA LPM

Contexte et historique

Le dispositif de sécurité des activités d'importance vitale (SAIV), inséré dans le Code de la défense, constitue l'un des fondements réglementaires permettant d'associer les opérateurs d'importance vitale (OIV) au système national de protection contre le terrorisme, le sabotage et les actes de malveillance.

Selon le Code de la défense (R1332-2), « *Un secteur d'activités d'importance vitale est constitué d'activités concourant à un même objectif. Ces activités soit ont trait, de manière difficilement substituable ou remplaçable, à la production et la distribution de biens ou de services indispensables, soit peuvent présenter un danger grave pour la population.*

Ces biens ou services doivent être indispensables :

- *à la satisfaction des besoins essentiels pour la vie des populations ;*
- *ou à l'exercice de l'autorité de l'État ;*
- *ou au fonctionnement de l'économie ;*
- *ou au maintien du potentiel de défense ;*
- *ou à la sécurité de la Nation* ».

La résilience de la Nation, définie comme étant « *La volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeures, puis rétablir rapidement leur capacité de fonctionner normalement* », a depuis longtemps été prise en compte par les autorités gouvernementales. Il existe donc tout un arsenal législatif et réglementaire encadrant et organisant ce dispositif :

- **La constitution de 1958** (*art. 5 : « ...fonctionnement régulier des pouvoirs publics ainsi que la continuité de l'État »*).
- **L'ordonnance n°58-1371** *du 29 décembre 1958 (les entreprises sensibles se doivent de coopérer à leur protection*).
- **L'ordonnance du 7 janvier 1959** (*art. 15 : « Chaque ministre est responsable des ...mesures de défense incombant au département dont il a la charge »*).
- **Le Code de la défense** (art. R.1332-1 définissant les OIV à R.1332-42 fixant l'obligation de contrôle des OIV).
- **Les directives nationales de sécurité (DNS)** en cours de révision par secteurs d'activité (voir annexe 1- DNS).

À la suite des attentats du 11 septembre 2001, la France a engagé une réflexion sur la notion d'infrastructure critique afin de moderniser la protection des points et des réseaux sensibles.

Cette réflexion a abouti au décret du 23 février 2006 relatif à la sécurité des activités d'importance vitale qui sont définies comme « *un ensemble d'activités, essentielles et difficilement substituables ou remplaçables, concourant à un même objectif ou visant à produire et à distribuer des biens ou des services indispensables* ».

Ainsi, les installations qui contribuent de façon essentielle à la préservation du potentiel de guerre et économique, de la sécurité et de la capacité de survie de la Nation, ou dont la destruction ou l'avarie peut présenter un danger grave pour la population, doivent être protégées contre toute menace, notamment à caractère terroriste.

- **Le Livre Blanc « défense et sécurité nationale »,** véritable analyse de risque de la Nation, fixe les grandes directions stratégiques de défense et de sécurité de la Nation. Initialement prévu sur des visions à 15 ans, l'accélération du monde et des menaces a nécessité de revoir le rythme de sa révision : 1994, 2008 puis plus récemment l'édition 2013 a permis d'adapter les priorités géostratégiques au nouvel environnement international. Il introduit notamment explicitement et pour la première fois la dimension des cyberattaques.

- **La loi de programmation militaire 2014-2019** s'appuie sur cette analyse de risques pour prioriser les actions et en planifier la mise en œuvre.

- **L'instruction générale interministérielle (IGI n°6600/SGDN/PSE/PSN) du 07 janvier 2014)** remplace celle du 26 septembre 2008. Elle constitue en quelque sorte le mode d'emploi de la mise en œuvre de ce dispositif. Elle apporte notamment des précisions sur les acteurs de la SAIV (instances nationales, ministre coordonnateur, instances territoriales, opérateurs d'importance vitale) et sur le dispositif (directive nationale de sécurité, plan de sécurité d'opérateur, point d'importance vitale, zone d'importance vitale...). Le texte détaille également le dispositif des audits internes des OIV et des contrôles administratifs et explicite l'articulation avec les autres plans et dispositifs réglementaires y compris à l'échelle européenne.

Cet arsenal de textes bien fourni est encore en pleine évolution tant à l'échelle nationale (arrêtés sectoriels LPM à paraître en 2015) qu'au-delà, car la protection des infrastructures vitales est traitée dans de nombreuses enceintes internationales telles que le G8, l'OTAN et surtout l'Union européenne (NIS - *Network and Information Security*). Les récentes affaires révélées au grand jour par « les lanceurs d'alertes » (*Snowden* ou *Wikileaks*) ont amené les autorités à réagir compte tenu des enjeux économiques et stratégiques sous-jacents et aussi face aux inquiétudes des citoyens sur la préservation des libertés individuelles.

Focus sur les articles ayant un impact sur la Sécurité des Systèmes d'Information

Cinq articles de la LPM 2014-2019 traitent de sujets cyber.

Tout d'abord, dans le **chapitre III : « Dispositions relatives au renseignement », l'article 20 relatif à « l'accès administratif aux données de connexion »** (*annexes 2 et 4*).

Puis les articles 21, 22, 23 et 24 qui font parties du **chapitre IV : « Dispositions relatives à la protection des infrastructures vitales contre la cybermenace »** (*annexe 3*) :

- **L'article 21 :** redéfinit les responsabilités et les actions possibles en matière de cybersécurité en modifiant le code de la défense.
- **L'article 22 :** désignation, responsabilités et obligations des OIV en termes de protection de leurs installations.
- **L'article 23 :** est relatif à l'utilisation non autorisée de dispositifs d'interception ou d'écoute par voie électronique.
- **L'article 24 :** est relatif à la protection et l'utilisation des données personnelles et de localisation.

Notre étude porte sur l'article 22.
Que dit l'article 22 ? En voici, un résumé.

Art 22 : responsabilités et obligations des OIV en termes de protection de leurs installations

Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, sont tenus de coopérer à leurs frais, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste.

Dans le cadre des dispositions spécifiques aux Systèmes d'information

Le Premier ministre fixe les **règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs** publics ou privés qui participent à ces systèmes.

Aux SI des OIV pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.

Aux SI des opérateurs publics et privés qui participent aux systèmes cités ci-dessus. Ces systèmes d'information sont appelés « systèmes d'information d'importance vitale » (SIIV).

Ces opérateurs sont tenus d'appliquer ces règles à leurs frais

Les règles peuvent notamment prescrire que les opérateurs mettent en œuvre des **systèmes qualifiés de détection des événements** susceptibles d'affecter la sécurité de leurs systèmes d'information. **Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information** ou par d'autres services de l'État désignés par le Premier ministre.

Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrées par le Premier ministre.

Les opérateurs (OIV) informent sans délai le Premier ministre des **incidents affectant le fonctionnement ou la sécurité** des systèmes d'information d'importance vitale (SIIV).

À la demande du Premier ministre, les opérateurs (OIV) **soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité**. Les contrôles sont effectués par l'autorité nationale de sécurité des systèmes d'information ou par des services de l'État désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier. **Le coût des contrôles est à la charge de l'opérateur**.

Pour répondre aux **crises majeures menaçant ou affectant la sécurité des systèmes d'information**, le Premier ministre peut décider des mesures que les opérateurs doivent mettre en œuvre.

L'État préserve la **confidentialité des informations qu'il recueille** auprès des opérateurs.

Dispositions pénales relatives aux manquements aux obligations d'OIV

La LPM reprécise que des sanctions sont prévues pour le non-respect des obligations qu'elle introduit.

Ainsi, pour rappel, est puni d'une **amende de 150 000 euros le fait, pour les dirigeants** des opérateurs et à l'expiration du délai défini par l'arrêté de mise en demeure, **d'omettre d'établir un plan de protection ou de réaliser les travaux prévus**.

Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, **d'entretenir en bon état les dispositifs de protection antérieurement établis**.

Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations prévues. Hormis le cas d'un manquement, cette sanction est précédée d'une mise en demeure. Les personnes morales déclarées responsables, dans les conditions prévues à l'article 121-2 du code pénal, des infractions prévues à la présente section encourent une

amende suivant les modalités prévues à l'article 131-38 du même code.

Le taux maximum de l'**amende applicable aux personnes morales est égal au quintuple** de celui prévu pour les personnes physiques par la loi qui réprime l'infraction.

Lorsqu'il s'agit d'un crime pour lequel aucune peine d'amende n'est prévue à l'encontre des personnes physiques, l'amende encourue par les personnes morales est de 1 000 000 euros.

Depuis le 27 mars 2015 deux décrets complètent la Loi :

- Décret n°2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense (*annexe 5*).
- Décret n°2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale (*annexe 6*).

Les objectifs, les moyens et les acteurs

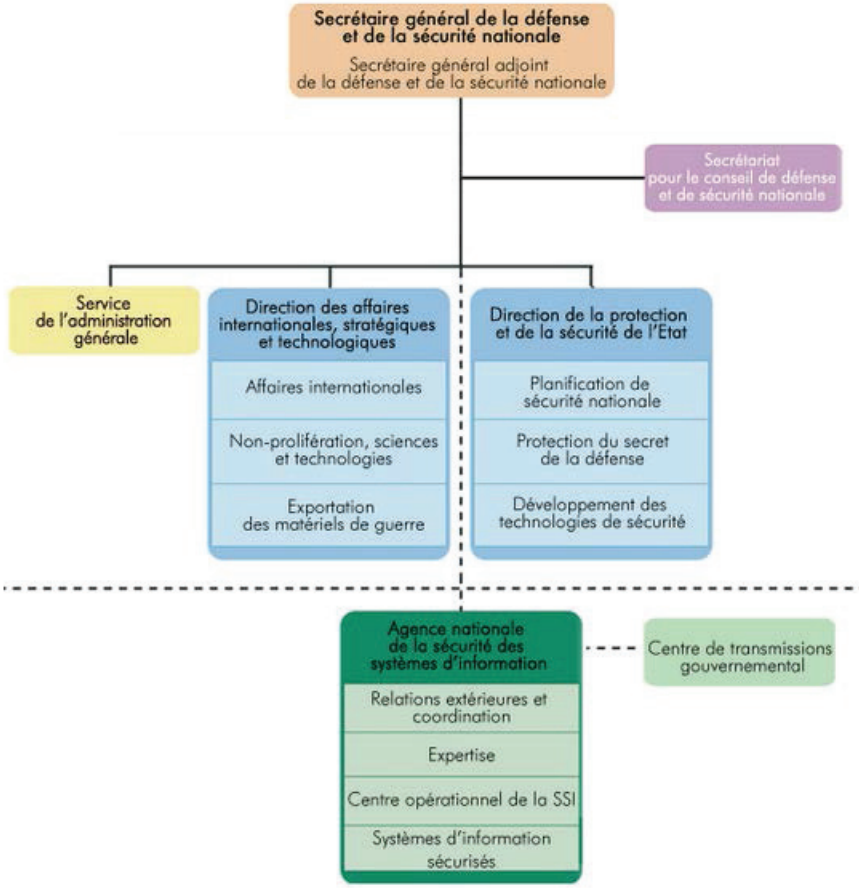
Les objectifs

L'objectif de la LPM est de suivre les lignes directrices et orientations exposées dans le Livre Blanc sur la défense et la sécurité nationale de 2013. Cette loi par son article 22 prévoit donc l'adoption de mesures de renforcement de la sécurité des Opérateurs d'Importance Vitale (OIV) et confère à l'ANSSI de nouvelles prérogatives. Ainsi :

- Obligation faite aux OIV et opérateurs publics ou privés, pour lesquels l'atteinte à la sécurité ou au fonctionnement de certains de leurs systèmes risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation de se conformer aux directives et règles de sécurité nécessaires à la protection des systèmes d'information essentiels fixées par le Premier ministre. Ces systèmes seront par la suite identifiés comme Système d'information d'importance vitale (SIIV).
- Obligation pour les OIV de mettre en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs SIIV.
- Notification sans délai par les OIV de tout incident de sécurité affectant le fonctionnement ou la sécurité des SIIV.
- Les OIV devront soumettre leurs Systèmes d'information d'importance vitale à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité prévues par la Loi.

Les moyens

Une organisation générique de défense a été mise en place par le Premier ministre, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) et de fait embrasse les nouveaux sujets liés à la Cyberdéfense.



Organigramme publié par le SGDSN

Parallèlement à l'organisation mise en place par le Premier ministre, dont l'ANSSI est l'acteur principal, le ministère de la Défense, à l'État-major des Armées, s'est dotée d'un Officier général à la cyberdéfense et le ministère de l'Intérieur à créer une fonction de Cyber-préfet.

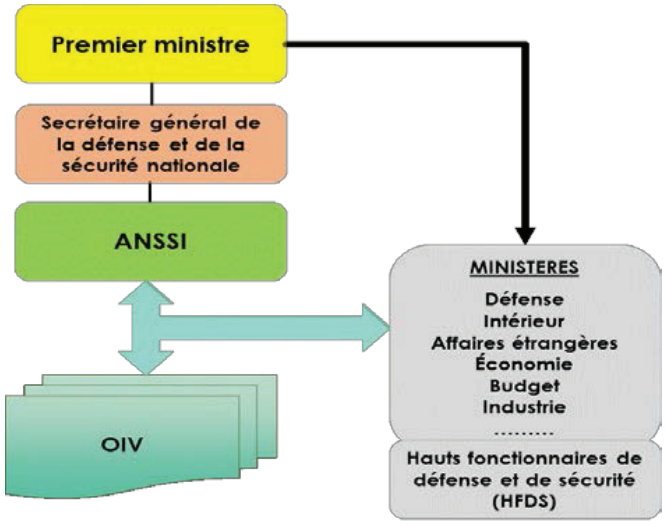
Ainsi est organisé le renforcement des capacités de l'État dans le domaine de la protection des SI, notamment au travers du recrutement de plusieurs centaines de spécialistes, de la mise en place d'une organisation et d'une chaîne opérationnelle centralisée et d'un effort important dans le cadre des études en amont, pour développer les instruments de pilotage de la cyberdéfense dont doit disposer le gouvernement et pour permettre une protection plus efficace des opérateurs d'importance vitale (OIV).

De plus, le Premier ministre pourra imposer aux opérateurs d'importance vitale des obligations en matière de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles de leur niveau de sécurité informatique ou de l'application des règles édictées. « *Des sanctions pénales (des amendes, des poursuites) sont prévues par le projet de loi en cas de non-respect de*

ces obligations ».

Les acteurs/périmètre

Les acteurs et le périmètre d'application proposés par la LPM sont représentés de façon globale dans le schéma ci-dessous :



Les premiers secteurs d'activité qui ont été répertoriés sont au nombre de douze. L'évolution de la loi pour 2015 est en train de faire évoluer ce premier recensement :

Secteurs étatiques :

- activités civiles de l'État ;
- activités militaires de l'État ;
- activités judiciaires ;
- espace et recherche.

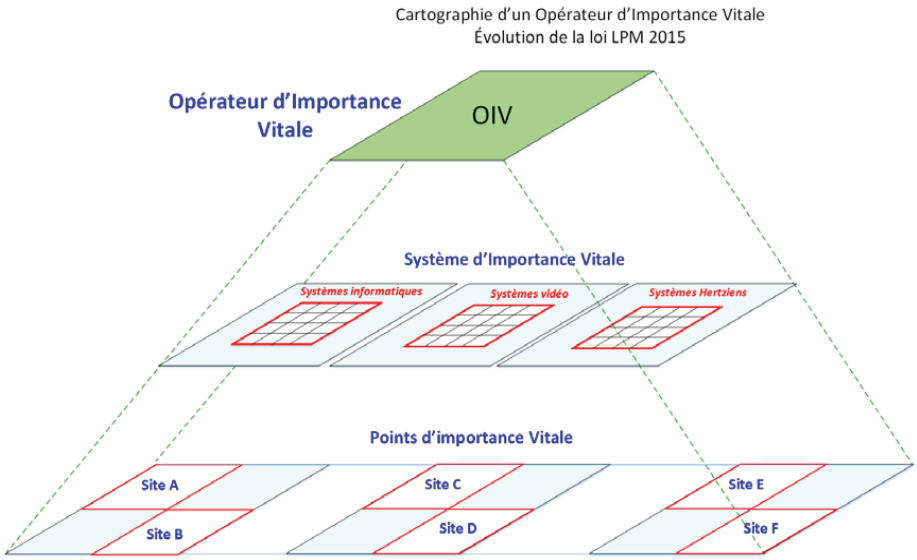
Secteurs de la protection des citoyens :

- santé ;
- gestion de l'eau ;
- alimentation.

Secteurs de la vie économique et sociale de la Nation :

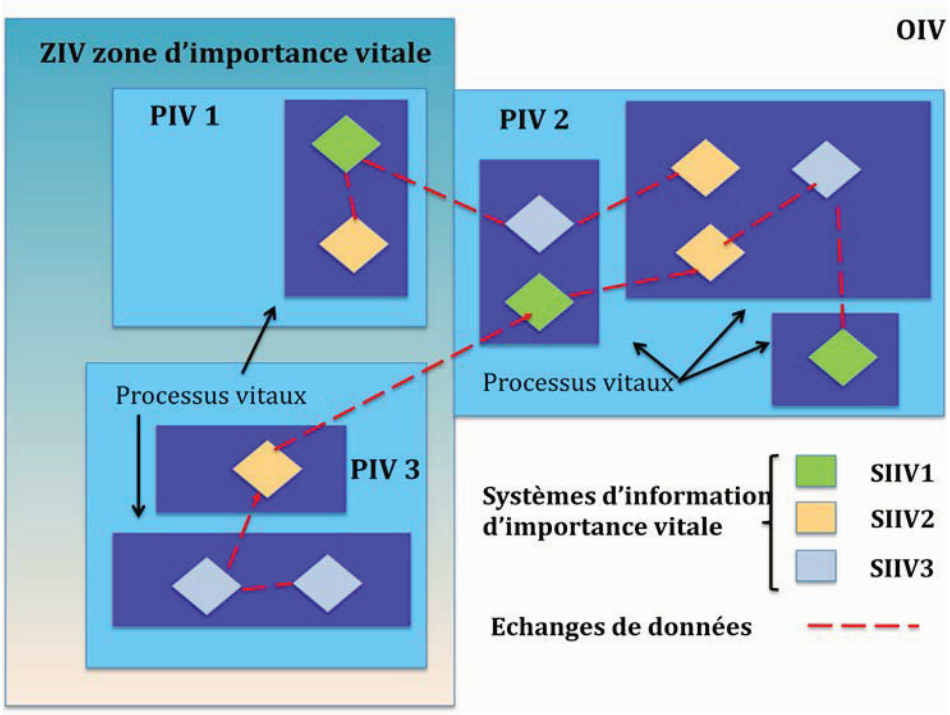
- énergie ;
- communications électroniques, audiovisuel et information ;
- transports ;
- finances ;
- industrie.

Le périmètre d'action de la loi est représenté par les notions d'OIV et SIIV (Système d'information d'importance vitale du point de vue d'un système informatique, système vidéo ou tout système de traitement des données).



Périmètre d'application de la LPM

Synoptique général



Un opérateur d'importance vitale (OIV) peut compter plusieurs Points d'importance vitale (PIV). Des Zones géographiques d'importances vitales (ZIV) comprennent des Points d'importances vitales (PIV).

Les Systèmes d'information d'importance vitale (SIIV) peuvent être situés sur des PIV mais cela n'est pas obligatoire : ils peuvent *a priori* être répartis sur plusieurs PIV, voire en dehors de tout PIV. Les SIIV sont d'ailleurs définis indépendamment de la notion de PIV.

Les organismes d'importance vitale auxquels la LPM impose des obligations sont parfois répartis sur plusieurs zones d'importance vitale.

Notions d'organisation associées à la DNS et à la LPM

Ces réglementations renvoient à des organisations et systèmes dont les principaux niveaux, utiles à la compréhension, sont décrits ici :

OIV

La LPM s'applique aux **Organismes d'importance vitale** (OIV) définis dans les articles **L1332-1 et 2 du Code de la défense**.

Article L1332-1

Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenues de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.

Article L1332-2

Les obligations prescrites par le présent chapitre peuvent être étendues à des établissements mentionnés à l'article L.511-1 du Code de l'environnement ou comprenant une installation nucléaire de base visée à l'article L.593-1 du Code de l'environnement quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population. Ces établissements sont désignés par l'autorité administrative.

- **Secteurs étatiques** : activités civiles de l'État ; activités militaires de l'État ; activités judiciaires ; espace et recherche.
- **Secteurs de la protection des citoyens** : santé ; gestion de l'eau ; alimentation.
- **Secteurs de la vie économique et sociale de la Nation** : énergie ; communication, électronique, audiovisuel et information ; transports ; finances ; industrie.

PIV

Les OIV mentionnés plus haut possèdent des **Points d'importance vitale** (PIV).

Un point d'importance vitale est un établissement, une installation ou un ouvrage *sis* sur le territoire national dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

- d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;
- ou de mettre gravement en cause la santé ou la vie de la population.

Cette notion de PIV, élément essentiel de l'organisation de la DNS, puisque lié à l'organisation physique, ne l'est pas dans la LPM.

SIIV

Le **Système d'information d'importance vitale** est l'élément principal du dispositif défini par la LPM.

Les SIIV participent à un processus vital de l'opérateur. Un processus est appelé « processus vital » lorsqu'au moins une des activités le composant est nécessaire à la réalisation d'une des missions vitales notifiées à l'opérateur. Cette notion de processus vital n'est pas un élément identifié dans la DNS ni dans la LPM. Elle a été rajoutée dans un but d'explication.

Un système d'information d'importance vitale est un SI « *pour lequel l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique ou la capacité de survie de la Nation* » (*cf. article L.1332-6-1 du Code de la défense nationale*), ainsi que les SI pour lesquels l'atteinte à la sécurité « *pourrait présenter un danger grave pour la population* » (*cf. article L.1332-2 du Code de la défense national*).

Seront définis comme SIIV parmi les SI ceux qui supportent les processus vitaux, ceux pour lesquelles une atteinte à la disponibilité, à la confidentialité ou à l'intégrité pourrait avoir un impact important pour l'OIV (le niveau d'impact étant défini par l'OIV).

Sont aussi à considérer comme SIIV, les SI dont le dysfonctionnement au-delà d'une certaine période :

- conduit l'opérateur à ne plus pouvoir satisfaire à des obligations définies avec leur modalité d'exécution, soit dans un contrat de service public, soit de façon légale ou réglementaire ;
- provoque des conséquences financières pouvant compromettre gravement la situation économique de l'opérateur et par voie de conséquence compromettre la réalisation des missions vitales qui lui ont été notifiées.

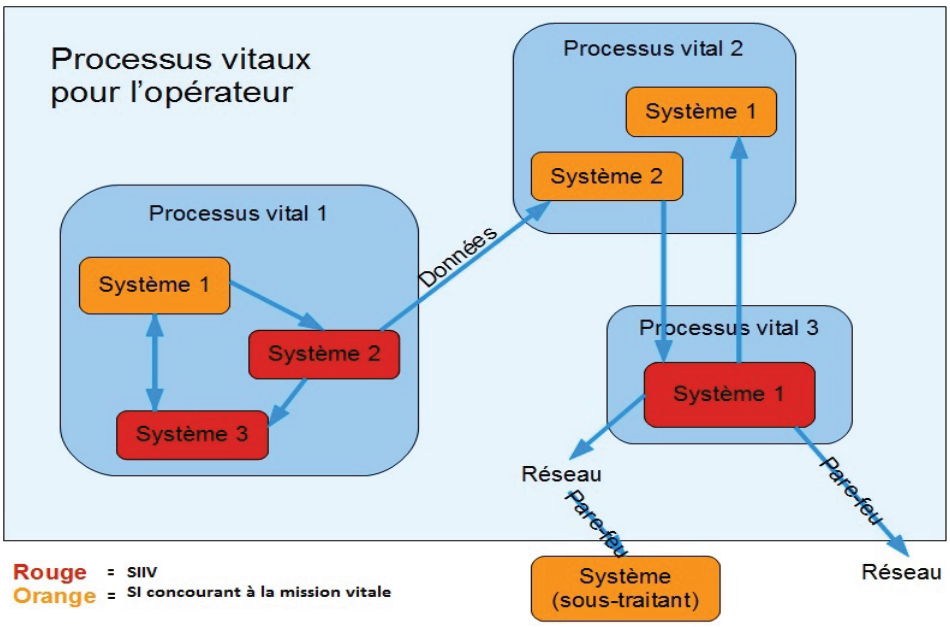
Le décret n°2015-351 du 27 mars 2015 prévoit que les OIV établissent la liste de leurs SIIV, sur la base de critères fixés dans les arrêtés sectoriels, et la transmettent à l'ANSSI. Ces listes ne feront pas l'objet d'une validation

formelle par l'État. Cependant, l'ANSSI pourra transmettre aux opérateurs des observations sur ces listes. Les opérateurs devront prendre en compte ces éventuelles observations en mettant à jour leur liste de SIIV.

Chaque arrêté sectoriel précisera, pour chaque secteur, une typologie de systèmes. Pour chacune des catégories de cette typologie, les opérateurs devront identifier les SIIV appartenant à cette catégorie.

Cette typologie ne sera ni limitante ni contraignante. Cependant, si aucun SIIV n'est identifié pour une catégorie donnée de la typologie, les opérateurs devront le justifier.

Certains ministères coordinateurs ont émis un guide pour la définition des Systèmes d'importance vitale à destination des opérateurs relevant de leur compétence.



Source : MEDDE

Non OIV

Les dispositions se cantonnent pour l'instant aux OIV*, entreprises ou administrations concourant à la survie de la Nation. Il faudra bien sûr sécuriser les autres entreprises (et leur imposer des mesures) en les identifiant par d'autres critères : celles qui emploient des personnels nombreux, celles qui traitent de secrets technologiques et industriels cruciaux… Mais, plus que d'assurer la survie de la Nation, il s'agira ici de protéger la compétitivité de ces entreprises, mais aussi l'emploi qu'elles génèrent. En effet, les entreprises françaises sont attaquées en permanence, espionnées et copiées, et ces attaques informatiques ont un impact direct sur leur compétitivité à l'échelle internationale.*

En attendant cet élargissement du champ d'application des textes actuellement en préparation à l'ensemble du tissu économique français, l'ANSSI espère que la première salve de mesures applicables aux OIV « fera tâche d'huile », et se répandra ainsi par des bonnes pratiques. De bonnes pratiques stimulées par la création d'un véritable marché de l'assurance aux cyber-risques, où la cybersécurité deviendra un enjeu de baisse à la prime incontournable.

Analyse de la mise en œuvre de la LPM

Défense de la Nation

La LPM dans son aspect cyber protection a bien pour objet la défense de la Nation et de la population. À savoir, en cas de cyber attaque, les Opérateurs d'importance vitale doivent être en mesure d'assurer le service qui est le leur, ou d'éviter une attaque dont les effets « catastrophiques » auraient un impact sur des populations environnantes. Pour cela, les Opérateurs protègeront et maintiendront les Systèmes d'information qui supportent ou participent à leur mission de service vitale.

Soutenabilité de la LPM

Une des clefs du succès de la mise en œuvre de l'article 22 de la LPM dans les entreprises, à commencer par les OIV, repose sur la soutenabilité financière, technique et organisationnelle des mesures et règles qui seront précisées dans les arrêtés sectoriels.

En d'autres termes, elles doivent être économiquement et organisationnellement supportables pour pouvoir être adoptées par les entreprises. En effet, il est rappelé dans la loi que les mesures seront à la charge des entreprises tant pour leur mise en œuvre que dans leur contrôle par les services de l'État.

Un certain nombre d'OIV sont déjà assujettis à des réglementations et donc à des obligations ou contraintes plus anciennes liées, par exemple, à l'industrie nucléaire, à l'industrie de l'armement, au secteur bancaire, etc. Souvent, les mesures prises pour se conformer à ces réglementations répondent aux exigences de la LPM. Les arrêtés sectoriels n'ajouteront pas une « surcouche » d'obligations si l'existant est considéré comme suffisant au regard des exigences de la LPM.

Planning de mise en œuvre

La LPM a été votée le 18 décembre 2013.

Les décrets d'application associés ont été signés le 27 mars 2015.

- Décret n°2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du Code de la défense (*annexe 5*).
- Décret n°2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale (*annexe 6*).

Les arrêtés sectoriels sont rédigés par l'ANSSI à l'issue de groupes de travail impliquant les OIV concernés, le ministère coordonnateur et l'ANSSI.

À compter de la publication de l'arrêté sectoriel, les entreprises OIV dudit secteur, sont soumises à :

- l'obligation de fournir la liste des SIIV dans un délai défini dans l'arrêté ;
- l'obligation de remonter les incidents affectant les SSIV avec effet immédiat ;
- la mise en œuvre des règles précisées dans l'arrêté dont le délai de mise en place sera spécifié dans l'arrêté pour chaque règle de sécurité.

Le calendrier global est encore incertain, dépendant de l'avancement des travaux de déclinaison sectorielle en cours et de la publication des arrêtés sectoriels qui suivra.

Contexte européen

Cybercriminalité et Conseil de l'Europe

L'Europe a très tôt tenté d'appréhender ce sujet. Dès 2001, le Conseil de l'Europe a élaboré une Convention dédiée à la cybercriminalité. C'est la première fois qu'un traité à vocation internationale aborde de front les infractions liées à l'informatique et spécifiquement celles commises *via* Internet. Elle établit les règles de base concernant le déroulement des enquêtes sur les réseaux et instaure une procédure de coopération internationale. Elle énonce aussi une liste d'infractions informatiques scindée en quatre grandes catégories :

- les infractions informatiques (falsification et fraude informatiques) ;
- les infractions liées à l'atteinte à la propriété intellectuelle et aux droits connexes ;
- les infractions relatives aux contenus (actes de production, diffusion, possession de pornographie enfantine, etc.) ;
- les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes (accès illégal, interception illégale, atteinte à l'intégrité des données, etc.).

Enfin, elle détermine des règles concernant la compétence juridictionnelle : désormais chaque pays signataire est juridiquement compétent lorsque l'infraction est commise sur son territoire ou que l'un de ses ressortissants en est l'auteur lorsque l'infraction ne relève de la compétence territoriale d'aucun autre État. Le texte du Conseil de l'Europe est complété par un protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais des systèmes informatiques du 28 janvier 2003, ratifié par la France en même temps que la Convention, par la loi du 19 mai 2005.

Cette convention a finalement connu un rayonnement plus large que celui purement européen, avec notamment une adhésion puis une entrée en vigueur aux États-Unis, le 1er janvier 2007. Elle témoigne de la volonté fédérative des

États de combattre la criminalité en ligne, même s'il convient de remarquer qu'une majorité d'entre eux reste, à l'échelle planétaire, à l'écart de cette convention.

Cybercriminalité et Union européenne

L'Union européenne – à distinguer du Conseil de l'Europe – a, quant à elle, abondé dans le sens de la présidence française. Cette dernière souhaitait mettre en place une plateforme européenne de lutte contre la cybercriminalité, hébergée par EUROPOL et capable de traiter le signalement des infractions commises *via* Internet, y compris en matière de pédopornographie. Le Conseil Justice et affaires intérieures, réuni à Bruxelles les 24 et 25 juillet 2008, a rapidement validé la proposition française. Ce n'est que près de quatre ans plus tard que la Commission européenne a décidé de relancer le projet tout en l'étayant. En effet, le 28 mars 2012, elle proposa d'ériger un Centre européen de lutte contre la cybercriminalité, rattaché à EUROPOL, et véritable centre névralgique de la lutte contre la criminalité en ligne au sein de l'Union européenne.

Ce Centre européen de lutte contre la cybercriminalité (EC3) a finalement vu le jour le 11 janvier 2013. Basé à La-Haye aux Pays-Bas et rattaché à EUROPOL, il est depuis cette date opérationnel. Parmi ses missions, il a en charge le soutien des enquêtes criminelles au niveau de l'Union européenne en assurant une coordination optimale des différents services de police et des différentes instances judiciaires. Notamment, il se concentre sur les activités illicites en ligne menées par des organisations criminelles, spécifiquement sur les attaques dirigées contre les services de banque en ligne ou d'autres activités financières en ligne, l'exploitation sexuelle en ligne des enfants et la criminalité touchant aux infrastructures critiques et aux systèmes d'information de l'Union. Il est aussi chargé du recueil des données relatives à la cybercriminalité, données qui permettront ultérieurement l'élaboration de rapports d'évaluation ou d'anticipation des menaces. Enfin, un service d'assistance (« *help desk* ») est mis en place par cette nouvelle institution, dont l'objet est la mise à disposition des unités répressives des États membres de toutes les données collectées afférentes à la cybercriminalité.

En sus de la création de ce nouveau centre, l'Union européenne a réitéré, dans une communication en date du 7 février 2013, sa volonté de combattre la criminalité sur les réseaux. L'objectif de ce nouveau « plan cybersécurité » est d'aboutir à « un cyberespace ouvert, sûr et sécurisé » respectueux des droits fondamentaux de chacun. De ce fait, l'Union européenne s'assigne cinq objectifs à réaliser :

- parvenir à la cyber-résilience ;
- faire reculer considérablement la cybercriminalité ;
- développer une politique et des moyens de cyberdéfense en liaison avec la politique de sécurité et de défense commune (PSDC) ;
- développer les ressources industrielles et technologiques en matière de cybersécurité ;
- instaurer une politique internationale de l'Union européenne cohérente en

matière de cyberespace et promouvoir les valeurs essentielles de l'UE.

Nul ne doute que la réalisation de ces objectifs se fera en étroite collaboration avec le très récent Centre européen de lutte contre la cybercriminalité.

Ce Centre constitue une réelle avancée dans le domaine de la criminalité en ligne car il dote l'Union de réels pouvoirs pour lutter efficacement contre les actes illicites dématérialisés. Néanmoins, Internet ayant par essence une vocation mondiale, ce projet apparaît quelque peu vain puisqu'il cantonne la lutte à une échelle exclusivement européenne. Cela est fortement dommageable lorsque l'on sait que les principales attaques informatiques proviennent de pays extérieurs à l'Union européenne et même, plus globalement, de l'Europe.

Directive NIS

La directive *Network and Information Security* (NIS), en cours de discussion au niveau européen, a notamment pour objectif d'imposer aux États membres des obligations similaires en matière de protection de leurs systèmes d'information. La directive prévoit à cet égard que :

- les opérateurs qui seront soumis à ces obligations soient désignés par chaque État membre ;
- les règles de sécurité s'appliquant à ces opérateurs soient définies par chaque État ;
- les opérateurs doivent notifier les incidents à leur autorité nationale compétente.

LA LPM DÉCLINÉE DE MANIÈRE PRATIQUE

Fiche pratique et Plan projet

Ce chapitre a pour ambition de donner les grandes lignes que pourrait suivre un OIV qui doit se mettre en adéquation avec les attentes formulées par la LPM.

Une fois identifiés les différents éléments, processus vitaux et SIIV définis dans les précédents chapitres (les PIV sont déjà connus, ayant été définis dans le cadre de la mise en œuvre de la DNS), il convient de balayer les règles énoncées par la LPM et son décret d'application, sur le périmètre concerné.

Pour chacune d'entre elles, il conviendra de trouver une implémentation qui ait du sens dans le contexte et qui soit réalisable aussi bien d'un point de vue organisationnel que financier ou technique.

Attention : les règles de sécurité LPM sont en Diffusion Restreinte. Leur contenu ne peut donc pas être diffusé largement.
***In fine*, les arrêtés sectoriels ne seront pas publiés et seront également en Diffusion Restreinte.**
Un espace dédié à la LPM, qui présentera les objectifs de chaque règle et fournira pour chaque règle un lien vers un guide de mise en œuvre, sera publié sur le site de l'ANSSI lors de la sortie du premier arrêté sectoriel.

Ci-dessous les 15 règles (○) réparties en 5 thématiques (●) et, pour chacune d'entre elles, des exemples de projet ou d'implémentation possibles (en bleu) qui pourront être déclinés .

● PILOTAGE DE LA GOUVERNANCE DE LA CYBERSÉCURITÉ

○ Rôles et responsabilité

- Impliquer les porteurs de risques métier dans le comité stratégique.
- Identifier les rôles manquants dans la gestion des SIIV et définir les objectifs de la mission.
- Décliner sur le périmètre des SIIV les procédures et référentiels déjà en place sur le reste du périmètre des SI.

- **PSSI** (Politique de sécurité des SI)
  - Démontrer une stratégie interne de contrôle de la sécurité des SIIV.
- **Indicateurs**
  - Créer des indicateurs et des données d'inventaires pour chaque SIIV.
  - Transmettre annuellement les indicateurs de chaque SIIV à l'ANSSI.
- **Formation**
  - Mettre en place un programme de sensibilisation et formation à la cyber sécurité.
  - Formation certifiante ou spécialisée (au moins au niveau de l'entreprise) d'administrateur SIIV.
  - Démontrer un plan de formation/sensibilisation SSI au périmètre SIIV.

MAÎTRISE DES RISQUES

- **Homologation**
  - Adapter les processus existants et les procédures d'audit.
  - Revoir annuellement le processus d'homologation.
  - Faire homologuer chaque SIIV tous les 3 ans par un audit d'homologation classifié CD (audit d'architecture + audit de configuration + audit organisationnel et physique) avec plan d'action.

MAÎTRISE DES SYSTÈMES D'INFORMATION

- **Cartographie**
  - Cartographier ou mettre à jour la cartographie de chaque SIIV.
  - Intégrer très en amont dans la conception des systèmes (Cahier des charges) des exigences de cartographie.
  - Cartographier les processus vitaux (essentiels aux missions vitales) et leurs dépendances respectives.
  - Classifier les processus vitaux en correspondance avec ma classification ANSSI.
- **MCS** (Maintien en condition de sécurité)
  - Imposer la pratique de *patch management* et de maintien en condition de sécurité.
  - Démontrer une politique de suivi des vulnérabilités et de leur traitement (correctifs) pour tout élément hard ou soft d'un SIIV.

GESTION DES INCIDENTS DE CYBERSÉCURITÉ

- **Détection**
  - Définir d'une politique de détection et de réaction
  - Installer des sondes de détection d'éléments suspects du SI (fichiers, clés de registre, protocoles, record DNS, etc...).
  - Recourir à un prestataire de détection des incidents qualifié par l'ANSSI sur chaque interconnexion des SIIV.

- **Journalisation**
  - Intégrer très en amont dès la conception des exigences de journalisation.
  - Formaliser et communiquer les directives de journalisation.
  - Miettre en place une journalisation.
  - Démontrer une politique de journalisation (6 mois mini) sur services applicatifs, réseaux, système, équipements de sécurité, postes d'administration (et ingénieur/ maintenance pour les SI industriels).
  - Installer, paramétrer et personnaliser les outils d'analyse et de corrélation de journaux (SIEM).
- **Traitement**
  - Recourir à un prestataire de réponse aux incidents qualifié par l'ANSSI.
- **Points de contact avec l'ANSSI**
  - Identifier et communiquer les points de contact à l'ANSSI.
  - Fournir la cartographie (applications + réseaux + flux + filtrage des interconnexions + solutions d'administration + liste des comptes admin et à privilèges, adresse IP des sous réseaux) de chaque SIIV à l'ANSSI.
  - Mettre en place le dispositif de remontée d'alerte vers l'ANSSI.
- **Gestion de crise**
  - Adapter les cellules de crise, astreintes et procédures pour les décliner sur le périmètre industriel.
  - Tous les 2 ans, démontrer sa capacité à pouvoir activer les mesures de crise.

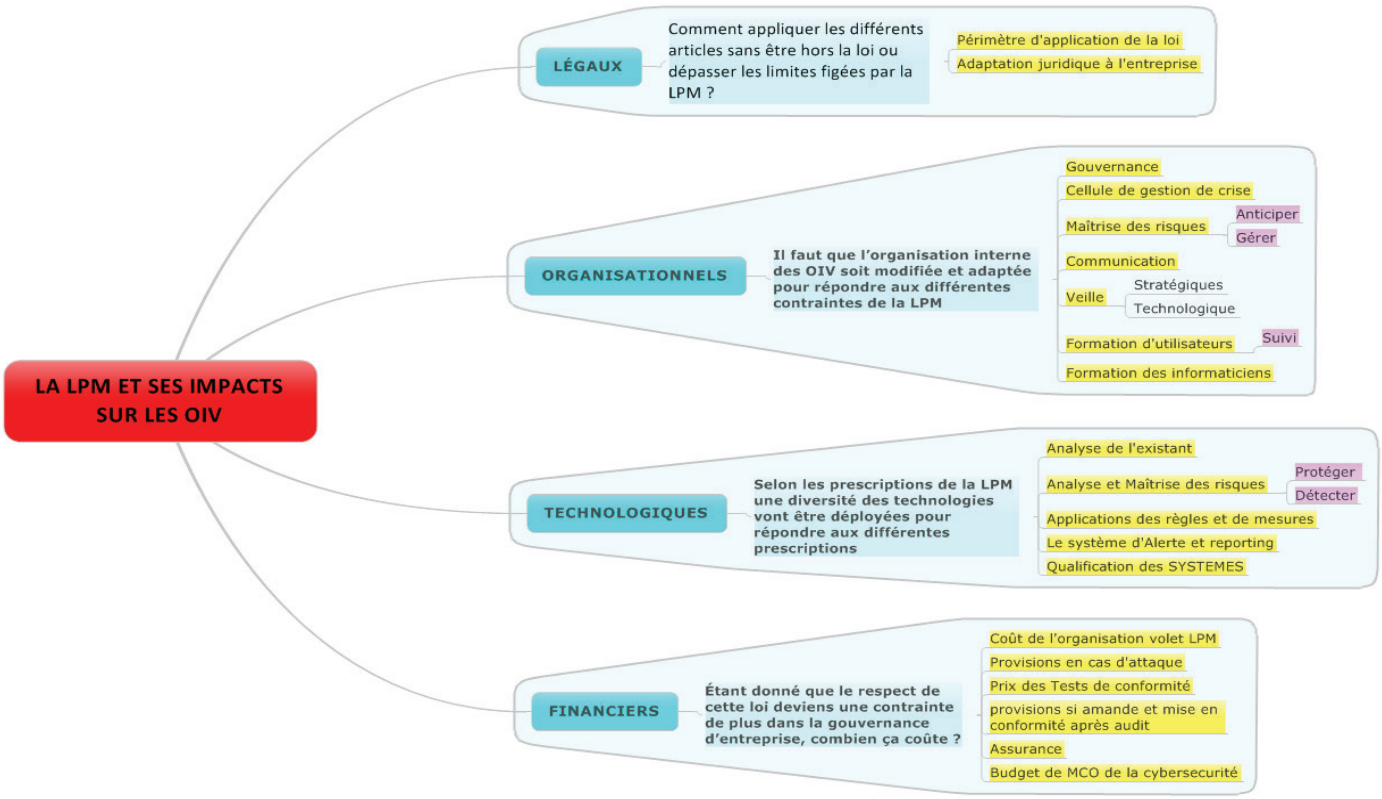
PROTECTION DES SYSTÈMES

- **Gestion des identités et des accès**
  - Identifier et valider les habilitations des personnes autorisées à accéder aux données confidentielles (ex. rapports d'audit, inventaires, etc.).
  - Créer un SI confidentiel défense afin de stocker les informations classifiées.
  - Mettre en place des infrastructures de contrôle d'accès et de gestion des habilitations.
- **Administration**
  - Formaliser une politique de gestion et de rationalisation des comptes à privilège.
  - Intégrer en amont à la conception des clauses de sécurité intégrant entre autre la gestion des comptes.
- **Défense en profondeur**
  - Durcir les accès d'administration, d'ingénierie/maintenance (pas d'Internet, de messagerie venant d'Internet, réseau dédié ou chiffré).
  - Mettre en place du cloisonnement *intra* SIIV.
  - Mettre en place 3 mesures de réaction (configuration spécifique, filtrage, isolement Internet).
  - Durcir les accès distants (hors opérateur ou prestataire qualifié SIIV) authentification, chiffrement des flux et des mémoires de masse.
  - Durcir les SIIV par la désactivation des services non nécessaires et un filtrage des média amovibles.

Analyse des impacts de la LPM

La Loi de Programmation Militaire va modifier structurellement les différents organismes de l'entreprise par sa mise en œuvre et par les divers impacts dans son fonctionnement, en particulier par les règles liées à la sécurité des systèmes d'information. Toutefois, si elle se veut efficiente, la sécurité ne doit pas uniquement être perçue comme un problème technique. C'est avant tout un problème de management et de gouvernance. Le fait de légiférer va obliger les OIV à réagir et à passer à une sécurité renforcée. La LPM permet effectivement de remettre à plat le sujet de la cybersécurité, mais aussi de légitimer le travail effectué par le DSI et les responsables sécurité auprès de leurs entreprises. La loi de programmation militaire aura des impacts à caractère :

- **Légal** : comment appliquer les différents articles sans être hors la loi, dépasser les limites fixées par la LPM ou simplement l'incompatibilité avec l'OIV (brevets par exemple ?.
- **Organisationnel** : il faut que l'organisation interne des OIV soit modifiée et adaptée pour répondre aux différentes contraintes de la LPM.
- **Technologique** : selon les directives de la LPM, une diversité des technologies va être déployée pour répondre aux différentes prescriptions, gestion du changement au niveau technique.
- **Financier** : la mise en œuvre a un coût associé aux modifications d'organisation, à la mise en place des nouveaux dispositifs techniques, leur exploitation, et leur contrôle.



Les impacts légaux

L'application légale de la LPM dans l'entreprise va modifier les différentes règles juridiques internes et externes de l'OIV. Ces changements en interne peuvent être :

- la politique de gestion des brevets ;
- le suivi de l'innovation ;
- la gestion comptable ;
- la gestion des ressources humaines ;
- le suivi financier ;
- la production ;
- l'ensemble du système d'information ;
- l'intervention d'un organisme extérieur certifié par l'ANSSI pour audit, control et arrêt de production si nécessaire ;
- etc.

En externe, ces changements vont être influencés par le respect des recommandations de la LPM avec :

- ses relations avec les partenaires commerciaux ;
- ses relations avec les prestataires de services ;
- ses clients ;
- etc.

La LPM, par définition, a une portée strictement nationale au sens territorial et, de fait, ne peut pas s'étendre au-delà des frontières. Ceci peut avoir une incidence sur certains SIIV qui peuvent être génériques pour une entreprise et donc s'étendre à d'autres pays.

De même, il est possible que l'administration de certains SIIV soit assuré par des équipes positionnées dans un autre état et de fait, l'opérateur ne répondrait plus à une des obligations : « ***Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'État désignés par le Premier ministre*** ».

Enfin, le point mentionné ci-dessus s'applique à des Opérateurs d'Importance Vitale qui ne sont pas nécessairement français. Il est possible que ceux-ci réfutent cette obligation de même que l'obligation : « ***les opérateurs (OIV) soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité prévues. Les contrôles sont effectués par l'Autorité nationale de sécurité des systèmes d'information ou par des services de l'État désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier*** ».

L'OIV est responsable légalement du non-respect de règles imposées par l'LPM. En général, la LPM change le périmètre juridique de l'OIV par l'adaptation de son système juridique dans le cadre de ses relations de gouvernance interne et externe.

Les impacts organisationnels

L'application de la LPM peut requérir une adaptation ou modification structurelle dans l'organisation de l'OIV.

Les impacts organisationnels dans l'OIV sont les suivants :

- **Gouvernance :** bien que ce point ne soit pas imposé par la LPM, il conviendrait de nommer un AQSSI : Autorité Qualifiée de Sécurité des Systèmes d'Information, dont le rôle de RSSI est complété par celui de contact officiel avec le ministère de coordination et l'ANSSI ou tout autre service de l'État. De plus, une modification de la chaîne interne de gestion des SIIV va s'imposer, en particulier du fait que « ***Les systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'Autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'État désignés par le Premier ministre*** ».

- **Maîtrise de risques et veille :** mise en place ou renforcement des moyens et des hommes nécessaires à la réalisation des différents *process* comme l'identification des menaces, l'analyse de risques, la cyber-intelligence pour anticiper et gérer les atteintes, compromissions ou attaques contre les SIIV et plus globalement le SI de l'OIV.

- **Gestion de crise :** mise en place d'un dispositif de gestion de cyber-crise qui permettra d'agir, de communiquer, de créer les liaisons opérationnelles avec l'ANSSI lors des cyber attaques qui s'imposent une intervention coordonnée.

- **Communication :** l'OIV par l'intermédiaire de l'AQSSI doit mettre en place un processus de communication et de remontée d'incidents vers l'ANSSI.

- **Plan de formation utilisateurs :** le RSSI propose des plans de formation et de sensibilisation à la sécurité des systèmes d'information en appliquant les diverses recommandations de l'ANSSI, en particulier sur les règles de l'arrêté sectoriel concernant son secteur d'activité.

  Un plan de suivi des utilisateurs est mis en place pour entretenir une base de connaissances d'amélioration des formations pour les utilisateurs.

- **Plan de formation des informaticiens, qualification et habilitation :** le RSSI, à l'aide du DSI, met en place un plan de formation à la sécurité des systèmes d'information. Il devient nécessaire de faire habiliter les personnels concernés car l'identification des processus vitaux, l'inventaire des SIIV sont des informations classifiées de niveau « confidentiel défense ». *A minima* cet obligation concerne l'AQSSI.

Les impacts technologiques

Les impacts technologiques de la LPM pour les OIV peuvent amener à une modification technique de son système d'information, laquelle est directement proportionnelle à celle de l'organisation.

Il faut commencer par l'analyse du système d'information existant et ses risques, grâce aux méthodes préconisées par l'ANSSI. Ces différentes actions permettront de proposer l'évolution des applications pour répondre aux règles de la LPM et ainsi de réaliser une qualification du système. Après la qualification du système existant, il restera à mettre en place des systèmes de techniques d'alerte et de suivi.

Les impacts technologiques pour l'OIV sont les suivants :

- **Analyse du système d'information d'importance Vitale :** après une identification des processus vitaux par et avec les métiers directement concernés, et l'établissement de l'inventaire des Systèmes d'Information d'Importance Vitale associés à ces processus vitaux, une expertise technique des SIIV existant doit être réalisée par la DSI et le RSSI. L'étude du système existant peut démontrer la non applicabilité des diverses exigences de la LPM, du fait, par exemple, de l'ancienneté des systèmes (un bon exemple est celui de la SNCF).

- **Analyse et maîtrise des risques :** le RSSI met en place un processus technique d'analyse des risques en utilisant les différentes méthodes proposées par l'ANSSI. (Défense en profondeur, MEHARI, EBIOS, etc.), résultat qui permettra de faire évoluer :
  - le système de protection (*Firewalls*, Antivirus, etc.) ;
  - la détection (sondes, *firewalls*, etc.)

- **Refonte et application des règles et mesures de la LPM :** grâce au résultat de l'analyse des risques et de l'étude de l'existant, le RSSI et le DSSI sont dans la capacité de proposer un plan technique de mise en œuvre des règles et mesures à respecter pour l'application de la LPM.

- **Le système d'alerte et *reporting* :** différents dispositifs d'alerte et d'intrusion peuvent être mis en place pour répondre aux règles et préconisations de la LPM, comme par exemple la mise en place de dispositifs de supervision de la sécurité (ex : SOCs, SIEMs, CERT, etc.).

  Cela permettra à l'OIV d'appliquer le processus de *reporting* unifié avec les différents organismes internes de l'entreprise (gouvernance) et avec l'ANSSI.

- **Qualification de la sécurité du système d'information :** un premier test de qualification et d'homologation doit être exécuté en interne pour vérifier la résilience et la réponse aux attaques du système mis en place. Lorsque le système a été testé et qualifié, une expertise extérieure permettra de valider la sécurité et la gestion de la crise en temps réel.

  Il faut prévoir pour un système jugé très critique l'interdiction de sa connexion sur Internet si nécessaire lors d'une attaque de grande ampleur (*Article 15 LPM*).

Les impacts financiers

La Loi de Programmation Militaire, dans son article 22, impose aux OIV la prise en charge financière des différentes modalités d'application de la loi dans sa mise en œuvre : « ***toutes les modifications de leurs systèmes d'information, les expertises et homologations sont à leur charge*** » et dans son contrôle : « ***Le coût des contrôles est à la charge de l'opérateur*** ».

Les principaux postes de coûts pour appliquer la loi correspondent aux investissements techniques nécessaires, aux coûts d'évolution de l'organisation, au budget de Maintien en Conditions Opérationnelles et le Maintien en Conditions de Sécurité, aux assurances (si elles existent), aux provisions financières en cas d'attaque et destruction des données, aux coûts associés aux tests de sécurité, aux provisions pour la non-conformité (amendes après audit).

Les impacts financiers pour l'application de la LPM sont les suivants (nous auront pu décrire les différents postes de dépenses, cependant, il n'est pas très réaliste de prévoir une enveloppe financière dû à l'hétérogénéité et la complexité des OIV) :

- **Le coût de l'organisation :** comme nous avons pu le constater dans les chapitres précédents, l'organisation de l'OIV doit s'adapter pour appliquer la LPM. L'organisation « LPM » peut devenir complexe pour l'OIV à cause du changement de son mode de fonctionnement. Le coût de l'organisation inclut, entre autres, le coût de l'audit du système existant, les coûts de la mise en place des nouveaux processus d'analyse des risques, la communication, la mise en place de la gestion de crise, les coûts des plans de formation, les coûts de la veille stratégique et technologique.

- **Le coût de la technique :** est un volet important, car après la mise en place de tous les processus organisationnels et d'expertise, il faut financer les modifications, les adaptations, les nouveaux systèmes de mesure, d'alerte, de sécurité (Maintien en Condition Opérationnel et le Maintien en Condition Sécurité) et de qualification pour répondre aux différents décrets de la LPM.

- **Le coût de la non-conformité :** Il convient aussi de prévoir les provisions en cas de cyber-attaque, les prix des tests de conformité après une attaque, les provisions à prévoir en cas d'amende de non-conformité ou de non-respect des dispositions de la LPM. Les assurances si elles existent.

Le coût le plus important après l'application des adaptations techniques est celui du Maintien en Condition Opérationnel.

Compte tenu des quelques cas de mise en œuvre des prescriptions de la LPM, le budget additionnel est environ de l'ordre de 5 % des coûts d'exploitation des infrastructures techniques (*backbone*) des entités porteuses de SIIV.

Analyse des opportunités, menaces, forces et faiblesses

La LPM apparaît clairement comme une opportunité et un levier fort d'amélioration de la Sécurité de l'information des entreprises OIV. Elle doit permettre de faire avancer les choses et de renforcer les démarches de sécurisation et de protection du patrimoine informationnel et des systèmes critiques de la Nation en impliquant les métiers au plus haut niveau. Entre les obligations légales et les sanctions prévues, les RSSI disposent, sur ce point particulier, d'un arsenal et d'arguments de poids pour obtenir les moyens et fédérer les énergies nécessaires à la mise en application opérationnelle de leur PSSI.

Comme l'histoire l'a montré, si les directions sont promptes à déprioriser des actions SSI, souvent considérées comme des projets lourds et des centres de coûts, quand apparaît le risque légal pour les dirigeants, l'arbitrage est moins facile et la sanctuarisation des moyens SSI est en général la sage décision. Reste que la rupture profonde marquée par ce texte engageant va nécessiter un accompagnement important dans les entreprises pour amener les métiers à s'approprier les sujets des risques SI jusqu'alors délégués un peu trop facilement. Toutes les organisations concernées ne sont pas au même niveau de maturité. Si pour les plus matures les facteurs de réussite sont importants, pour les autres, la marche à gravir risque d'être très (trop) haute tant en matière technique que de pratiques d'entreprises.

La résilience des infrastructures : une obligation

La continuité des services critiques de la Nation passe forcément par la refonte des infrastructures et socles techniques IT, qui, à ce jour, sont rarement en état de supporter la résilience exigée (vers des architectures SI sécurisées par *design*).

Les plans d'amélioration devront être déployés selon trois axes :

- les dispositions **prévention** visant à créer les conditions de conception des systèmes pour réduire la survenue du problème (respect des bonnes pratiques, protection des systèmes contre les malveillances, supervision des infrastructures,...) ;
- les dispositions de **prévision** visant à se doter et à positionner en anticipation des moyens propres à limiter les conséquences d'une attaque ou d'un sinistre (systèmes de détection, dispositif de retardement défense en profondeur, dispositifs de confinement) ;
- le dispositif de **réaction** visant à disposer des moyens et compétences pour mettre en œuvre les mesures de protection, qualifier, circonscrire et instruire les incidents SSI et éventuellement de gérer une crise SSI dans une approche transverse d'entreprise.

En premier lieu, l'existence d'un plan de continuité informatique n'est, dès lors, plus une option, au moins sur toutes les « poutres techniques » porteuses du SI : réseaux, *datacenter*, serveurs d'infrastructure (DNS, DHCP,...), systèmes d'accès (FW, VPN, IPS, IDS...), annuaires d'accès et d'habilitations au SI (AD, IAM,...).

Si le dispositif de continuité SI est nécessaire, il n'est bien sûr pas suffisant ! Le PCIT (plan de continuité informatique et télécoms) doit forcément être complété par l'organisation de la continuité d'activité des métiers qui devront commencer par identifier les impacts business (BIA) d'une indisponibilité des SI et définir les modes de travail et dispositions compensatrices adaptées et testées (procédures dégradées sans SI principal).

Si la LPM est une opportunité pour les OIV, elle présente aussi certains risques liés à l'ambition et la portée de la démarche, notamment pour les « stocks » de systèmes existants pas toujours en mesure de supporter simplement les évolutions demandées.

À ce stade, 4 risques majeurs d'applicabilité ont été identifiés :

- Risque sur les **délais de mise en œuvre des mesures** exigées par l'ANSSI qui pourraient être incompatibles avec les cycles de régénération des systèmes industriels des OIV.
- Risque de **soutenabilité de la démarche** compte tenu de la portée financière et organisationnelle de ces mesures à estimer (des coûts récurrents importants déjà identifiés).
- Risque sur l'**impossibilité technique à sécuriser** des systèmes existants trop obsolètes pour appliquer les règles ANSSI sans une réingénierie complète.
- Risque d'exploitation et de **maintien en condition de sécurité des systèmes dans la durée**. Les mesures techniques de maintien en condition de sécurité sont particulièrement contraignantes pour des systèmes informatiques industriels ayant une longévité difficilement compatibles avec l'évolution rapide des technologies informatiques et de télécommunication.

L'objectif des groupes de travail sectoriels mis en place par l'ANSSI est bien de prendre en compte ces quatre risques majeurs, afin d'écrire avec les OIV des règles soutenables et adaptées aux métiers des opérateurs et à leurs systèmes.

Dans la pratique, un projet de règles génériques est proposé par l'ANSSI aux opérateurs de chaque secteur et des réunions de travail permettent d'identifier les adaptations sectorielles nécessaires.

Mise en œuvre des mesures de protection des SIIV

Historiquement, le dispositif SAIV avait prévu dès le départ la notion de « point d'importance vitale » (PIV) des opérateurs et des plans de protection de ces PIV. En introduisant la notion de SIIV, le paradigme change un peu : la protection doit s'appliquer non plus à un point mais sur un système potentiellement diffus et éventuellement réparti. Cela nécessite une appréhension un peu différente de la conception des protections de ces composants.

Dans la démarche, les fondamentaux demeurent valides :

- **L'aspect protection physique** : les espaces hébergeant des centres névralgiques de SIIV devront, par héritage, bénéficier des mesures applicables au PIV. Cela veut dire sécurisation physique périmétrique anti intrusion, limitation et traçabilité des accès, protection électrique, climatique et redondance télécoms.
- **L'aspect protection Logique** : les systèmes logiques proprement dit devront *a minima* respecter les règles d'hygiène informatique de l'ANSSI. L'objectif est de protéger les informations (confidentialité et intégrité des données), de garantir la délivrance des services métiers (disponibilité, intégrité) et enfin de permettre une ségrégation stricte des rôles et des habilitations afin de garantir une imputabilité des actions réalisées sur les SIIV (traçabilité, non répudiation).
- **L'aspect RH** : il conviendra aussi de traiter la dimension humaine de la démarche en garantissant la probité et la fiabilité des personnes habilitées à intervenir avec des privilèges sur ces systèmes directement ou sur les couches d'infrastructures techniques qui les supportent (administrateurs des systèmes informatiques, développeur de solutions, infogérant des systèmes,...) et en traçant les actions réalisées sur les systèmes. De la même manière, les contrats de sous-traitance devront être bordés par des clauses spécifiques aux SIIV strictes dans les plans d'assurance sécurité. Le recours à des prestataires qualifiés de confiance sera également imposé.

LA LPM ET LE SECTEUR FRANÇAIS DE LA CYBER-SÉCURITÉ

Sécurité nationale et souveraineté

Par essence, cette loi a pour objet de participer à la sécurité nationale, dans ses aspects liés à la vie quotidienne de la Nation, à sa survie. Par ailleurs, sur ce petit périmètre de la cyber-sécurité, elle a pour ambition de mettre en place les conditions pour favoriser le développement ou le maintien d'un secteur industriel et de service indépendant de toute législation externe contraignante ou contraire à la souveraineté et à l'indépendance nationale.

Analyse des impacts de la LPM sur l'industrie

Dans sa présentation de l'article 22 de la LPM, le Directeur de l'ANSSI, ne cachait pas son vœu de voir sa mise en œuvre avoir des effets collatéraux à long terme. D'une part, sur l'extension du périmètre d'application des règles au-delà des SIIV identifiés dans l'entreprise, à une part plus large de ses SI, qui ne sont pas nécessairement qualifiés de Vitaux ou critiques, et ce, par la simple extension de la bonne pratique. D'autre part, favoriser le développement d'une industrie pérenne de solutions techniques et de services souverains dans le domaine de la cyber-sécurité.

Impacts organisationnels, technologiques, financiers

La mise en œuvre de l'article 22 de la LPM a pour objectif associé d'organiser l'industrie des services et des produits de sécurité par le simple fait d'appliquer le principe énoncé dans la loi : « *Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'Autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'État désignés par le Premier ministre.* »

On peut penser que, compte tenu de l'offre actuelle de solutions techniques dans l'ensemble du dispositif de protection des SIIV, apparaisse une règle qui impose l'insertion dans cette chaîne, d'au moins un élément de confiance souverain, ceci afin de créer un point de rupture. À titre d'exemple, si l'OS

de la machine, le routeur, l'administrateur du réseau sont de technologie(s) étrangère(s), ne convient-il pas que l'outil de chiffrement des données soit souverain ?

On verra alors un secteur d'offres qui trouvera un marché, mais celui-ci sera-t-il suffisant pour supporter l'activité pérenne d'*a minima* un fournisseur ?

Impacts légaux

La mise en œuvre de l'article 22 de la LPM dans les entreprises identifiées comme OIV aura des impacts légaux dont on ne mesure pas encore l'ampleur. À titre d'exemples :

- Comment s'organise l'entreprise pour se conformer à la certification « Confidentiel Défense » pour les acteurs du SI concernés ?
- Quelles sont les mesures contre les OIVs qui se refusent à appliquer les règles précisées dans l'arrêté d'application ?
- Quelles sont les mesures contre les OIVs qui ne respectent pas le calendrier de mise en œuvre des règles précisées dans l'arrêté d'application ?
- Quels sont les impacts pour les cyber-agresseurs d'un OIV ?
- Quelles sont les responsabilités de l'État dans la prise de décision d'isoler un système en cas d'agression externe ?
- De quels moyens juridiques et ou financiers l'État se dote-t-il pour s'assurer que les prestataires de service qualifiés en matière de sécurité de systèmes d'information ou fournisseurs de solutions techniques qualifiées ne passent pas sous le contrôle d'entreprise étrangère ?

Il faut savoir que l'OIV ne pourra pas avoir de recours juridique si l'un de ses employés lance une attaque délibérée contre un autre OIV et que les organismes d'État répondent à l'attaque en détruisant son système d'information.

Une bulle économique ?

Aujourd'hui, il est beaucoup trop tôt pour mesurer l'impact global sur l'écosystème de la cyber-sécurité française. En effet, d'autres éléments devraient être pris en considération : dans ses divers programmes économiques l'État veut-il s'engager à soutenir et développer ce secteur ?

Sous quelle forme ? En favorisant des petites structures, certes agiles mais fragiles ? Ou plutôt des gros porteurs, de type *Bull, Orange, Thales*, etc. ?

Il n'est pas possible de prédire si ce développement sera perceptible ou s'il transformera rapidement et durablement le visage de la cyber-industrie française. Une bonne partie de la réponse repose sur le volume des SIIV identifiés par les OIV. On le perçoit, la prise en charge par les industriels de l'intégralité des coûts de mise en place des règles et dispositifs associés à la LPM, y compris les audits de contrôle, incite ces industriels à la modestie dans l'identification et la déclaration des SIIV, donc réduit le marché.

ACRONYMES et GLOSSAIRE

ACRONYMES

ANSSI Agence nationale de sécurité des systèmes d'information
AME Activités militaires de l'État
AQSSI Autorité qualifiée pour la sécurité des systèmes d'information
ASS Aire spéciale de surveillance
BIA Bussines Impact Analysis
CEMA Chef d'État-major des armées
CERT Computer Emergency Response Team
CIDS Commission interministérielle de défense et de sécurité
CDAOA Commandement de la défense aérienne et des opérations aériennes
CZDS Commission zonale de défense et de sécurité
DDS Délégué pour la défense et la sécurité
DGA Direction générale de l'armement
DNS Directives nationales de sécurité
DOT Défense opérationnelle du territoire
DSI Direction/Directeur des systèmes d'information
DSSI Directeur de la sécurité des systèmes d'information
EBIOS Expression des besoins et Identification des objectifs de sécurité
EMIZDS État-major Interministériel de la zone de défense et de sécurité
EUROPOL Police européenne
FSD Fonctionnaire de sécurité de défense
FFDN Fédération de fournisseurs Internet
FSSI Fonctionnaire de sécurité des systèmes d'information FSSI. Service du HFDS
HFDS Haut fonctionnaire de défense et de sécurité
IAN Inspection des armements nucléaires
ICE Infrastructure critique européenne
ICPE Installation classée pour la protection de l'environnement
IDA Inspection des armées
IGI Instruction générale interministérielle
INB Installation nucléaire de base
INID Installations nucléaires intéressant la dissuasion
IPD Installation prioritaire de défense
MEHARI Méthode harmonisée d'analyse de risques
MSD Missions de sécurité et de défense
NIS Network and Information Security
OIV Opérateur d'importance vitale
PIV Point d'importance vitale
PSDC Politique de sécurité et de défense commune
PSO Plan de sécurité d'opérateur
PPE Plan de protection externe
PPP Plan particulier de protection
PSSI Politique de sécurité des systèmes d'information
RSSI Responsable de sécurité des systèmes d'Information
SAIV Sécurité des activités d'importance vitale
SGDSN Secrétariat général de la défense et de la sécurité nationale
SHFD Service du haut fonctionnaire de défense
SIC Standard Industrial Classification
SIEM Security Event Information Management (Management de la sécurité des événements de l'information)
SIIV Système d'information d'importance vitale
SOC Centre opérationnel de sécurité
ZIV Zone d'importance vitale

GLOSSAIRE

ACSSI (CD, SD); (DR, NP): Articles Contrôlés de la Sécurité des Systèmes d'Information, Classifiés (Confidentiel Défense, Secret Défense); (Diffusion Restreinte ou Non Protégé).

Aire Spéciale de Surveillance (ASS): aire géographique définie par le préfet autour d'un point estimé particulièrement sensible et dans laquelle s'exerce en permanence une recherche coordonnée du renseignement au profit des autorités responsables de la sécurité de l'installation.

Attractivité: attrait d'une cible pour un acte de malveillance ou de terrorisme, par suite des effets attendus sur les plans humain, économique, médiatique ou psychologique.

Composant névralgique: élément à la fois indispensable au fonctionnement d'une installation prioritaire de défense ou d'un point d'importance vitale et vulnérable, de niveau plus fin que ce point (salle de contrôle ou de commande,...).

DACSSI: Décision d'Accès aux Articles Contrôlés de la Sécurité des Systèmes d'Information.

Danger: toute situation, condition ou pratique qui comporte en elle-même une capacité à occasionner des dommages aux personnes, aux biens ou à l'environnement.

Défense dans la profondeur: la défense en profondeur consiste en la superposition de plusieurs lignes de défense, composées d'un ensemble de mesures de sécurité, chaque ligne devant contribuer à affaiblir l'attaque et à permettre aux suivantes de se renforcer en vue soit d'empêcher la destruction ou la prise de contrôle des composants névralgiques du PIV, soit d'en limiter les effets.

Directive nationale de sécurité (DNS): fondées sur une analyse de risque du secteur concerné en tenant compte des scénarios de menaces élaborés par le ministre coordonnateur, la ou les directives nationales de sécurité d'un secteur d'activité d'importance vitale précisent les objectifs et les politiques de sécurité du secteur ou d'une partie du secteur.

DSI: Direction/Directeur des Systèmes d'Information.

Établissement: unité géographique de production ou d'exploitation.

Exigences de sécurité: éléments requis pour atteindre les objectifs de sécurité, exprimés dans un ou plusieurs des cinq domaines que sont la planification, la sensibilisation, l'organisation, la prévention et la protection.

Faisabilité d'une action malveillante ou d'un acte de terrorisme: possibilité de conduire une telle action à partir de connaissances, de l'acquisition de moyens, de l'exploitation de vulnérabilités, de la capacité à accéder à la cible sans être détecté dans un délai qui rendrait l'action impossible.

Fonctionnaire de Sécurité de Défense (FSD): nommé par le Président, il a pour mission la protection du patrimoine scientifique et technique de l'établissement.

HFDS: Haut fonctionnaire de défense et de sécurité.

Infrastructure critique européenne (ICE): infrastructure critique située dans les États membres de l'Union européenne dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins.

Installation prioritaire de défense (IPD): installation autour de laquelle a été délimité par le président de la République en conseil de défense un secteur de sécurité et dont la sécurité doit être assurée en priorité et en tout temps. Une aire spéciale de surveillance (ASS) est par ailleurs définie par le préfet autour de chaque IPD (*cf. définition de l'ASS plus haut*).

Les autorités militaires auxquelles incombe l'exécution de la défense opérationnelle du territoire ont pour mission en tout temps, de participer à la protection des installations militaires et, en priorité, de celles de la force nucléaire stratégique4. Les IPD sont concernées par ces mesures.

Menace : tout événement physique, phénomène ou activité humaine potentiellement préjudiciable, susceptible de provoquer des décès ou des lésions corporelles, des dégâts matériels ou immatériels, des perturbations sociales et économiques ou une détérioration de l'environnement. Pour la démarche de sécurité des secteurs d'activités d'importance vitale, les menaces seront réputées avoir un caractère malveillant ou être de nature terroriste.

Mesures de sécurité : systèmes ou procédures identifiés pour répondre aux exigences de sécurité.

Ministre coordonnateur : le ministre coordonnateur d'un secteur d'activité d'importance vitale désigne les opérateurs d'importance vitale relevant du ou des secteurs d'activités dont il a la charge, élabore la ou les directives nationales de sécurité du ou de ces secteurs et notifie la liste des points d'importance vitale. Il est responsable de la coordination du secteur vis-à-vis des autres secteurs et, pour chaque secteur dont il est chargé, de la prise en compte des intérêts des autres ministères. Ce rôle ne lui donne toutefois aucune tutelle sur les opérateurs du secteur concerné par la directive nationale de sécurité qui relèvent d'autres ministères.

Objectif de sécurité : but à atteindre pour amener un risque identifié à un niveau acceptable, en agissant sur l'attractivité, la faisabilité, la vulnérabilité ou les impacts.

Ouvrage : construction.

Plan de sécurité d'opérateur (PSO) : plan définissant la politique générale de protection de l'ensemble des activités de l'opérateur, notamment celles organisées en réseau, comportant des mesures permanentes de protection et des mesures temporaires et graduées. Il n'est requis que si l'opérateur gère plusieurs points d'importance vitale.

Plan particulier de protection (PPP) : plan établi pour chaque point d'importance vitale à partir du plan de sécurité d'opérateur d'importance vitale, qui lui est annexé, et comportant des mesures permanentes de protection et des mesures temporaires et graduées.

Plan de protection externe (PPE) : plan établi pour chaque point d'importance vitale par le préfet de département en liaison avec le délégué de l'opérateur pour la défense et la sécurité de ce point, récapitulant les mesures planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics.

Point d'importance vitale (PIV) : tout établissement, installation ou ouvrage dont le dommage l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

- si son activité est difficilement substituable ou remplaçable, d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;
- ou de mettre gravement en cause la santé ou la vie de la population.

Risque encouru : appréciation combinée de la vraisemblance d'une agression réussie (résultant des scénarios de menace et de l'analyse des vulnérabilités) et de ses impacts.

Secteur d'activité d'importance vitale : secteur constitué d'activités concourant à un même objectif :

- qui ont trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, ou à l'exercice de l'autorité de l'État, ou au fonctionnement de l'économie, ou au maintien du potentiel de défense, ou à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables ;
- ou qui peuvent présenter un danger grave pour la population.

Sécurité des systèmes d'information (SSI) : la sécurité des systèmes d'information a pour objet de contrer ces menaces par des mesures proportionnées aux risques pouvant peser sur la confidentialité de l'information, son intégrité, sa disponibilité, la possibilité d'en authentifier la source et de la signer.

Système d'information (SI) : ensemble d'entités (logiciels, matériels, réseaux, locaux, organisation, personnels) organisé pour accomplir des fonctions de traitement d'informations.

Vulnérabilité : propension d'un milieu, d'un bien ou d'une personne à subir des conséquences dommageables à la suite d'un événement. Elle ne produit pas nécessairement de dommage par elle-même.

Zone d'importance vitale (ZIV) : zone géographique continue dans laquelle sont implantés plusieurs points d'importance vitale relevant d'opérateurs différents et interdépendants.

Zone protégée : zone créée par arrêté des ministres intéressés et faisant l'objet d'une interdiction d'accès sans autorisation, sanctionnée pénalement en cas d'infraction (articles 413-7 et R. 413-1 à R. 413-5 du code pénal).

DOCUMENTS

- INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE RELATIVE À LA SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE n°6600/SGDSN/PSE/PSN du 7 janvier 2014
- LPM
- IGI

ANNEXES

Annexe 1

LE DISPOSITIF DNS

Source : www.sgdsn.gouv.fr 02-2015

Douze secteurs d'activités d'importance vitale ont été définis dans un arrêté du 2 juin 2006, modifié par un arrêté du 3 juillet 2008.

Chaque secteur est **rattaché à un ministre coordonnateur** chargé du pilotage des travaux et des consultations interministérielles.

Il revient à **chaque opérateur d'identifier, dans son système de production, les composants névralgiques et de les proposer comme points d'importance vitale** devant faire l'objet d'une protection particulière.

Il dispose pour cela de la **directive nationale de sécurité du secteur dans lequel il exerce**. Ce document décrit les menaces, identifie les vulnérabilités génériques, fixe les exigences de protection et détermine les mesures graduées à mettre en œuvre en fonction de l'intensité de la menace, en cohérence avec le plan gouvernemental Vigipirate. 21 directives ont été approuvées par le Premier ministre. Elles spécifient les menaces à prendre en compte, les enjeux, les vulnérabilités et les objectifs de sécurité correspondants.

L'élaboration des directives nationales de sécurité et des documents méthodologiques a constitué une phase essentiellement conceptuelle. Lui succède actuellement la première mise en œuvre des directives.

150 opérateurs d'importance vitale ont été désignés dans sept secteurs dont l'alimentation, la gestion de l'eau, l'énergie, la santé et les transports. Ils ont commencé à élaborer leurs plans de sécurité.

L'opérateur conçoit un système de sécurité à deux étages : un plan de sécurité pour l'ensemble de ses activités relevant du ou des secteurs traités, et des plans particuliers de protection pour chacun de ses points d'importance vitale. Un guide méthodologique a été élaboré à cet effet.

Les 12 secteurs d'activité d'importance vitale sont :

Secteurs étatiques :
- activités civiles de l'État ;
- activités militaires de l'État ;
- activités judiciaires ;
- espace et recherche.

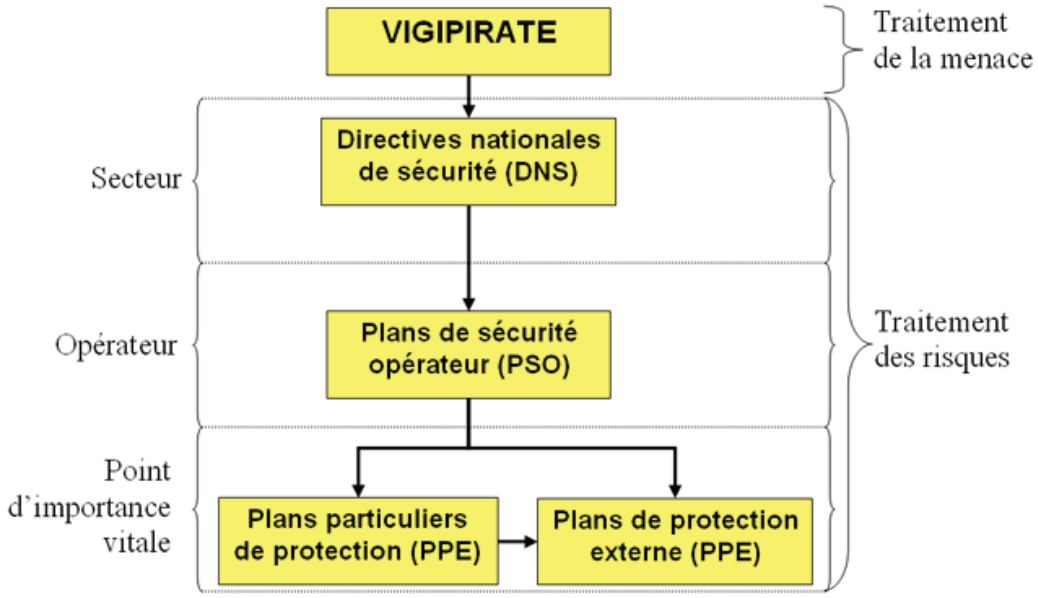
Secteurs de la protection des citoyens :
- santé ;
- gestion de l'eau ;
- alimentation.

Secteurs de la vie économique et sociale de la Nation :
- énergie ;
- communications électroniques, audiovisuel et information ;
- transports ;
- finances ;
- industrie.

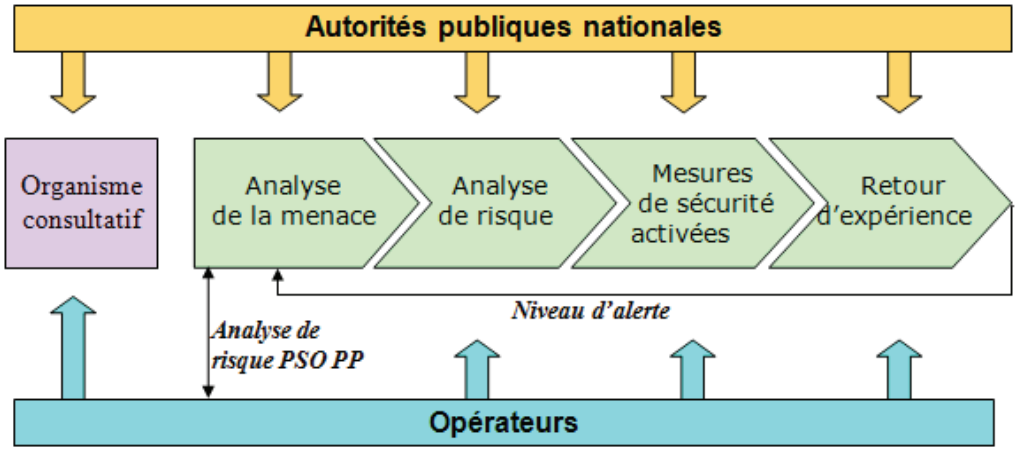
Les obligations des opérateurs d'importance vitale

- **Former leurs responsables** et leurs directeurs de la sécurité tant au niveau central qu'au niveau local.
- **Après une analyse de risques, établir un plan de sécurité opérateur (PSO)** prenant en compte les attendus de la directive nationale de sécurité au titre de laquelle ils ont été désignés opérateurs d'importance vitale.
- **Identifier leurs points d'importance vitale qui feront l'objet d'un plan particulier de protection (PPP)** à leur charge et d'un plan de protection externe (PPE) à la charge du préfet de département.

Dispositif SAIV



Organisation générale du décret de 2006 :



Annexe 2

ART 20 : ACCÈS ADMINISTRATIF AUX DONNÉES DE CONNEXION

Art. L.246-1 – Pour les finalités énumérées à l'article L.241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Art. L.246-2.-I. – Les informations ou documents mentionnés à l'article L.246-1 sont sollicités par les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L.241-2.

II. – Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité, sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Ces décisions, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

Art. L.246-3. – Pour les finalités énumérées à l'article L.241-2, les informations ou documents mentionnés à l'article L.246-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents mentionnés au I de l'article L.246-2.

L'autorisation de recueil de ces informations ou documents est accordée, sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie et du budget ou des personnes que chacun d'eux a spécialement désignées, par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de trente jours. Elle peut être renouvelée, dans les mêmes conditions de forme et de durée.

Elle est communiquée dans un délai de quarante-huit heures au président de la Commission nationale de contrôle des interceptions de sécurité.

Si celui-ci estime que la légalité de cette autorisation au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au deuxième alinéa.

Au cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.

Elle porte également cette recommandation à la connaissance du ministre ayant proposé le recueil de ces données et du ministre chargé des communications électroniques.

Art. L. 246-4. – La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil des informations ou documents mis en œuvre en vertu du présent chapitre, afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L.246-1 à L.246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté.

Les modalités d'application du présent article sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis.

Art. L. 246-5. – Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnées à l'article L. 246-1 pour répondre à ces demandes font l'objet d'une compensation financière de la part de l'État. » ;

3° Les articles L.222-2, L.222-3 et L.243-12 sont abrogés.

4° À la première phrase du premier alinéa de l'article L. 243-7, les mots : « *de l'article L.243-8 et au ministre de l'Intérieur en application de l'article L.34-1-1 du code des postes et des communications électroniques et de l'article 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » sont remplacés par les références : « des articles L.243-8, L.246-3 et L.246-4* ».

5° À l'article L.245-3, après le mot : « violation », sont insérées les références : « des articles L.246-1 à L.246-3 et ».

II. – L'article L.34-1-1 du code des postes et des communications électroniques est abrogé.

III. – Le II bis de l'article 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est abrogé.

IV. – Le présent article entre en vigueur le 1er janvier 2015.

.

Annexe 3

LPM – ARTICLE 21 À 24

• Chapitre IV : Dispositions relatives à la protection des infrastructures vitales contre la cybermenace

Art 21 : redéfinit les responsabilités et les actions possibles en matière de cyber sécurité en modifiant le code de la défense

• **Article L2321-2** Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 21

Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, **procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque**.

Pour être en mesure de répondre aux attaques mentionnées au premier alinéa, les services de l'État déterminés par le Premier ministre peuvent **détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du Code pénal, en vue d'analyser leur conception et d'observer leur fonctionnement**.

Art 22 : désignation, responsabilités et obligations des OIV en termes de protections de leurs installations

Dans le cadre des dispositions générales du Code de la défense:

Article L.1332-1

Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, sont tenues de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité administrative a été désignée par le décret n°2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L.1332-2

Les obligations prescrites par le présent chapitre peuvent être étendues à des établissements mentionnés à l'article L.511-1 du Code de l'environnement ou comprenant une installation nucléaire de base visée à l'article L.593-1 du Code de l'environnement quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population. Ces établissements sont désignés par l'autorité administrative.

Article L.1332-2-1

L'accès à tout ou partie des établissements, installations et ouvrages désignés en application du présent chapitre est autorisé par l'opérateur qui peut demander l'avis de l'autorité administrative compétente dans les conditions et selon les modalités définies par décret en Conseil d'État.

L'avis est rendu à la suite d'une enquête administrative qui peut donner lieu à la consultation du bulletin n°2 du casier judiciaire et de traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification.

La personne concernée est informée de l'enquête administrative dont elle fait l'objet.

Article L.1332-3

Les opérateurs dont un ou plusieurs établissements, installations et ouvrages sont désignés en application du présent chapitre réalisent pour chacun d'eux les mesures de protection prévues à un plan particulier de protection dressé par l'opérateur et approuvé par l'autorité administrative.

Ces mesures comportent notamment des dispositions efficaces de surveillance, d'alarme et de protection matérielle. En cas de non-approbation du plan et de désaccord persistant, la décision est prise par l'autorité administrative.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité administrative a été désignée par le décret n°2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L.1332-4

En cas de refus des opérateurs de préparer leur plan particulier de protection, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises assujettis en demeure de l'établir dans le délai qu'elle fixe.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité a été désignée par le décret n°2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L.1332-5

Le plan de protection établi dans les conditions prévues à l'article L.1332-4, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises en demeure de le réaliser dans le délai qu'elle fixe.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité a été désignée par le décret n°2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L.1332-6

Les arrêtés de mise en demeure prévus aux articles L.1332-4 et L.1332-5 fixent un délai qui ne peut être inférieur à un mois, et qui est déterminé en tenant compte des conditions de fonctionnement de l'opérateur et des travaux à exécuter.

Les arrêtés concernant les entreprises nationales ou faisant appel au concours financier de l'État sont transmis au ministre de tutelle et au ministre de l'économie et des finances, qui sont immédiatement informés des difficultés susceptibles de se produire dans l'application de l'arrêté.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité a été désignée par le décret n°2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Dans le cadre des dispositions spécifiques au Systèmes d'information

Article L.1332-6-1 Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22

Le Premier ministre fixe les **règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs** mentionnés aux articles L.1332-1 et L.1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. **Ces opérateurs sont tenus d'appliquer ces règles à leurs frais**.

Les règles mentionnées au premier alinéa peuvent notamment prescrire que les opérateurs mettent en œuvre des **systèmes qualifiés de détection des événements** susceptibles d'affecter la sécurité de leurs systèmes d'information. **Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information** ou par d'autres services de l'État désignés par le Premier ministre.

Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrées par le Premier ministre.

Article L.1332-6-2 Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22

Les opérateurs mentionnés aux articles L.1332-1 et L.1332-2 informent sans délai le Premier ministre des **incidents affectant le fonctionnement ou la sécurité** des systèmes d'information mentionnés au premier alinéa de l'article L.1332-6-1.

Article L.1332-6-3 Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22

À la demande du Premier ministre, les opérateurs mentionnés aux articles L.1332-1 et L.1332-2 **soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité** prévues à l'article L.1332-6-1. Les contrôles sont effectués par l'autorité nationale de sécurité des systèmes d'information ou par des services de l'État désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier. **Le coût des contrôles est à la charge de l'opérateur**.

Article L.1332-6-4 Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22

Pour répondre aux **crises majeures menaçant ou affectant la sécurité des systèmes d'information**, le Premier ministre peut décider des mesures que les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 doivent mettre en œuvre.

Article L.1332-6-5 Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22

L'État préserve la **confidentialité des informations qu'il recueille** auprès des opérateurs mentionnés aux articles L.1332-1 et L.1332-2 dans le cadre de l'application de la présente section.

Article L.1332-6-6 Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22

Un décret en Conseil d'État précise les conditions et limites dans lesquelles s'appliquent les dispositions de la présente section.

Dispositions pénales relatives aux manquements aux obligations d'OIV:

Article L.1332-7 Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 22

Est puni d'une **amende de 150000 euros le fait, pour les dirigeants** des opérateurs mentionnés à l'article L.1332-4 et à l'expiration du délai défini par l'arrêté de mise en demeure, **d'omettre d'établir un plan de protection ou de réaliser les travaux prévus**.

Est puni d'une amende de 150000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, **d'entretenir en bon état les dispositifs de protection antérieurement établis**.

Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations prévues aux articles L.1332-6-1 à L.1332-6-4. Hormis le cas d'un manquement à l'article L. 1332-6-2, cette sanction est précédée d'une mise en demeure.

Les personnes morales déclarées responsables, dans les conditions prévues à l'article 121-2 du code pénal, des infractions prévues à la présente section encourent une amende suivant les modalités prévues à l'article 131-38 du même code.

Article 131-38 Modifié par Loi n°2004-204 du 9 mars 2004 - art. 55 JORF 10 mars 2004

Le taux maximum de l'**amende applicable aux personnes morales est égal au quintuple** de celui prévu pour les personnes physiques par la loi qui réprime l'infraction.

Lorsqu'il s'agit d'un crime pour lequel aucune peine d'amende n'est prévue à l'encontre des personnes physiques, l'amende encourue par les personnes morales est de 1 000 000 euros.

Art 23 : relatif à l'utilisation non autorisée de dispositifs d'interception ou d'écoute par voie électronique

Article 226-15 Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 23

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.

Article 226-3 Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 23

Est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende :

1° La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du code de procédure pénale et figurant sur une liste dressée dans des conditions fixées par décret en Conseil d'État, lorsque ces faits sont commis, y compris par négligence, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par ce même décret ou sans respecter les conditions fixées par cette autorisation ;

2° Le fait de réaliser une publicité en faveur d'un appareil ou d'un dispositif technique susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 lorsque cette publicité constitue une incitation à commettre cette infraction ou ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du code de procédure pénale lorsque cette publicité constitue une incitation à en faire un usage frauduleux.

Art 24 : relatif à la protection et l'utilisation des données personnelles et de localisation

Article L.34-1 Modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 24

I. Le présent article s'applique au **traitement des données à caractère personnel** dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, **effacent ou rendent anonyme toute donnée relative au trafic**, sous réserve des dispositions des III, IV, V et VI. Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.
Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

III. Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il **peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques**. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs.

IV. Pour les **besoins de la facturation et du paiement** des prestations de communications électroniques, les opérateurs peuvent, **jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées** pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le VI, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés.
Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

V. Sans préjudice des dispositions du III et du IV et sous réserve des nécessités des enquêtes judiciaires, **les données permettant de localiser l'équipement** terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut

retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

VI. Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

Article L.2321-3 Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 24

Pour les besoins de la sécurité des systèmes d'information de l'État et des opérateurs mentionnés aux articles L.1332-1 et L.1332-2, les agents de l'autorité nationale de sécurité des systèmes d'information, **habilités par le Premier ministre et assermentés** dans des conditions fixées par décret en Conseil d'État, **peuvent obtenir des opérateurs** de communications électroniques, en application du III de l'article L.34-1 du code des postes et des communications électroniques, **l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système**.

Annexe 4

ARTICLE 20 - ANALYSE

C'est à la veille des fêtes de Noël 2014, qu'a été publié le très attendu décret d'application de l'article 20 de la loi de programmation militaire qui a fait polémique. Il précise donc les modalités d'application de cet article relatif à « ***l'accès administratif aux données de connexion*** ». Applicable depuis le 1er janvier 2015, son objectif est que les autorités publiques puissent avoir accès à tous les « documents » et « informations » stockés chez les hébergeurs ou transmis au travers des câbles des opérateurs télécoms, FAI, etc.

Pour cela, il suffit que les pouvoirs publics justifient de la recherche de renseignements intéressant notamment la sécurité nationale, la prévention du terrorisme, la criminalité et la délinquance organisées ou surtout de « la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », une notion assez floue. Les intermédiaires peuvent être tenus de transmettre « en temps réel » ces données recueillies après « sollicitation du réseau ».

Le texte, signé le 24 décembre, indique que le « groupement interministériel de contrôle », créé en 1960 et officialisé en 2002, placé auprès du Premier ministre, est le point pivot du dispositif sur un plan technique, puisqu'il reçoit les données fournies par les opérateurs et hébergeurs. Il travaille en lien direct avec la « personnalité qualifiée » chargée d'examiner puis de transmettre les demandes d'interception aux opérateurs ou aux hébergeurs, suite à la requête d'un service (section de recherches de la gendarmerie, service central du renseignement territorial,...).

Cette personnalité et ses adjoints seront désignés par la Commission nationale de contrôle des interceptions de sécurité sur proposition du Premier ministre – qui devra fournir une liste de plusieurs noms.

Le décret prévoit que chaque demande d'accès comporte obligatoirement :

- Le nom, le prénom et la qualité du demandeur ainsi que son service d'affectation et l'adresse de celui-ci.
- La nature précise des informations ou des documents dont le recueil est demandé et, le cas échéant, la période concernée.
- La date de la demande et sa motivation au regard des finalités mentionnées à l'article L.241-2 [prévention du terrorisme, etc.].
- L'autorisation formelle est prise « par décision écrite du Premier ministre ou des personnes spécialement désignées par lui », pour une durée maximale de 30 jours renouvelables.

Au travers de ce texte d'application, les « documents » et « informations » pouvant faire l'objet d'une demande d'accès sont ceux déjà mentionnés aux articles R10-13 et R10-14 du Code des postes et des communications électroniques, ainsi qu'à l'article 1er du décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

En pratique cela devrait concerner :

- Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication.
- Les données « permettant d'identifier le ou les destinataires d'une communication » électronique.
- Les données permettant d'identifier l'origine de la communication.
- L'identifiant de la connexion.
- Les dates et heures de début et de fin de la connexion.
- Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus.
- Les informations fournies lors de la souscription d'un contrat d'abonnement à Internet ou lors de la création d'un compte auprès d'un hébergeur : l'identifiant de la connexion utilisée pour la création du compte, les noms et prénoms, adresse postale, pseudonymes utilisés, adresse email, numéros de téléphone, « mot de passe ainsi que les données permettant de le vérifier ou de le modifier ».
- D'éventuelles informations relatives à un paiement : type, montant et référence du paiement, ou bien encore date et heure de la transaction.

Dés lors, les autorités ne pourront donc pas aller plus loin que ce que la loi leur permettait jusqu'ici.

La CNIL a ainsi salué ces dispositions qui « ne permettent en aucun cas de réaliser des interceptions de contenus ou des perquisitions en ligne et visent uniquement les données mentionnées aux articles R. 10-13 et R. 10-14 CPCE et 1er du décret du 25 février 2011 susvisé, à l'exclusion de toute autre information ».

Néanmoins, ce décret a peine publié vient, en février 2015, de faire l'objet d'un recours auprès du Conseil d'État par les fournisseurs d'accès associatifs de la fédération (FFDN) au titre de la neutralité d'Internet et sur la base de récentes décisions de la Cour de Justice de l'Union européenne (CJUE) sur le sujet... à suivre donc !

Annexe 5

DÉCRET RELATIF À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DES OIV

Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du Code de la défense

Publics concernés : opérateurs d'importance vitale mentionnés aux articles L.1332-1 et L.1332-2 du Code de la défense, services de l'État et prestataires de service mentionnés aux articles L.1332-6-1 et L.1332-6-3 du même code.

Objet : conditions et limites dans lesquelles s'appliquent les dispositions relatives à la sécurité des systèmes d'information des opérateurs d'importance vitale prévues aux articles L.1332-6-1 et suivants du code de la défense.

Entrée en vigueur : le décret est entré en vigueur le lendemain de sa publication.

Notice : le décret précise les conditions et limites dans lesquelles :

- sont fixées les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale ;
- sont mis en œuvre les systèmes de détection d'événements affectant la sécurité de ces systèmes d'information ;
- sont déclarés les incidents affectant la sécurité ou le fonctionnement de ces systèmes d'information ;
- sont contrôlés ces systèmes d'information ;
- sont qualifiés les systèmes de détection d'événements et les prestataires de service chargés de leur exploitation ou du contrôle des systèmes d'information ;
- sont proposées les mesures pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information.

Références : le Code de la défense, modifié par le présent décret, peut être consulté, dans sa rédaction issue de cette modification, sur le site Légifrance (http://www.legifrance.gouv.fr).

Le Premier ministre,

Vu le Code de la défense, notamment ses articles L.1332-1 et suivants, L.2321-1, R.*1132-3, R.1332-1 et suivants et R.2311-1 et suivants ;

Vu le Code pénal, notamment son article 413-9 ;

Vu le décret n°97-1184 du 19 décembre 1997 modifié pris pour l'application au Premier ministre du 1° de l'article 2 du décret n°97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n°2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;

Vu le décret n°2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale ;

Le Conseil d'État (section de l'administration) entendu,

Décrète :

Art. 1er. – Après la section 7 du chapitre II du titre III du livre III de la partie 1 du code de la défense (partie réglementaire), il est inséré une section 7 bis ainsi rédigée :

Dispositions spécifiques à la sécurité des systèmes d'information

Règles de sécurité

« **Art. R.1332-41-1.** – L'Agence nationale de la sécurité des systèmes d'information élabore et propose au Premier ministre les règles de sécurité prévues à l'article L.1332-6-1. Ces règles sont établies par arrêté du Premier ministre pris après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés. Lorsque l'arrêté n'est pas publié, il est notifié aux personnes ayant besoin d'en connaître.

« Les arrêtés mentionnés au premier alinéa peuvent prévoir des règles de sécurité différentes selon le secteur ou le type d'activité de l'opérateur. Ils fixent les délais dans lesquels les opérateurs d'importance vitale sont tenus d'appliquer les règles de sécurité. Ces délais peuvent être différents selon les règles de sécurité, le type de systèmes d'information concernés ou la date de mise en service de ces systèmes.

« **Art. R. 1332-41-2.** – Chaque opérateur d'importance vitale établit et tient à jour la liste des systèmes d'information mentionnés à l'article L.1332-6-1, y compris ceux des opérateurs tiers qui participent à ces systèmes, auxquels s'appliquent les règles de sécurité prévues au même article.

« Les systèmes d'information figurant sur la liste mentionnée au premier alinéa sont dénommés "systèmes d'information d'importance vitale".

« La liste est établie selon des modalités fixées par arrêté du Premier ministre pris après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés. Ces arrêtés peuvent prévoir des modalités différentes selon le secteur ou le type d'activité de l'opérateur. Lorsque l'arrêté n'est pas publié, il est notifié aux personnes ayant besoin d'en connaître.

« Chaque opérateur communique sa liste de systèmes d'information d'importance vitale et les mises à jour de celle-ci à l'Agence nationale de la sécurité des systèmes d'information selon des modalités et dans des délais fixés par l'arrêté mentionné au troisième alinéa.

« L'Agence nationale de la sécurité des systèmes d'information peut, après avis des ministres coordonnateurs concernés, faire des observations à l'opérateur sur sa liste. Dans ce cas, l'opérateur modifie sa liste conformément à ces observations et communique la liste modifiée à l'Agence nationale de la sécurité des systèmes d'information dans un délai de deux mois à compter de la réception des observations.

« La liste des systèmes d'information d'importance vitale est couverte par le secret de la défense nationale.

Détection des événements de sécurité

« **Art. R.1332-41-3.** – Les règles de sécurité prévues à l'article L.1332-6-1 fixent les conditions et les délais dans lesquels les opérateurs d'importance vitale mettent en œuvre des systèmes de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information d'importance vitale. Elles déterminent également le type de système de détection utilisé.

« **Art. R.1332-41-4.** – Lorsque l'opérateur d'importance vitale est une administration de l'État, le Premier ministre, après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés, décide, en fonction des risques particuliers encourus par les systèmes d'information en cause, si les systèmes de détection sont exploités par l'Agence nationale de la sécurité des systèmes d'information, par un autre service de l'État ou par un prestataire de service qualifié.

« Dans les autres cas, les systèmes de détection sont exploités exclusivement par un prestataire de service qualifié.

« Lorsque les systèmes de détection sont exploités par un prestataire de service qualifié, l'opérateur choisit le prestataire sur la liste prévue à l'article R.1332-41-9.

« **Art. R.1332-41-5.** – L'opérateur d'importance vitale conclut une convention avec le service de l'État ou le prestataire de service chargé d'exploiter les systèmes de détection. Cette convention précise :

« 1° Les systèmes d'information de l'opérateur qui font l'objet du service de détection ;

« 2° Les fonctionnalités du service de détection et le type de système de détection utilisé ;

« 3° Les systèmes de détection qualifiés utilisés et leurs modalités d'installation et d'exploitation par le service de l'État ou le prestataire ;

« 4° La nature des informations échangées entre l'opérateur et le service de l'État ou le prestataire, les conditions dans lesquelles elles sont utilisées et protégées ainsi que les moyens de communication sécurisés nécessaires à ces échanges ;

« 5° Les moyens techniques et humains nécessaires à l'opérateur pour la mise en œuvre du service de détection.

« La convention est conclue dans des délais compatibles avec ceux prévus pour la mise en service des systèmes de détection.

« Une copie de la convention signée est adressée sans délai par l'opérateur à l'Agence nationale de la sécurité des systèmes d'information.

« **Art. R.1332-41-6.** – Afin de rechercher et d'analyser des événements susceptibles d'affecter la sécurité des systèmes d'information d'importance vitale, l'Agence nationale de la sécurité des systèmes d'information peut demander aux services de l'État et aux prestataires de service chargés d'exploiter les systèmes de détection d'utiliser dans ces systèmes des données techniques qu'elle leur fournit.

« L'utilisation de ces données techniques est soumise à des conditions particulières définies par l'Agence nationale de la sécurité des systèmes d'information, en particulier lorsque les données sont couvertes par le secret de la défense nationale.

Qualification des systèmes de détection et des prestataires de service exploitant ces systèmes

« **Art. R. 1332-41-7.** – Les systèmes de détection et les prestataires de service mentionnés à l'article L. 1332-6-1 sont qualifiés dans les conditions prévues respectivement par les chapitres II et III du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

« **Art. R.1332-41-8.** – Un opérateur d'importance vitale peut agir comme prestataire de service exploitant des systèmes de détection au profit d'autres opérateurs d'importance vitale ou pour ses besoins propres sous réserve d'être qualifié dans les conditions prévues à l'article R.1332-41-7.

« **Art. R.1332-41-9.** – L'Agence nationale de la sécurité des systèmes d'information met à la disposition du public par voie électronique la liste des systèmes de détection et des prestataires de service exploitant ces systèmes, qualifiés dans les conditions prévues à l'article R.1332-41-7.

Déclaration des incidents de sécurité

« **Art. R.1332-41-10.** – En application de l'article L.1332-6-2, les opérateurs d'importance vitale communiquent à l'Agence nationale de la sécurité des systèmes d'information les informations relatives aux incidents affectant la sécurité ou le fonctionnement de leurs systèmes d'information d'importance vitale.

« Les opérateurs communiquent les informations dont ils disposent dès qu'ils ont connaissance d'un incident et les complètent au fur et à mesure de leur analyse de l'incident. Ils répondent aux demandes d'informations complémentaires de l'Agence nationale de la sécurité des systèmes d'information concernant l'incident.

« Le Premier ministre précise par arrêté, en distinguant le cas échéant selon le secteur ou le type d'activité de l'opérateur, les informations qui doivent être communiquées, les modalités de leur transmission ainsi que les types d'incident auxquels s'applique l'obligation prévue à l'article L.1332-6-2. Lorsque l'arrêté n'est pas publié, il est notifié aux personnes ayant besoin d'en connaître.

« **Art. R. 1332-41-11.** – L'Agence nationale de la sécurité des systèmes d'information transmet aux ministres coordonnateurs des secteurs d'activités d'importance vitale concernés, lorsque son analyse de l'incident le justifie, une synthèse des informations recueillies relatives à cet incident.

Contrôles de sécurité

« **Art. R.1332-41-12.** – Le Premier ministre, après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés, notifie aux opérateurs d'importance vitale sa décision d'imposer un contrôle prévu à l'article L.1332-6-3. Il précise les objectifs et le périmètre du contrôle et fixe le délai dans lequel le contrôle est réalisé. Il précise, en fonction de la nature des opérations à mener, si ce contrôle est effectué par l'Agence nationale de la sécurité des systèmes d'information, par un autre service de l'État ou par un prestataire de service qualifié. Dans ce dernier cas, l'opérateur choisit le prestataire sur la liste prévue à l'article R.1332-41-16.

« Le Premier ministre ne peut imposer à un opérateur plus d'un contrôle par année civile d'un même système d'information, sauf si les systèmes d'information de cet opérateur sont affectés par un incident de sécurité ou si des vulnérabilités ou des manquements aux règles de sécurité ont été constatés lors d'un contrôle précédent subi par l'opérateur.

« **Art. R.1332-41-13.** – L'opérateur d'importance vitale fournit au service de l'État ou au prestataire de service chargé du contrôle :

« 1° Les informations nécessaires pour évaluer la sécurité de ses systèmes d'information, notamment la documentation technique des équipements et des logiciels utilisés dans ses systèmes ainsi que les codes sources de ces logiciels ;

« 2° Les moyens nécessaires pour accéder à ses systèmes d'information et à l'ensemble de leurs composants afin de permettre au service de l'État ou au prestataire de réaliser des analyses sur les systèmes, notamment des relevés d'informations techniques.

« **Art. R.1332-41-14.** – L'opérateur d'importance vitale conclut une convention avec le service de l'État ou le prestataire de service chargé d'effectuer le contrôle. Cette convention précise :

« 1° Les systèmes d'information qui font l'objet du contrôle ;

« 2° Les objectifs et le périmètre du contrôle ;

« 3° Les modalités de déroulement du contrôle, notamment les conditions d'accès aux sites et aux systèmes d'information de l'opérateur ;

« 4° Les informations nécessaires à la réalisation du contrôle, fournies par l'opérateur, et les conditions de leur protection ;

« 5° Les modalités selon lesquelles sont effectuées les analyses techniques sur les systèmes d'information de l'opérateur.

« La convention est conclue dans des délais compatibles avec le délai fixé par le Premier ministre pour la réalisation du contrôle.

« Une copie de la convention signée est adressée sans délai par l'opérateur à l'Agence nationale de la sécurité des systèmes d'information.

« **Art. R.1332-41-15.** – Le service de l'État ou le prestataire ayant réalisé le contrôle rédige un rapport exposant ses constatations, au regard de l'objectif du contrôle, sur le niveau de sécurité des systèmes d'information contrôlés et le respect des règles de sécurité prévues à l'article L.1332-6-1. Les vulnérabilités et les manquements aux règles de sécurité constatés lors du contrôle sont indiqués dans le rapport, qui formule le cas échéant des recommandations pour y remédier. Le rapport est couvert par le secret de la défense nationale.

« Après avoir mis l'opérateur en mesure de faire valoir ses observations, le service de l'État ou le prestataire remet, dans le délai fixé pour la réalisation du contrôle, le rapport à l'Agence nationale de la sécurité des systèmes d'information.

« L'Agence nationale de la sécurité des systèmes d'information peut auditionner, dans un délai de deux mois à compter de la remise du rapport, le service de l'État ou le prestataire ayant réalisé le contrôle, le cas échéant en présence de l'opérateur, aux fins d'examiner les constatations et les recommandations figurant dans le rapport. Elle peut inviter les ministres coordonnateurs des secteurs d'activités d'importance vitale concernés à assister à cette audition.

« L'Agence nationale de la sécurité des systèmes d'information communique aux ministres coordonnateurs des secteurs d'activités d'importance vitale concernés les conclusions du contrôle.

« **Art. R.1332-41-16.** – Les prestataires de service mentionnés à l'article L.1332-6-3 sont qualifiés dans les conditions prévues par le chapitre III du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

« L'Agence nationale de la sécurité des systèmes d'information met à la disposition du public par voie électronique la liste des prestataires de service qualifiés mentionnés au premier alinéa.

« **Art. R. 1332-41-17.** – Le coût des contrôles effectués par un service de l'État en application de l'article L.1332-6-3 est calculé en fonction du temps nécessaire à la réalisation du contrôle et du nombre d'agents publics qui y participent. Un arrêté du Premier ministre fixe le coût d'un contrôle mobilisant un agent public pendant une journée.

« Le coût des contrôles effectués par un prestataire de service est déterminé librement par les parties.

Réponse aux crises majeures

« **Art. R.1332-41-18.** – L'Agence nationale de la sécurité des systèmes d'information propose au Premier ministre les mesures mentionnées à l'article L. 1332-6-4.

Dispositions diverses

« **Art. R.1332-41-19.** – Les opérateurs d'importance vitale prennent les mesures nécessaires, notamment par voie contractuelle, pour garantir l'application des dispositions prévues à la présente section aux systèmes d'information des opérateurs tiers mentionnés au premier alinéa de l'article R.1332-41-2.

« **Art. R.1332-41-20.** – Chaque opérateur d'importance vitale désigne une personne chargée de le représenter auprès de l'Agence nationale de la sécurité des systèmes d'information pour toutes les questions relatives à l'application des dispositions prévues à la présente section. Nul ne peut être désigné s'il n'est titulaire de l'habilitation mentionnée à l'article R.2311-7.

« **Art. R.1332-41-21.** – L'Agence nationale de la sécurité des systèmes d'information peut imposer aux opérateurs d'importance vitale et aux prestataires de service mentionnés aux articles L.1332-6-1 et L.1332-6-3 l'utilisation d'un moyen particulier pour protéger les échanges d'information prévus à la présente section lorsqu'ils sont effectués par voie électronique.

« **Art. R.1332-41-22.** – Les services de l'État et les prestataires de service mentionnés aux articles L.1332-6-1 et L.1332-6-3 accèdent aux systèmes d'information des opérateurs d'importance vitale et, le cas échéant, aux informations qu'ils contiennent dans le respect des secrets protégés par la loi.

« **Art. R.1332-41-23.** – Si un opérateur d'importance vitale ne satisfait pas aux obligations prévues aux articles L.1332-6-1 à L.1332-6-4, l'Agence nationale de la sécurité des systèmes d'information saisit l'autorité judiciaire aux fins de poursuite de l'auteur du délit prévu au troisième alinéa de l'article L.1332-7. Hormis le cas d'un manquement à l'article L.1332-6-2, cette saisine est précédée d'une mise en demeure adressée à l'opérateur par l'Agence nationale de la sécurité des systèmes d'information. »

Art. 2. – Le Code de la défense est également modifié comme suit :

I. – A l'article R.1332-10 :

1° La numérotation : « 7° » est remplacée par la numérotation : « 8° » ;

2° Après le 6°, il est inséré un 7° ainsi rédigé :

« 7° Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant ; ».

II. – A l'article R.1332-33, après les mots : « l'article R.1332-26 », sont insérés les mots : « ou de toute décision mentionnée à la section 7 bis du présent chapitre ».

Art. 3.

I. – Le second alinéa de l'article 1er du décret du 7 juillet 2009 susvisé est remplacé par un alinéa ainsi rédigé :

« L'Agence nationale de la sécurité des systèmes d'information est dirigée par un directeur général, qui a rang de directeur d'administration centrale. Le directeur général est compétent pour agir au nom de l'agence. Il a qualité pour signer les décisions relevant de la compétence de l'agence. Il peut donner délégation à son adjoint pour signer ces décisions, y compris celles relatives aux affaires pour lesquelles il a lui-même reçu délégation. »

II. – L'article 3 du décret du 7 juillet 2009 susvisé est modifié comme suit :

1° Au troisième alinéa, la deuxième phrase est remplacée par la phrase suivante : « En cette qualité, elle propose au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne, dans le cadre des orientations fixées par le Premier ministre, l'action gouvernementale en matière de défense des systèmes d'information ; » ;

2° Les septième et huitième alinéas sont complétés par les mots : « et des opérateurs d'importance vitale ».

III. – Le second alinéa de l'article 8 du même décret est supprimé.

IV. – Les articles 1er et 3 du décret du 7 juillet 2009 susvisé dans leur rédaction résultant des I et II du présent article peuvent être modifiés par décret.

Art. 4. – Sous l'intitulé « Sécurité et défense nationale » du point 2 de l'annexe au décret du 19 décembre 1997 susvisé, il est ajouté, dans le tableau relatif au code de la défense, la ligne suivante :

Décisions imposant aux opérateurs d'importance vitale un contrôle de leurs systèmes d'information.

Art. 5.

I. – Au 2° des articles R.1641-2, R.1651-3, R.1661-3 et R.1671-3 du code de la défense, après les mots : « R.1332-38 » sont ajoutés les mots : « R.1332-41-1 à R.1332-41-23 ».

II. – L'article 2 du présent décret est applicable sur l'ensemble du territoire de la République.

Art. 6. – La ministre des Outre-mer est chargée de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait le 27 mars 2015.

Par le Premier ministre : MANUEL VALLS

La ministre des outre-mer, GEORGE PAU-LANGEVIN

Annexe 6

DÉCRET RELATIF À LA QUALIFICATION DES PRODUITS ET PRESTATAIRES DE SERVICE DE CONFIANCE

Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale

Publics concernés : fournisseurs ou fabricants de produits de sécurité, prestataires de service de confiance, centres d'évaluation de services de confiance dans le domaine de la sécurité des systèmes d'information.

Objet : déterminer les procédures de qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

Entrée en vigueur : le décret est entré en vigueur le lendemain de sa publication.

Notice : le décret définit les procédures de qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Il définit également la procédure d'agrément des centres chargés d'évaluer les services de confiance dans le cadre de la procédure de qualification des prestataires. Les décisions de qualification et d'agrément sont prises par le Premier ministre à l'issue d'une évaluation ou d'un audit selon le cas. Le décret permet notamment de qualifier les systèmes de détection et les prestataires de service mentionnés aux articles L.1332-6-1 et L.1332-6-3 du code de la défense.

Références : le décret peut être consulté sur le site Légifrance (http://www.legifrance.gouv.fr).

Le Premier ministre,

Vu le code de la consommation, notamment son article L.115-28 ;

Vu le code de la défense, notamment ses articles L.1332-6-1, L.1332-6-3, L.2321-1 et R.

2311-1 et suivants ; Vu le code pénal, notamment ses articles 226-13 et 413-9 ;

Vu le code de la sécurité intérieure, notamment ses articles L.114-1 et R.114-2 ;

Vu la loi n° 2000-321 du 12 avril 2000 modifiée relative aux droits des citoyens dans leurs relations avec les administrations, notamment son article 21 ;

Vu le décret n° 97-1184 du 19 décembre 1997 modifié pris pour l'application au Premier ministre du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;

Le Conseil d'État (section de l'administration) entendu,

Décrète :

Dispositions générales

Art. 1er. – Il est institué une procédure de qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

Au sens du présent décret, on entend par :

1° « Produit de sécurité », tout dispositif, matériel ou logiciel, mettant en œuvre des fonctions qui contribuent à la sécurité des systèmes d'information ;

2° « Prestataire de service de confiance », toute personne fournissant des services qui contribuent à la sécurité des systèmes d'information.

Qualification des produits de sécurité

Art. 2. – La demande de qualification d'un produit de sécurité est adressée à l'Agence nationale de la sécurité des systèmes d'information. Celle-ci met à la disposition du public par voie électronique la liste des pièces à joindre à la demande, qui contient notamment

une description détaillée du produit et de ses fonctions de sécurité ainsi que les objectifs de sécurité qu'il vise à satisfaire.

Lorsque le dossier de demande est complet, l'Agence nationale de la sécurité des systèmes d'information s'assure, au vu des pièces fournies, que :

1° Les objectifs de sécurité du produit sont définis de manière pertinente au regard des menaces pesant sur la sécurité des systèmes d'information ;

2° Les fonctions de sécurité du produit sont cohérentes avec les objectifs de sécurité qu'il vise à satisfaire ;

3° Les matériels, les logiciels, leurs codes sources et la documentation nécessaires pour réaliser l'évaluation des fonctions de sécurité du produit sont disponibles sans restriction.

Lorsqu'elle estime que les conditions prévues aux 1° à 3° sont remplies, l'Agence nationale de la sécurité des systèmes d'information invite le demandeur à faire évaluer les fonctions de sécurité du produit en vue d'obtenir une qualification. Dans le cas contraire, elle lui indique les motifs pour lesquels le produit ne peut être qualifié.

Art. 3. – Pour faire évaluer les fonctions de sécurité du produit, le demandeur choisit un ou plusieurs centres d'évaluation agréés dans les conditions prévues par le décret du 18 avril 2002 susvisé. Il détermine avec chacun de ces centres le programme de travail et les délais nécessaires pour réaliser l'évaluation ainsi que les conditions dans lesquelles sera protégée la confidentialité des informations traitées dans le cadre de l'évaluation.

Lorsque l'évaluation de certaines fonctions de sécurité nécessite des compétences techniques particulières dont ne disposent pas les centres d'évaluation, l'Agence nationale de la sécurité des systèmes d'information évalue elle- même ces fonctions.

En l'absence de centre d'évaluation agréé, l'Agence nationale de la sécurité des systèmes d'information peut réaliser l'ensemble de l'évaluation.

Art. 4. – Le demandeur met à la disposition de l'Agence nationale de la sécurité des systèmes d'information et de chaque centre d'évaluation concerné l'ensemble des matériels, des logiciels, des codes sources et de la documentation nécessaires pour évaluer les fonctions de sécurité du produit.

Art. 5. – L'Agence nationale de la sécurité des systèmes d'information veille à la bonne exécution des travaux d'évaluation. Les centres d'évaluation l'informent sans délai de toute difficulté. L'agence peut à tout moment demander à assister à ces travaux ou à obtenir des informations sur leur déroulement. Elle peut également demander aux centres de compléter leur évaluation.

Art. 6. – Au terme de l'évaluation, chaque centre d'évaluation concerné remet un rapport au demandeur et à l'Agence nationale de la sécurité des systèmes d'information. Lorsqu'elle a réalisé tout ou partie de l'évaluation, l'agence remet un rapport d'évaluation au demandeur.

Les rapports d'évaluation sont des documents confidentiels susceptibles de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du Code pénal. Ils sont, le cas échéant, couverts par le secret de la défense nationale.

Art. 7. – Au vu des rapports d'évaluation, l'Agence nationale de la sécurité des systèmes d'information propose au Premier ministre de qualifier ou non le produit.

Lorsqu'il décide de qualifier le produit, le Premier ministre notifie au demandeur une décision mentionnant les objectifs de sécurité que satisfait le produit et précisant le niveau de qualification obtenu. La décision est assortie, le cas échéant, de conditions et de réserves et précise sa durée de validité.

En cas de manquement aux conditions et réserves fixées par la décision de qualification ou en cas de changement des circonstances de droit ou de fait dans lesquelles le produit a été qualifié, le Premier ministre peut, après que le demandeur a pu faire valoir ses observations, suspendre ou abroger la qualification.

Qualification des prestataires de service de confiance

Évaluation et qualification des prestataires

Art. 8. – La demande de qualification est adressée par le prestataire de service de confiance à l'Agence nationale de la sécurité des systèmes d'information. Celle-ci met à la disposition du public par voie électronique la liste des pièces à joindre à la demande, qui contient notamment :

1° La description des services sur lesquels porte la demande ;

2° L'organisation, les procédures et les méthodes mises en place par le prestataire pour fournir les services ;

3° Les coordonnées du centre d'évaluation choisi par le prestataire pour évaluer les services sur lesquels porte la demande ;

4° Le programme de travail défini par le prestataire avec le centre d'évaluation.

Art. 9. – Lorsque le dossier de demande est complet, l'Agence nationale de la sécurité des systèmes d'information s'assure, au vu des pièces fournies, que :

1° Les services fournis par le prestataire sont susceptibles de répondre aux besoins de sécurité des systèmes d'information ;

2° Le centre d'évaluation choisi est agréé pour évaluer les services sur lesquels porte la demande ;

3° Le programme de travail défini avec le centre d'évaluation est cohérent ;

4° Les documents nécessaires à l'évaluation sont disponibles ;

5° Les conditions d'accès aux locaux, au personnel et aux moyens techniques du prestataire sont satisfaisantes. Lorsqu'elle estime que les conditions prévues aux 1° à 5° sont remplies, l'Agence nationale de la sécurité des systèmes d'information invite le prestataire à faire évaluer ses services en vue d'obtenir une qualification. Dans le cas contraire, elle lui indique les motifs pour lesquels il ne peut être qualifié.

Art. 10. – Les services fournis par le prestataire sont évalués au regard de règles fixées par des référentiels propres à chaque type de services. Ces référentiels sont élaborés par l'Agence nationale de la sécurité des systèmes d'information et approuvés par le Premier ministre. Le cas échéant, les référentiels peuvent imposer au prestataire de respecter les prescriptions prévues aux articles R. 2311-1 et suivants du code de la défense.

L'évaluation est réalisée sur pièce et sur place par un centre d'évaluation agréé dans les conditions prévues à la section 2 du présent chapitre. Elle vise à s'assurer que le prestataire respecte les règles prévues par les référentiels mentionnés au premier alinéa, en particulier qu'il dispose du personnel compétent ainsi que des moyens techniques et des locaux adéquats pour fournir ses services.

Lorsque l'évaluation nécessite des compétences techniques particulières dont ne disposent pas les centres d'évaluation, l'Agence nationale de la sécurité des systèmes d'information apporte son concours à ces centres.

En l'absence de centre d'évaluation agréé, l'Agence nationale de la sécurité des systèmes d'information peut évaluer les services du prestataire.

Art. 11. – Le prestataire choisit un centre d'évaluation agréé sur la liste prévue à l'article 19. Il détermine avec le centre d'évaluation :

1° Les services à évaluer ;

2° Les conditions d'accès à ses locaux, à son personnel et à ses moyens techniques ;

3° Les conditions de protection des informations traitées dans le cadre de l'évaluation ;

4° Le programme de travail du centre.

Il met à la disposition de l'Agence nationale de la sécurité des systèmes d'information et du centre d'évaluation tous les documents nécessaires à l'évaluation. Il leur permet d'accéder à ses locaux et à ses moyens techniques et de rencontrer son personnel.

Dans le cadre de l'évaluation, l'Agence nationale de la sécurité des systèmes d'information et le centre d'évaluation peuvent chacun demander à assister au déroulement d'une prestation de service effectuée par le prestataire.

Art. 12. – L'Agence nationale de la sécurité des systèmes d'information veille à la bonne exécution des travaux d'évaluation. Le centre d'évaluation l'informe sans délai de toute difficulté. L'agence peut à tout moment demander à assister à ces travaux ou à obtenir des informations sur leur déroulement. Elle peut également demander au centre de compléter son évaluation.

Art. 13. – Au terme de l'évaluation, le centre d'évaluation remet un rapport au prestataire et à l'Agence nationale de la sécurité des systèmes d'information. Lorsqu'elle a réalisé l'évaluation, l'agence remet un rapport d'évaluation au prestataire.

Le rapport d'évaluation est un document confidentiel susceptible de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Il est, le cas échéant, couvert par le secret de la défense nationale.

Art. 14. – Au vu du rapport d'évaluation et, le cas échéant, des conclusions d'une enquête administrative sur le prestataire menée en application de l'article L.114-1 du Code de la sécurité intérieure, l'Agence nationale de la sécurité des systèmes d'information propose au Premier ministre de qualifier ou non le prestataire.

Lorsqu'il décide de qualifier le prestataire, le Premier ministre lui notifie une décision attestant sa capacité à respecter les règles mentionnées au premier alinéa de l'article 10 et précisant, s'il y a lieu, le niveau de qualification obtenu. La décision précise les services qualifiés et est assortie, le cas échéant, de conditions et de réserves.

La qualification est valable pour une durée maximale de trois ans et peut être renouvelée dans les mêmes conditions.

Art. 15. – L'Agence nationale de la sécurité des systèmes d'information peut s'assurer à tout moment que le prestataire respecte les règles au vu desquelles il a été qualifié. Le prestataire l'informe sans délai de toute modification des circonstances dans lesquelles il a été qualifié.

En cas de manquement aux conditions et réserves fixées par la décision de qualification ou en cas de changement des circonstances de droit ou de fait dans lesquelles le prestataire a été qualifié, le Premier ministre peut, après que le prestataire a pu faire valoir ses observations, suspendre ou abroger la qualification.

Agrément des centres d'évaluation

Art. 16. – La demande d'agrément est adressée par le centre d'évaluation à l'Agence nationale de la sécurité des systèmes d'information. Celle-ci met à la disposition du public par voie électronique la liste des pièces à joindre à la demande, qui contient notamment :

1° La description des moyens, des ressources et de l'activité passée du centre d'évaluation ;

2° Les types de services pour l'évaluation desquels le centre demande un agrément ;

3° Une accréditation comme centre d'évaluation de services, délivrée par une instance nationale mentionnée au premier alinéa de l'article L.115-28 du code de la consommation.

Lorsque le dossier de demande est complet, l'Agence nationale de la sécurité des systèmes d'information instruit la demande et en informe le centre d'évaluation.

Art. 17. – L'Agence nationale de la sécurité des systèmes d'information audite sur pièce et sur place le centre demandeur au regard des compétences de son personnel, de ses moyens, de ses ressources et de son activité passée. Lors de cet audit, l'agence peut demander à assister au déroulement d'une évaluation de services effectuée par le centre.

Le centre permet à l'agence d'accéder à ses locaux et de rencontrer son personnel. Il lui communique en outre tous documents nécessaires à l'audit.

Art. 18. – Le centre d'évaluation ne peut être agréé s'il n'est en mesure de respecter les prescriptions prévues aux articles R.2311-1 et suivants du code de la défense.

Art. 19. – Au vu des résultats de l'audit prévu à l'article 17 et, le cas échéant, au vu des conclusions d'une enquête administrative sur le centre d'évaluation menée en application de l'article L.114-1 du code de la sécurité intérieure, l'Agence nationale de la sécurité des systèmes d'information propose au Premier ministre d'agréer ou non le centre d'évaluation.

Lorsqu'il décide d'agréer le centre d'évaluation, le Premier ministre lui notifie une décision précisant les types de service pour l'évaluation desquels le centre est agréé. La décision est assortie, le cas échéant, de conditions et de réserves.

L'agrément est valable pour une durée maximale de trois ans et peut être renouvelé dans les mêmes conditions. L'Agence nationale de la sécurité des systèmes d'information met à la disposition du public par voie électronique la liste des centres d'évaluation agréés.

Art. 20. – L'Agence nationale de la sécurité des systèmes d'information peut s'assurer à tout moment que le centre d'évaluation respecte les conditions au vu desquelles il a été agréé. Le centre d'évaluation l'informe sans délai de toute modification des circonstances dans lesquelles il a été agréé, notamment de la suspension, du retrait ou de toute modification de son accréditation.

En cas de manquement aux conditions et réserves fixées dans la décision d'agrément ou en cas de changement des circonstances de droit ou de fait dans lesquelles le centre d'évaluation a été agréé, le Premier ministre peut, après que le centre d'évaluation a pu faire valoir ses observations, suspendre ou abroger l'agrément.

Dispositions diverses

Art. 21. – Sous l'intitulé « Sécurité et défense nationale » du point 2 de l'annexe au décret du 19 décembre 1997 susvisé, il est ajouté, après le tableau relatif au décret n° 2010-112 du 2 février 2010, le titre et le tableau suivants :

« Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale :

1	Délivrance, suspension et abrogation de la qualification des produits de sécurité.	Deuxième et troisième alinéas de l'article 7.
2	Délivrance, suspension et abrogation de la qualification des prestataires de service de confiance.	Deuxième alinéa de l'article 14 et second alinéa de l'article 15.
3	Délivrance, suspension et abrogation de l'agrément des centres d'évaluation.	Deuxième alinéa de l'article 19 et second alinéa de l'article 20.

Art. 22. – En application du 4° du I de l'article 21 de la loi du 12 avril 2000 susvisée, le silence gardé pendant deux mois par le Premier ministre sur les demandes mentionnées aux articles 2, 8 et 16 vaut décision de rejet.

Art. 23. – Le 1° de l'article R.114-2 du code de la sécurité intérieure est complété par deux alinéas ainsi rédigés :

« *m)* Des prestataires de service de confiance mentionnés au chapitre III du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale ;

« *n)* Des centres d'évaluation mentionnés au chapitre III du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale ; ».

Art. 24.

I. – Après le troisième alinéa de l'article 4 du décret du 7 juillet 2009 susvisé, il est inséré l'alinéa suivant :

« – de la qualification des produits de sécurité et des prestataires de service de confiance ainsi que de l'agrément des centres d'évaluation prévus par le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale ; ».

II. – L'article 4 du décret du 7 juillet 2009 susvisé dans sa rédaction résultant du I du présent article peut être modifié par décret.

Art. 25. – Le chapitre Ier, le chapitre II, le chapitre III ainsi que les articles 22, 23 et 26 du présent décret sont applicables sur l'ensemble du territoire de la République.

Art. 26. – Les dispositions du présent décret peuvent être modifiées par décret, à l'exception de l'article 7, du premier et du deuxième alinéa de l'article 14, du second alinéa de l'article 15, du premier et du deuxième alinéa de l'article 19, du second alinéa de l'article 20, de l'article 21 et de l'article 22.

Art. 27. – Le ministre de l'Intérieur et la ministre des Outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait le 27 mars 2015.

Par le Premier ministre : MANUEL VALLS
Le ministre de l'Intérieur, BERNARD CAZENEUVE

La ministre des Outre-mer, GEORGE PAU-LANGEVIN