WAVESTONE

OPÉRATEUR D'IMPORTANCE VITALE

CYBERSÉCURITÉ ET CONFORMITÉ LPM

La loi de programmation militaire (LPM) de décembre 2013 a notamment servi de véhicule législatif pour adresser le sujet de la cybersécurité des opérateurs d'importance vitale (OIV). Elle traduit les orientations du livre blanc sur la défense et la sécurité nationale, publié en avril de la même année.

En particulier, le chapitre IV de la LPM donne plus de pouvoirs au Premier ministre et à l'ANSSI en matière de sécurité et de défense des systèmes d'information. Ce texte responsabilise pour la première fois les OIV quant à la sécurisation de leurs systèmes d'information d'importance vitale (SIIV).

Mobilisés par l'ANSSI et les Ministères depuis de nombreux mois, les OIV ont désormais enclenché leur mise en conformité à ces nouvelles exigences.

Ce document vise, en respectant le secret de la défense nationale, à **résumer le cadre législatif et règlementaire de la LPM** et à partager des retours d'expérience liés aux **projets de mise en conformité**, qui ont marqué l'actualité ces derniers mois.

1958 – 2016 : DE LA SÉCURITÉ PHYSIQUE À LA CYBERSÉCURITÉ

La notion d'opérateur d'importance vitale apparaît dans l'ordonnance n°58-1371 du 29 décembre 1958, tendant à renforcer la protection des installations d'importances vitales : « Les entreprises 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 fixées à la présente ordonnance, à la protection desdits établissements, installations et ouvrages contre toute tentative de sabotage ». La liste des opérateurs est confidentielle.

AUTEUR

ETIENNE CAPGRAS
etienne.capgras@wavestone.com

Ainsi, les exigences portaient exclusivement sur la **protection physique des points d'importance vitale** (PIV) vis-à-vis des actes de sabotage. Depuis, les principes de sécurisation et les interlocuteurs mobilisés sont globalement restés les mêmes, tandis que les OIV se sont vus structurés en douze secteurs d'activité, via le décret n°2006-212 du 23 février 2006. Tout cela est résumé dans l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale (SAIV), l'IGI n°6600 du 7 janvier 2014.

En juin 2008, une nouvelle menace est mise en avant par le livre blanc sur la défense et la sécurité nationale et mène notamment à la création de l'agence nationale de la sécurité des systèmes d'information (ANSSI) en 2009 : la **cybermenace**. En avril 2013, elle se retrouve élevée au rang de menace de première importance.

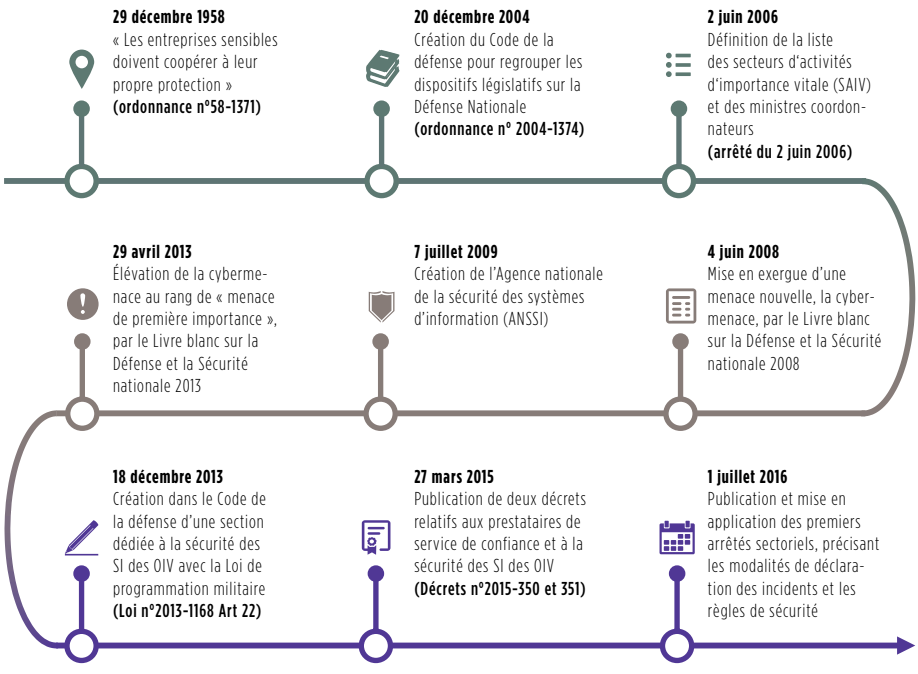
C'est ainsi qu'en décembre 2013, **la LPM vient compléter le dispositif SAIV existant et déployé chez les OIV par un volet cybersécurité**. Elle apporte par la même occasion son lot de nouveaux interlocuteurs, avec en tête l'ANSSI et les RSSI des OIV, et nécessite de faire évoluer un existant en place souvent depuis plusieurs dizaines d'années.

ARRÊTÉS SECTORIELS : 20 RÈGLES POUR PROMOUVOIR LES BONNES PRATIQUES, LABELS ET RÉFÉRENTIELS ANSSI

Le premier objectif de la LPM est de **sécuriser les SI d'importance vitale** (SIIV) dont la définition fait écho à celle des OIV : « 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 ou pourrait présenter un danger grave pour la population ». Il peut aussi bien s'agir de SI de gestion que de SI Industriel.

Au-delà de la loi et des décrets fixant les conditions de sa mise en œuvre, les exigences concrètes devant s'appliquer aux SIIV ont été rédigées par l'ANSSI en concertation avec les OIV. Elles ont progressivement été publiées dès la mi-2016, sous la forme d'**arrêtés sectoriels** et sous-sectoriels : produits de santé, gestion de l'eau, alimentation, transport terrestre, transport maritime et fluvial, transport aérien, énergie électrique, gaz naturel et hydrocarbures pétroliers. Les arrêtés manquants devraient être publiés d'ici au premier trimestre 2017.

Sécurité des activités d'importance vitale : de la sécurité physique à la cybersécurité



Les différences d'un arrêté à l'autre sont par ailleurs assez mineures.

Au final, tout OIV devra être conforme à 20 règles de sécurité précisées dans ces arrêtés, selon des **délais variables d'une règle à l'autre** et d'un secteur à l'autre (ces délais sont en Diffusion Restreinte et notifiées par l'ANSSI aux seules personnes ayant besoin d'en connaître) :

- **Gouvernance (règles 1 et 20) :** être doté d'une politique de sécurité du SI (PSSI) intégrant la notion de SIIV et posant notamment des exigences en termes de sensibilisation, de formation et de reporting à la Direction de l'OIV. Certains indicateurs SSI doivent également être générés (suivi des comptes, patch management, etc.).
- **Maîtrise des risques (règle 2) :** l'OIV doit mener une homologation formelle de chacun de ses SIIV. La décision d'homologation est prise par une commission interne à l'OIV, en capacité de représenter l'OIV sur le plan pénal. Tout acte d'homologation sera précédé d'un audit SSI. réalisé conformément au référentiel PASSI LPM , soit par un prestataire qualifié soit par une équipe interne de l'OIV. Le renouvellement de l'homologation est à prévoir à minima tous les 3 ans, pour prendre en compte l'évolution du contexte et des menaces.
- **Maîtrise des SI (règles 3 et 4) :** il est attendu de l'OIV qu'il connaisse à tout moment les composants constituant chacun de ses SIIV (cartographies à disposition de l'ANSSI sur demande) et qu'il sache y déployer tous les correctifs de sécurité nécessaires ou mettre en œuvre des mesures compensatoires appropriées.
- **Gestion des incidents de sécurité (règles 5 à 10) :** au niveau de la détection des incidents, les journaux d'événements clés doivent être activés, centralisés et archivés, puis corrélés et analysés sur une infrastructure dédiée et en s'appuyant sur le référentiel PDIS. Des sondes réseaux qualifiées doivent être mise en place entre les SIIV et les réseaux tiers à ceux de l'OIV. Le traitement des incidents doit s'appuyer sur le référentiel PRIS et l'OIV doit posséder un service de permanence, communément appelé astreinte, pour assurer le traitement des alertes en 24/7. Enfin, une procédure de gestion de crise doit

pouvoir être déclenchée sur demande du Premier Ministre afin d'assurer la cyber-résilience des SIIV et du SI de l'OIV.

/ **Protection des systèmes (règles 11 à 19) :** chaque SIIV doit respecter les bonnes pratiques de sécurité sur l'authentification et l'habilitation des utilisateurs des SIIV, sur les principes et infrastructures d'administration, sur le cloisonnement des SIIV et la gestion des flux, sur les principes d'accès à distance ainsi que sur le durcissement des composants à leur installation.

Cet ensemble de règles rappelle donc les **bonnes pratiques de sécurité** et exige qu'elles soient respectées **à minima sur le périmètre des SIIV** que ceux-ci soit des SI de gestion ou des SI industriels malgré leurs spécificités.

Au travers de ces arrêtés, l'État en profite également pour **promouvoir les documents produits** ces dernières années : référentiels PASSI, PDIS, PRIS, guides de sécurisation et bonnes pratiques, stratégie d'homologation, méthodologie d'analyse de risque EBIOS, II 901 sur la protection des SI sensibles, etc.

RÉUSSIR SA MISE EN CONFORMITÉ À LA LPM

L'entrée en application de la LPM mène nécessairement à un **investissement conséquent de la part des OIV**, ne serait-ce que pour décliner la notion de SIIV sur leur périmètre, démontrer leur conformité à chacune des règles et aligner leurs processus et corpus documentaire sur le formalisme imposé par la LPM.

De par ses relations privilégiées avec l'ANSSI et son rôle sur la SSI au sein de son entreprise, le **RSSI est l'acteur légitime pour piloter et animer cette mise en conformité**. De la mobilisation des acteurs à la généralisation des principes de sécurité, en passant par le cadencement des chantiers et la construction de cibles acceptées par tous, quels sont les facteurs clés de réussite ?

Par où commencer ? Dresser la liste des SIIV

Tous les OIV **doivent déclarer leurs SIIV à l'ANSSI dans un délai de 3 mois** à compter de l'entrée en vigueur de l'arrêté les concernant. Il est important de noter que les **exigences portent uniquement sur les SIIV**, et non sur l'ensemble du SI de l'OIV. L'identification des SIIV doit par conséquent être un **chantier réalisé avec le plus grand soin pour être conforme à la loi tout en limitant les impacts au maximum**.

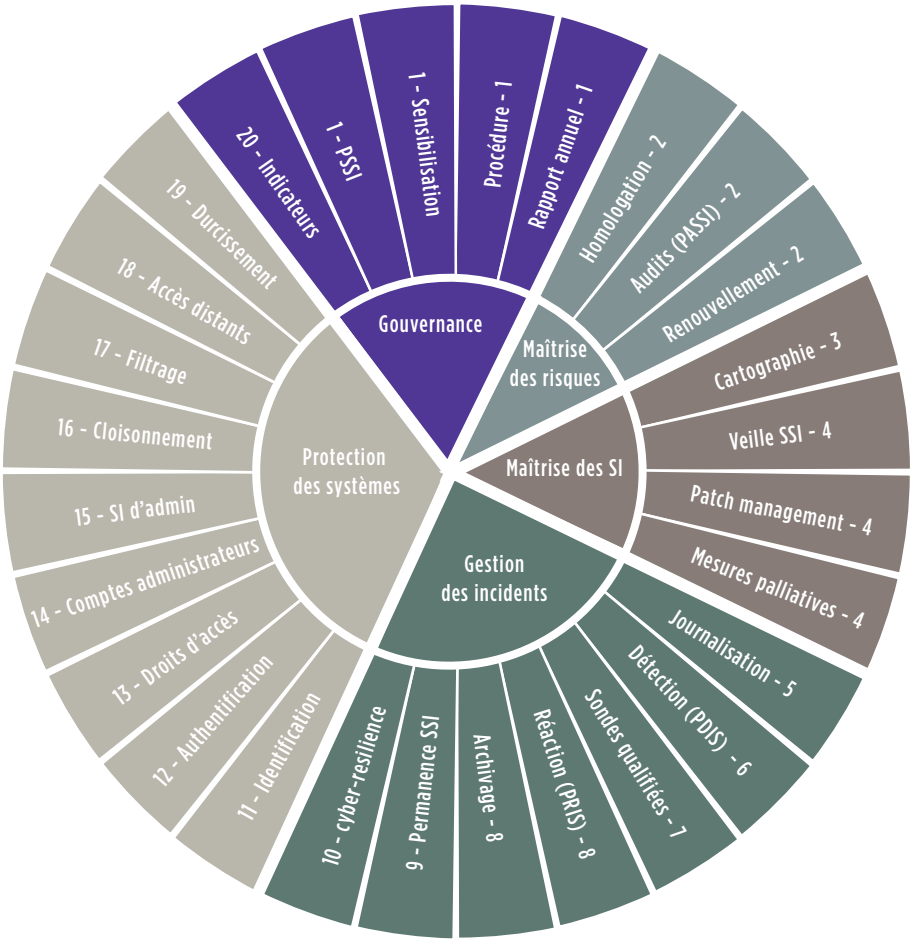
Au-delà des typologies de SI éligibles (proposées en annexe III de chaque arrêté), l'analyse doit partir des missions d'importance vitale (MIV) confiées par l'État à l'OIV. Elles sont listées dans les Directives Nationales de Sécurité (DNS), en possession de l'Officier de Sécurité de l'OIV puisque c'est un document classifié Confidentiel Défense. Des rencontres avec les métiers permettront ensuite d'affiner la compréhension des processus et de leur transcription sur le SI en termes d'applications.

L'enjeu est ici de définir une méthode systématique et une justification rigoureuse sur les critères d'inclusion et d'exclusion des applications potentiellement éligibles.

D'autre part, nos retours d'expérience sur l'identification des SIIV montrent que la logique « d'importance vitale » diffère entre une vision de l'entreprise (qui vise à assurer sa propre survie) et celle de l'État (qui vise à assurer la sécurité des citoyens). Concrètement, les systèmes commerciaux assurant les ventes ou la facturation, ne sont souvent pas répertoriés dans la liste des SIIV.

Les applications d'importance vitale représentent aujourd'hui au maximum 3% du parc applicatif de nos clients. Les SIIV sont quant à eux constitués de l'ensemble des applications concourant à un même processus d'importance vitale.

20 règles pour promouvoir les bonnes pratiques, labels et référentiels ANSSI



Recenser les écarts et dessiner des premières cibles

L'analyse d'écart doit elle aussi débuter au plus vite, **sans attendre la stabilisation de la liste des SIIV**.

Certes des subtilités techniques seront présentes, mais des tendances devraient rapidement apparaitre sur les nombreux thèmes transverses tels que la supervision SSI, les cartographies, les principes d'authentification voire la gestion des correctifs de sécurité. Ce qui, en particulier sur les SI industriels, n'est pas sans poser des interrogations assez importantes.

Ici, l'enjeu est double : **anticiper le macro-budget** qui sera nécessaire à la mise en conformité et l'inscrire dans l'exercice de prévision budgétaire pluriannuel. Expliquer la LPM aux futurs porteurs d'actions et les **mobiliser autour de l'identification de cibles** qui pourraient répondre aux différentes exigences.

Il est crucial de **ne pas traiter la mise en conformité règle par règle** : selon les cas, certaines cibles d'apparence plus complexe permettent de couvrir plusieurs règles à la fois, diminuant ainsi l'investissement nécessaire au global. Ce constat est d'autant plus fort sur la protection des systèmes, où les principes de cloisonnement, les pratiques d'administration et les mécanismes d'authentification sont très liés.

Favoriser la pratique à la théorie

Les situations où il est **difficile de faire converger** les différentes approches sont légions dans ce type de programme. Aussi, le passage à la pratique est souvent le meilleur des alliés :

- La réalisation d'un audit à blanc technique et organisationnel permettra d'obtenir des réponses factuelles et détaillées et d'ainsi débloquer les éventuelles analyses d'écart fastidieuses ;
- De même, la réalisation d'une homologation sur un SIIV pilote permettra à la fois de préciser le processus d'homologation et le contenu du dossier et fluidifiera d'autant les autres homologations ;
- Enfin, la mise en œuvre sur un SIIV pilote des principes de sécurisation retenus permettra de concrétiser les modalités d'implémentation spécifiques et transverses et d'affiner les modèles initialement retenus, avant généralisation.

Paralléliser les chantiers

Les délais associés aux différentes règles sont très ambitieux. Aussi, il est indispensable de traiter en parallèle tous les sujets qui peuvent l'être.

C'est notamment le cas de la formalisation des **guides de durcissement**, des évolutions de la **PSSI**, des processus d'**intégration de la sécurité dans les projets**, des modifications au niveau des **clauses contractuelles** et des processus de **sélection des fournisseurs**, etc.

Tirer parti de la complémentarité des équipes

La LPM aborde le sujet de la cybersécurité au travers d'une loi et en l'inscrivant dans le dispositif SAIV. Les **interlocuteurs sont donc tout aussi nombreux que variés** : les dirigeants dans la mesure où la responsabilité pénale de l'OIV est engagée, les responsables de la sûreté garants du bon maintien du dispositif SAIV, les RSSI interlocuteurs habituels de l'ANSSI, les responsables de la conformité, les métiers en regard des missions d'importances vitales qu'ils peuvent porter, les DSI au vu des impacts potentiels sur le SI, les achats sur la gestion des fournisseurs, les équipes techniques opérant le SI au quotidien, etc.

Face à cette multitude d'interlocuteurs et d'approches parfois radicalement opposées, il est impératif de voir au-delà de la complexité apparente : cette situation est surtout l'occasion de mobiliser un nombre inédit d'acteurs autour de la cybersécurité et d'ainsi **actionner des leviers jusque-là inaccessibles**. Il est notamment plus facile d'**obtenir les ressources nécessaires** à la bonne réussite du programme lorsqu'autant d'enjeux sont réunis.

UN PAYSAGE CYBERSÉCURITÉ MODELÉ EN PROFONDEUR

Les cadrages menés jusqu'à présent par les OIV démontrent une forte **volonté de prendre en compte la LPM** le plus en amont possible, avec au sein des grands comptes que nous accompagnons, plusieurs dizaines de millions d'euros budgétés pour les années à venir.

Par ailleurs, la LPM a **démontré l'intérêt de la cybersécurité à des décideurs historiquement peu mobilisés sur ce sujet**, que ce soit au sein des OIV ou de leurs fournisseurs. Gageons que cette prise de conscience annonce une sécurisation pérenne des SIIV et des SI plus largement.

Dans tous les cas, l'enjeu à venir pour les OIV est de ne surtout pas réduire la cybersécurité aux programmes LPM mais bien au contraire de les utiliser comme accélérateur pour leurs autres projets, sous peine de délaisser leurs SI critiques non considérés comme vitaux pour la survie de la nation (et ils sont nombreux). C'est bien cet équilibre qui déterminera la réussite ou l'échec des projets de mise en conformité à la LPM.

WAVESTONE

www.wavestone.com