siapartners

INSIGHT

NOVEMBRE 2015

LA LOI DE PROGRAMMATION MILITAIRE,
UN CADRE JURIDIQUE DE LA POLITIQUE DE CYBER DEFENSE NATIONALE FRANÇAISE

La Loi de Programmation Militaire (LPM) définit l'ensemble des moyens à mettre en œuvre pour assurer la défense de la Nation et la sécurité des citoyens en cas de conflit. Faisant l'objet d'une révision tous les 5 ans pour prendre en compte les nouvelles menaces, la dernière révision, adoptée par le parlement en décembre 2013, concerne la période 2014 – 2019. Parmi les changements notables de cette nouvelle édition, la prise en compte des menaces relatives à la cyber-sécurité et l'obligation pour les Opérateurs d'Importance Vitale (OIV) d'assurer la protection et la résilience de leurs systèmes d'information (SI) contre les cyber-attaques.

On dénombre environ 250 OIV publics et privés répartis dans 12 secteurs d'activité dits «d'importance vitale » (la santé, la gestion de l'eau, l'alimentation, l'énergie, les télécommunications & les médias d'information, les transports, la finance, l'industrie, la sécurité civile, les activités militaires, la justice et enfin l'espace et la recherche).
Les OIV sont désignés par les Ministères de tutelle en charge des activités d'importance vitale (pour les télécoms, le ministère du redressement productif) et son représentant pour tout ce qui a trait à la sécurité et la défense : le Haut Fonctionnaire de Défense et Sécurité (HFDS). Cette désignation est confidentielle pour des raisons évidentes de sécurité

LPM et Cyber défense au sein des OIV

La cyber-sécurité, un enjeu stratégique

Jusqu'au milieu des années 2000, le principal objectif des programmes malicieux et attaques informatiques était de vandaliser le « SI victime ». Le **panorama des cyber-menaces a évolué** depuis **vers un cyber-crime** de plus en plus **organisé et ciblé**, avec des **objectifs** souvent financiers à la clé[1].

Le risque informatique (ou cyber-risque) n'est en effet plus sporadique, il cible de manière structurée les entreprises et les pays.

[1] « Panorama des cyber-menaces » - Kaspersky Lab - 2014

Les organisations terroristes sont de plus en plus « digitalisées ». Et au-delà de l'intérêt pécuniaire, ce « cyber-terrorisme » constitue désormais une réelle menace à la **sécurité**, l'**intégrité** ou l'**économie d'un Etat**.

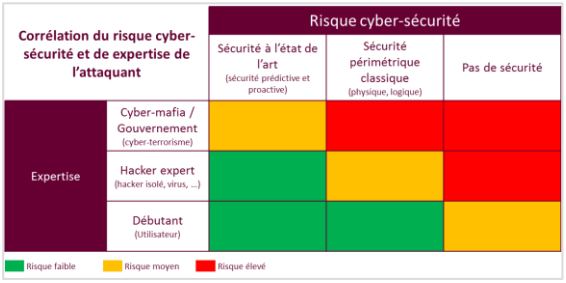

FIGURE 1 - CARTOGRAPHIE DU NIVEAU DE CYBER-RISQUE EN FONCTION DU NIVEAU DE CYBER-MENACE ET CYBER-SECURITE

La complexité de la définition de la « cyberdéfense » au niveau d'un Etat réside dans le périmètre à couvrir. Il est ainsi nécessaire d'**identifier les ressources nationales critiques**, **d'adapter les plans de gestion de crises, de continuité et de reprises d'activité** et de les coordonner le cas échéant, pour **supporter une gestion de crise à l'échelle nationale**. La LPM constitue ainsi un cadre à cette cyber-sécurité nationale.

Exigences cyber défense de la LPM : un palier structurant de la « cyber-sécurité » au sein des OIV

Dans son volet cyber-sécurité, la LPM fixe les grandes orientations et les objectifs à atteindre en matière de sécurité des infrastructures d'importance vitale, appelées aussi **Systèmes d'Information d'Importance Vitale** (SIIV). Il s'agit principalement de renforcer la **protection** et **la résilience des SIIV contre les Cyber-attaques**.

L'**Agence Nationale de Sécurité des Systèmes d'Information** (ANSSI), référant étatique en matière de Cyber-sécurité, est désignée par la LPM comme le bras armé du Premier Ministre en termes de cyber défense, notamment à travers son rôle d'accompagnateur des OIV pour l'intégration des exigences cyber défense. L'ANSSI a aussi un rôle de **contrôle ponctuel** de la bonne mise en œuvre de ce volet cyber défense au sein des OIV

Les premiers décrets d'application publiés en mars 2015 exigent des OIV de :

- **Sécuriser leur SIIV**, selon les modalités à définir en concertation avec l'ANSSI
- Dérouler un premier exercice de **contrôles mené par l'ANSSI**
- **Mettre en œuvre des systèmes de supervision et de détection d'évènements sécurité** (Security Operation Center - **SOC**) et signaler leurs incidents de sécurité aux autorités.

Les arrêtés sectoriels sont attendus d'ici la fin de l'année. Ils seront le point de départ de la phase de déploiement.

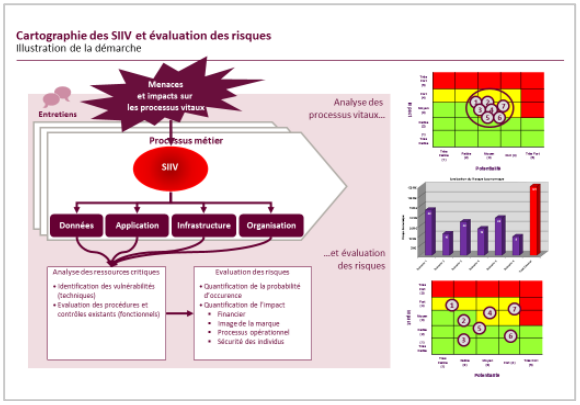

FIGURE 2 - EXEMPLE DE DEMARCHE D'ANALYSE DE RISQUES LPM

Mise en conformité des OIV aux exigences de cyber-sécurité de la LPM

L'ANSSI estime que la durée nécessaire aux OIV pour un **déploiement global des mesures de cyber-sécurité** serait de **trois ans**. C'est une durée significative qui souligne l'importance d'un tel chantier ainsi que le niveau d'exigence que peut avoir l'ANSSI vis-à-vis des OIV.

Définition de la cible cyber-sécurité au sein des OIV, une première étape stratégique

Dans l'optique de respecter les exigences de la LPM, un plan de mise en conformité doit être mis en place. Il présentera les actions à mener durant les trois prochaines années tout en s'adaptant au contexte de chaque OIV. En effet, au-delà de la **cartographie des SIIV**, les OIV devront mettre en place **un système de management de la sécurité informatique** (**SMSI**) complet sur leur périmètre critique, basé sur une **analyse de risques** préalable. Cette étape, structurante pour les OIV, permettra de définir un **plan d'actions priorisé** à valider avec l'ANSSI avant implémentation.

Préparation de l'écosystème cyber-sécurité

L'ANSSI ne se satisfera pas de quelques produits de sécurité pour bloquer les attaques. Elle prône depuis longtemps déjà une sécurité en profondeur sur les systèmes avec notamment une gestion rigoureuse des accès et de l'étanchéité des réseaux. Il s'agit ainsi pour les OIV de **construire un écosystème** régi par des **conventions tripartites** avec les **prestataires de confiance** (Prestataires de Détection d'Incident de Sécurité -PDIS- et Prestataires de Réponse aux Incidents de Sécurité -PRIS-) et **les autorités** pour mettre en place des systèmes de détection d'incidents efficients.

Mise à niveau du dispositif cyber-sécurité des OIV, un équilibre entre coût et risque à trouver

Dans un contexte réglementaire de plus en plus vigilent quant aux risques liés à la cyber-sécurité (ex. : protection des données à caractère personnel, localisation des données, etc.) le coût de l'opération, à la charge des opérateurs, sera important. On estime que la mise en œuvre de la LPM engendrerait un **triplement des budgets de sécurité SI sur 3 à 6 ans**[2].

Les amendes de non-conformité LPM peuvent aller jusqu'à 150 000 € à l'encontre du Directeur de l'OIV et 1 000 000 € pour l'OIV elle-même)

[2] Estimations SOGETI

Même si l'ANSSI accepte le principe de priorisation en limitant le champ de la réglementation aux SIIV, le **périmètre à sécuriser sera important**. Il couvre aussi bien le système d'information de gestion (poste de travail, annuaire, rebond, coffre-fort numérique, etc.) que les infrastructures (réseau de télécommunication, système industriel type SCADA, etc.).

La **transversalité du périmètre** à sécuriser et les enjeux de cette nouvelle réglementation obligera certainement les OIV à **revoir leur politique de sécurité** et **l'organisation** qui en a la charge (vision transverse des systèmes, interlocuteur pour les autorités, …). La notion de **gouvernance de la sécurité des systèmes d'information** et les processus associés doivent être clairement définis et bien appliqués.

Mis à part le rôle du RSSI, du DSI et du directeur de l'OIV dans le respect des exigences de la LPM, **la responsabilité du métier** est un facteur important. Il est le premier utilisateur des SI en entreprise. **Sensibiliser les utilisateurs**, souvent le maillon faible de la sécurité informatique, sur les bonnes pratiques cyber-sécurité constitue une première étape vers la mise en place de procédures de sécurité.

Dans cette course à « l'hyper-sécurité », il sera sans doute nécessaire de ne pas perdre de vue deux principes clés d'une cyber-sécurité efficiente, à savoir : (1) **le coût de la sécurité ne devra pas dépasser le coût du risque** (risque des cyberattaques et risque réglementaire) et (2) les **mesures de sécurité ne devront pas impacter** (trop) **négativement le métier au quotidien**. Et pour ce faire, les OIV devront collaborer avec l'ANSSI pour mettre aboutir à un plan de mise en conformité adapté.

Rappelé par le Premier Ministre, Manuel Valls, lors de la présentation de la stratégie nationale pour la sécurité du numérique, le 16 octobre dernier, l'objectif « ultime » de la mise en place de cette cyberdéfense, confirmé à travers la LPM, est finalement de « faire de la sécurité du numérique un facteur de compétitivité ».

VOS CONTACTS

MASSIMO SPADA

Partenaire
Massimo.spada@sia-partners.com

THIERRY BORGEL

Directeur Projet
Thierry.borgel@sia-partners.com

CHRISTOPHE LAMBERT

Supervising Senior
Christophe.lambert@sia-partners.com

TAHA BARAKATE

Consultant Senior
Taha.barakate@sia-partners.com

BADR BOUGANGA

Consultant
Badr.bouganga@sia-partners.com

ROMARY SIATOU

Consultant
Romary.siatou@sia-partners.com

A PROPOS DE SIA PARTNERS

Sia Partners est devenu en quinze ans le leader des cabinets de conseil français indépendants. Cofondé en 1999 par Matthieu Courtecuisse, Sia Partners compte 700 consultants pour un chiffre d'affaires de 120 millions de dollars. Le Groupe est présent dans treize pays, les Etats-Unis représentant le deuxième marché. Sia Partners est reconnu pour son expertise pointue dans les secteurs de l'énergie, les banques, l'assurance, les télécoms et le transport.

Sia Partners dispose d'une équipe hautement compétente dédiée au conseil aux DSI. L'unité CIO Advisory est composée de 20 experts en SI présentant des compétences et connaissances variées, impliqués dans des projets sur différents secteurs dont principalement le secteur Public, les secteurs de l'Energie, de l'Industrie, du Transport et de la Banque / Assurance.

Asia

Hong Kong
23/F, The Southland Building, 48 Connaught Road, Central – HK
T.+852 3975 5611

Singapore
3 Pickering street #02-38
048660 Singapore
T.+ 65 6635 3433

Tokyo
Level 20 Marunouchi Trust Tower-Main
1-8-3 Marunouchi, Chiyoda-ku
Tokyo 100-0005
Japan

Europe

Amsterdam
Barbara Strozzilaan 101
1083 HN Amsterdam - Netherlands
T. +31 20 240 22 05

Brussels
Av Henri Jasparlaan, 128
1060 Brussels - Belgium
+32 2 213 82 85

London
Princess House, 4th Floor, 27 Bush Lane,
London, EC4R 0AA – United Kingdom
T. +44 20 7933 9333

Lyon
Tour Oxygène, 10-12 bd Vivier Merle
69003 Lyon - France

Milan
Via Medici 15
20123 Milano - Italy
T. +39 02 89 09 39 45

Paris
12 rue Magellan
75008 Paris – France
T. +33 1 42 77 76 17

Rome
Via Quattro Fontane 116
00184 Roma - Italy
T. +39 06 48 28 506

Middle East & Africa

Dubai, Riyadh, Abu Dhabi
PO Box 502665
Shatha Tower office 2115
Dubai Media City
Dubai, U.A.E.
T. +971 4 443 1613

Casablanca
14, avenue Mers Sultan
20500 Casablanca - Morocco
T. +212 522 49 24 80

North America

New York
115 Broadway 12th Floor
New York, NY10006 - USA
T. +1 646 496 0160

Charlotte
401 N. Tryon Street, 10th Floor
Charlotte, NC 28202

Montréal
2000 McGill College, Suite 600, Montreal, QC H3A 3H3 - Canada