

**HACK’NEOM**

**–**

**LES ENJEUX**

**DE LA CYBERDEFENSE**

1. **Contexte général**

Définition (ANSSI - [Agence nationale de la sécurité des systèmes d'information](http://www.ssi.gouv.fr/)) de la cyberdéfense : « Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d’information jugés essentiels».

Le marché de la sécurité informatique est très vaste, couvrant tous les aspects d’un système d’information : Management et gouvernance de la sécurité (normes), Gestion et unification des identités, Sécurité technique du système d’information (prévention/audit, intrusion detection system), Supervision des incidents de sécurité…

A court terme, les DSI mettront en place un pilotage de la sécurité de plus en plus orienté vers la gestion des risques et de la conformité, ainsi qu’une utilisation de plus en plus intensive des produits de sécurité en mode SaaS (Software as a service).

En tendance, les SI devront faire face à une augmentation des problématiques de sécurité liées aux terminaux mobiles.

* 1. **La LPM et OIV**

La [loi de programmation militaire 2014-2019](http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id) (LPM),  organise le modèle de la « défense et la sécurité nationale » sur les 5 ans à venir, en tenant compte de nos moyens, et des menaces qui pèsent sur notre pays. Elle fixe le cadre et les budgets pour faire évoluer les capacités de renseignement, de dissuasion et d’armement de nos forces…

Bien au-delà du monde « militaire de la défense », la LPM décline aussi les enjeux de « cyberdéfense » pour la sécurité de notre pays. Cette loi amende quelques articles de différents codes (code de la défense, code de procédure pénale, code de la sécurité intérieure, code de la propriété intellectuelle …), et en ajoute quelques-uns.

<http://www.orange-business.com/fr/blogs/securite/lois-reglementations-standards-et-certifications/loi-de-programmation-militaire-les-operateurs-d-importance-vitale-en-ligne-de-mire-osd14>

Sur les plus de 200 OIV repartis en 12 secteurs d’activités d’importance vitale (quels sont ces secteurs ?), tous ne sont pas des acteurs du « cyber », mais la majorité sont dépendants de systèmes opérants de plus en plus connectés, et encore trop constitués de composants « cyberfragiles ».

Avec cette LPM, la cybersécurité a bien les pieds dans le réel du « citoyen » … et l’article 22 donne aux OIV quelques obligations :

* assurer la détection d’incidents avec des solutions et les prestataires qui les exploitent devant  être « qualifiés » par les services du premier Ministre ;
* de déclaration immédiate de tout incident affectant le système d’information ;
* possibilité d’audit des systèmes à la demande du Premier Ministre par l’ANSSI ou autre service de l’Etat, ou par une société labellisée ;
* et un pouvoir élargi du Premier Ministre pour imposer aux OIV les mesures nécessaires en cas de crise;
  1. **Activités autour de la SSI**
     1. **Domaines de compétences**
* Sécurité offensive :

Tests de pénétration, Audit de sites web

* Sécurité défensive :

Développement applicatif sécurisé, sécurisation des réseaux et plateformes (IDS, SIEM, Infra PKI), gestion des identités (IAM), gestion des incidents au travers des entités SOC, CERT/CSIRT

* Forensique :

Investigation (rétro-ingénierie, analyse de cellulaires, PC, récupération de données à des fins juridiques)

* Gouvernance de la sécurité d’un SI:

Mise en conformité, normalisation ISO 2700X, continuité d’activité, risk management

**Quid des développeurs d’applications sensibilisés à la sécurité ?**

**Quid de la sécurité des IoT (Internet-Of-Things) ?**

**Quid de la sécurité des mobiles (Android premier visé par les malwares) ?**

**TOP 10 DES VULNÉRABILITÉS DES SYSTÈMES INDUSTRIELS, ÉTABLI PAR LEXSI (\*) :**

* Absence de patchs sécurité et durcissement des systèmes (OS/firmwares)
* Utilisation de protocoles non sécurisés
* Absence de supervision sécurité (SIEM / IDS) 🡺 Sujet revenant fréquemment, expertise Big Data requise, Top 10 des vulnérabilités, outils existants mais peu de positionnement sur la part des cabinets sur leurs intégrations/développements
* Interface Homme Machine toujours connecté
* Pas de veille en cyber-sécurité
* Absence d’antivirus actif et à jour sur les postes de travail et serveurs
* Interconnexion SIG / SII non sûre
* Mauvaise gestion des comptes & mots de passe
* Pas de tests / évaluation du niveau de sécurité
* Pas de développement sécurisé
  + 1. **Les labels / normes**
* Les gages de qualités pour le prestataire;

Labels de l’ANSSI :

* + - * PASSI : les audits de sécurité
      * PRIS : Réponse aux incidents de sécurité (CERT)
      * PDIS : Détection des incidents de sécurité (SOC) – le SIEM s’inscrit comme un élément du SOC
* Les gages de qualités pour le client (confirmité, management, datacenter, …);
  + - * ISO 2700X
      * TIER3+
      * TIER4
      * PCI
      * ISAE 3402
    1. **Les outils**
* Management des identités (Sailpoint, IBM Tivoli)
* Outil de détection d’intrusion, malware (Gatewatcher, Tenable network security (<http://www.tenable.com/fr/securitycenter-continuous-view/)>)
* Scanner de vulnerabilities (Nessus, Qualys)
* Monitoring réseau (Qualys, Tenable network security)
* Corrélation de logs, infrastructure de supervision de la sécurité, SIEM (Splunk - https://fr.wikipedia.org/wiki/Splunk, ArcSight, IBM Security QRadar, ELK (open source : <https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04>, http://logz.io/learn/complete-guide-elk-stack/)



Autres ; outils partenaires de Qualys : <https://www.qualys.com/partners/solution-technology/#/>

* 1. **Chiffres clés**
  2. **Evènements clés**
  3. **Contacts**

1. **Analyse concurrentielle**

Définir les OIV qui présentent une cyberfragilité et qui sont déjà les acteurs positionnés sur ces domaines/clients. (banque, télécoms,mobile/embarqué, santé, défense, gouvernemental/administration,…)

**Les acteurs ;**

**Specialisés (unique cœur de métier):**

*Lexsi* (racheté par Orange tout récemment), a son CERT – Audit, détection, gestion incidents

*Synaktiv* – idem

*Sysdreams* – idem + plateforme de simulation pour l'entraînement à la cyberdéfense.

*Celteam* – Sécurisation des données au niveau logique (systèmes, réseaux, applis) et physiques (bâtiments, zones sensibles, ..).

*Harmonie Technologies* (GRC - Governance, Risk & Compliance, IAM - Identity & Access Management,DSP - Data Security & Privacy, CYBER - Cyber security)

*Intrisec + Cloud Temple* (I-SOC and CERT), solution tout-en-un, Cloud avec datacenters labellisés + détection des incidents + response team (CERT), objectif 🡺 mise en conformité de la sécurité SI. Questions ; quelles sont les solutions sous-jacentes (détection d’intrusion, SIEM), développées maison, open-source, d’autres prestataires sont-ils sollicités ?



*Quarkslab –* sécurité offensive, défensive + pen tests Iphone/Android

**Cabinets avec une entité/offre cybersécu :**

*Orange Business Services* (Lexsi, Atheos)

*Devoteam*, a son pôle cyberdéfense également + CERT

*GFI* (http://www.gfi.fr/is/securite.php)

*Mazars* -- Sécurité IT ( Protection des données personnelles, CNIL) & tests d’intrusion (http://www.mazars.fr/Accueil/Expertise/Consulting/Ethique-et-conformite/Nos-expertises)

Capgemini – (https://www.fr.capgemini.com/news/le-groupe-capgemini-lance-une-nouvelle-ligne-de-services-mondiale-dediee-a-la-cybersecurite)

**Autres :**

*Bull* (disque dur sécurisé, SPhone, …), travaille avec ERCOM (sécurisation des télécoms)

Les offres de sécurité sont souvent associées à une infogérance IaaS (Cloud).

<QuiFaitQuoi.xlsx>

1. **Etude quantitative**
   1. **Modèle économique**
   2. **Stratégie d’entrée sur le marché**
   3. **Garantie/Support**
2. **Annexes**

*Blog orange business services –LPM :*

<http://www.orange-business.com/fr/blogs/securite/lois-reglementations-standards-et-certifications/loi-de-programmation-militaire-les-operateurs-d-importance-vitale-en-ligne-de-mire-osd14>

**Importance de développer le marché français pour protéger nos entreprises et éviter toute fuite sur des logiciels principalement américains ou israéliens souvent de connivence avec leurs états**

*Gatewatcher :*

<http://www.globalsecuritymag.fr/GATEWATCHER-Une-solution-made-in,20150619,53686.html>

<http://www.gatewatcher.com/gatewatcher-intelligence-defense/>

*Regardez les profils linkedin pour se faire une idée des prestas ;*

[*https://www.linkedin.com/in/gladys-koskas-0aa09034?authType=NAME\_SEARCH&authToken=eSkG&locale=en\_US&trk=tyah&trkInfo=clickedVertical%3Amynetwork%2CclickedEntityId%3A119626114%2CauthType%3ANAME\_SEARCH%2Cidx%3A1-1-1%2CtarId%3A1463599175546%2Ctas%3AGladys%20Koskas*](https://www.linkedin.com/in/gladys-koskas-0aa09034?authType=NAME_SEARCH&authToken=eSkG&locale=en_US&trk=tyah&trkInfo=clickedVertical%3Amynetwork%2CclickedEntityId%3A119626114%2CauthType%3ANAME_SEARCH%2Cidx%3A1-1-1%2CtarId%3A1463599175546%2Ctas%3AGladys%20Koskas)

*Plaquette de formation sysdreams ;*

[*https://sysdream.com/files/catalogue-formations-2016.pdf*](https://sysdream.com/files/catalogue-formations-2016.pdf)

*Discussion sur les technos SIEM ;*

[*https://skizzlesec.com/2014/06/08/security-analysts-discuss-siems-elasticsearchlogstashkibana-vs-arcsight-splunk-and-more/*](https://skizzlesec.com/2014/06/08/security-analysts-discuss-siems-elasticsearchlogstashkibana-vs-arcsight-splunk-and-more/)

*Etude de marché secteur sécurité informatique ;*

[*http://www.xerfi.com/presentationetude/Le-marche-de-la-cybersecurite-en-France-et-dans-le-monde\_5SAE24*](http://www.xerfi.com/presentationetude/Le-marche-de-la-cybersecurite-en-France-et-dans-le-monde_5SAE24)

*Article SIEM, IDS ;*

[*http://connect.ed-diamond.com/MISC/MISC-069/SIEM-IDS-l-union-fait-elle-la-force*](http://connect.ed-diamond.com/MISC/MISC-069/SIEM-IDS-l-union-fait-elle-la-force)