



Introduction : Cybersécurité Objectifs, politiques et déploiement

Eric DUPUIS^{1,2*}

🕒 Résumé

Ce document donne les éléments d'introduction du domaine de la cybersécurité vous permettant de situer cette discipline dans l'environnement des technologies de l'information.

Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.

Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

🔑 Mots clefs

Cybersécurité, Définitions

¹ Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France

² RSSI Orange Cyberdefense

*email : eric.dupuis@lecnam.net – eric.dupuis@orange.com

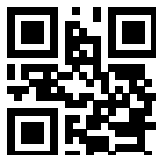
DRAFT NOTES 2020-2021

Vérifiez la disponibilité d'une version plus récente de

SEC101-C0a-Intro.doc.pdf sur GITHUB CYBERDEF ¹



2020 eduf@ction Publication en Creative Common BY-NC-ND



1. <https://github.com/edufaction/CYBERDEF/raw/master/Builder/SEC101-C0a-Intro.doc.pdf>



1. Avant propos

Chaque jour la presse se fait l'écho d'attaques et de piratages informatiques, de divulgations d'informations sensibles ou de fragilités découvertes dans les produits et services numériques. Derrière ces incidents, nous découvrons des menaces certaines fois complexes, des actions criminelles, étatiques ou activistes. Construire des systèmes sûrs, les protéger et les défendre, dans une société où accélérer la digitalisation est devenu un challenge quotidien pour les équipes spécialisées qui luttent contre ces menaces. La cybersécurité est un domaine de mythes et de légendes. Ses activités plongent au plus profond de notre histoire avec des luttes ancestrales entre le méchant et le gentil, le gendarme et le voleur, le corsaire et le pirate, en n'oubliant pas les luttes secrètes entre les espions et le contre-espionnage. Une thématique qui résonne, donc comme un domaine de romans, qui se traduit toutefois par une réalité souvent moins réjouissante pour les équipes chargées de la cybersécurité dans les entreprises. Les métiers de la cybersécurité sont nombreux, pour certains très techniques, d'autres plus fonctionnels, juridiques, ou managériaux.

La cybersécurité est, en effet, une discipline transverse et interdisciplinaire à plusieurs titres. Elle nécessite :

- ▶ de maîtriser les nombreuses techniques et technologies des systèmes d'information ainsi que leurs zones de fragilités ;
- ▶ de maîtriser de nombreuses solutions de sécurité permettant de couvrir, en n'oubliant qu'elles aussi peuvent être fragiles² ;
- ▶ de faire coopérer des métiers et des cultures différentes ;
- ▶ de gérer l'entreprise dans des cadres de conformité souvent complexes et coûteux ;
- ▶ d'intégrer ces démarches en tenant compte des cultures et des pratiques des nombreux métiers de l'entreprise.

Les métiers de la cybersécurité concourent tous à une seule et même mission : « **assurer la continuité de la mission ou du service en préservant le patrimoine de l'entreprise contre toute menace dans l'environnement numérique** ».

Ce sont des métiers de passion, des métiers extrêmement techniques pour partie, fortement marqués par le fonctionnel pour d'autres. S'il est vrai qu'une grande partie des experts du domaine sont issus de formations en informatique ou en électronique, les domaines d'expertises s'élargissent et font naître de nouveaux chemins d'excellence. On trouvera en particulier, des métiers issus du domaine juridique comme celui du Data Protection Officer.

2. cf. Certification et Qualification de produits de sécurité et Critères communs ??





FIGURE 1. Cybersécurité : un domaine hollistique

2. Aborder la cybersécurité

La cybersécurité ou la sécurité du numérique³ peut être découverte par de nombreuses voies.

La plus courante est certainement pour les technophiles, l'aventure passionnante de découvrir ce domaine par la technique, et le hacking. Longtemps abordé par le triptyque académique cryptologie, sécurité protocolaire des réseaux, et informatique fondamentale (compilation et théorie des langages, architecture système et bases de données), le domaine s'est vulgarisé avec une forme de gamification de l'apprentissage.

On y trouve en particulier :

- ▶ Les challenges comme les *Capture The Flag (CTF)*, ou les *Defend The Flag (DTF)* qui permettent de mettre le pied dans les techniques et stratégies d'intrusion pour les pentesteurs et auditeurs techniques en herbe ;
- ▶ Les bug-bounty qui permettent de se confronter à ses propres limites avec la recherche de failles dans les logiciels avec pour partie des rémunérations au niveau des difficultés ;

Toutefois, un volet peu enseigné, qui ne mobilise pas spécialement les jeunes apprenants du domaine concerne la gouvernance de cette sécurité numérique de l'entreprise.

J'ai souhaité m'intégrer dans une approche globale de la sécurité du numérique pas le

3. Historiquement d'autres termes sont utilisés comme Sécurité des Systèmes d'information (SSI) ou Sécurité Informatique



biais de quelques processus, en particulier ceux de la sécurité opérationnelle. L'enjeu est de fournir une trame de connaissances pour déployer des actions de cybersécurité en entreprise. Cette trame a pour intention de fournir des points d'accroche et des modèles de compréhension des différentes compétences, actions, et outils du large domaine de la cybersécurité.

Destiné à un public large, cet ouvrage tente d'offrir un niveau de lecture permettant à un expert technique de repositionner sa technicité dans un ensemble plus large, et à un débutant de découvrir de nombreuses facettes du domaine avec quelques éclairages techniques.

La cybersécurité dans une entreprise est une co-activité d'hommes de l'art. C'est aussi un domaine en perpétuelle évolution, soutenu et contraint par des lois, des règlements, des normes, des méthodologies, des technologies spécialisées et en particulier des expertises. Il nécessite pour être efficace d'être orchestré pour maintenir en condition de sécurité une organisation dont le périmètre peut être complexe face à des menaces elles aussi en perpétuelles évolutions.

Il y a de nombreuses manières d'aborder le pilotage de la cybersécurité au sein de l'entreprise, et nombreux ouvrages spécialisés en détaillent les concepts et les méthodologies. Nous avons toutefois délibérément choisi ici de confronter, si ce n'est corrélér, dans un seul support, trois domaines qui apparaissent souvent dans la littérature comme des domaines d'expertise différents : la gestion des risques, la gouvernance de la cybersécurité et la cybersécurité opérationnelle.

Nous avons donc fait ce choix de structurer notre approche suivant le prisme de la cyberdéfense d'entreprise avec une analyse en trois axes majeurs qui résument les difficultés dont relève cette discipline holistique (**sch13**).

2.1 Politiques versus stratégies

La figure 2 présente la dynamique avec laquelle nous avons structuré ce document. De l'**analyse de risque**, nous pouvons déduire et/ou modifier des politiques de sécurité adaptées. Sur la base de l'existant, il est alors possible d'adapter ou simplement de mieux utiliser ou configurer les architectures techniques et organisationnelles pour définir un niveau de protection attendu. Il y a malheureusement toujours un écart entre les mesures de sécurité souhaitées et la réalité des mesures déployées. Que ce soit des défauts de configuration, des délais de mise en place plus longs que prévu, le système n'est que très rarement au niveau décrit dans les éléments de spécification ou les documents d'assurance sécurité. Mesurer ce niveau, analyser les écarts et remédier relève d'un des grands thèmes de la gouvernance sécurité. Il reste à lui seul un consommateur à plus de 30% des charges d'activité de cette gouvernance.

Après avoir défini des **politiques de sécurité** et mesurer leur déploiement dans l'environnement de l'entreprise, il n'en demeure pas moins que l'ennemi est toujours à ses portes et de plus en plus souvent. Il arrive à pénétrer le périmètre de sécurité. Non pas que les barrières et filtre de l'entreprise ne sont plus efficaces mais simplement parce que l'atta-



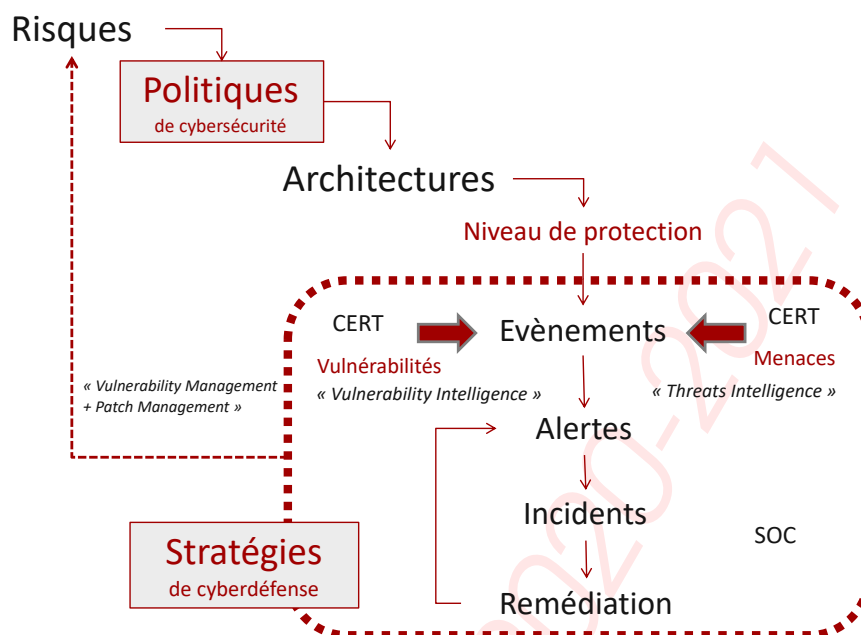


FIGURE 2. Processus Cyber d'entreprise

quant change plus souvent de stratégie que l'entreprise de politique. La sécurité se doit d'être plus dynamique. L'entreprise doit faire face à des attaquants qui ne raisonnent pas sous forme de politiques d'attaque, mais en stratégie d'action. L'entreprise doit raisonner aussi de la même manière pour se défendre. C'est à ce titre que l'on parle de stratégie de Cyberdéfense. C'est avec des stratégies de « cyberdéfense » que nous aborderons les moyens organisationnels et techniques à mettre en place.

Vous trouverez dans ce document une terminologie qui peut être certaines fois éloignée des expressions classiques de la sécurité informatique. J'ai choisi d'utiliser et mixer sans trop de complexes des termes et concepts issus du monde militaire (renseignement, tenir une position, infiltration ...) et de nombreux autres issus de l'univers médical (infection, épidémie, comportement). Ces incursions dans les analogies d'autres champs professionnels, bien que présents pour illustrer certains concepts, n'en demeurent pas moins justifiés par leurs usages de plus en plus répandus dans le monde de la cybersécurité. Par ailleurs, les termes sécurité et cybersécurité pourront être utilisés indifféremment dans le corps de ce document.

2.2 Transformation numérique

La cybersécurité est devenue en quelques années un axe fondamental dans la prise en compte de ces nouveaux risques sociétaux qu'apporte l'informatique au cœur de chaque activité sociale, économique ou politique.

Les transformations digitales d'une grande partie des acteurs économiques apportent de nouveaux risques. Les modifications des conditions d'utilisation des technologies dans



les crises comme celle du COVID-19 engendrent aussi des risques globaux réduisant les frontières entre les espaces professionnels et les espaces privés.

Le législateur s'en est saisi depuis bien des années avec de nombreuses réglementations et lois permettant de protéger en particulier, le citoyen et l'Etat.

On notera en particulier dans cette évolution du cadre réglementaire, la protection des données personnelles, mais aussi la protection des systèmes sensibles stratégiques⁴ en lien avec la protection de la nation avec la dynamique de Cyberdéfense soutenue par les différentes lois de programmation militaire depuis 2008. L'entreprise se trouve quant à elle prise en sandwich entre les exigences de l'état et les désirs de liberté que défend le citoyen. Il faut aussi noter que le salarié est souvent un citoyen et son rôle dans la cybersécurité de l'entreprise peut soulever des problématiques complexes⁵.

Se sentir en sécurité dans un monde de transformation digitale c'est bien entendu disposer des moyens de se protéger et protéger son patrimoine, que ce dernier soit ou non informationnel, mais aussi de le défendre en continu. Il est de moins en moins accepté de le protéger, en érigeant des murs épais, solides et supposés infranchissables. L'entreprise a besoin de faire circuler rapidement les savoirs, de partager largement des informations entre les salariés, les clients, les citoyens, les fournisseurs...

Il est donc nécessaire de correctement définir les biens vitaux ou essentiels pour y mettre les meilleurs moyens pour les défendre. Par ailleurs comme toute activité protégée et défendue qui peut subir des dommages, il est important de structurer l'activité numérique d'une entreprise ou d'une organisation pour pouvoir fonctionner en mode dégradé, et revenir à la normale en moins de temps possible.

Entre une maîtrise des risques cyber et une capacité de se défendre et réagir, il est nécessaire de disposer déjà d'un bon niveau de protection adaptée aux enjeux du numérique. Il existe de nombreuses définitions de cette cybersécurité.

Pour ma part je vous propose de poser pour la suite de mon propos, une définition simple, qui fait consensus et résume en une pseudo équation la manière dont nous traiterons ce domaine dans ce cours.

Une définition de la cybersécurité :

$$\text{Cybersécurité} \cong \text{Cyberprotection} \oplus \text{Cyberdéfense} \oplus \text{Cyberrésilience} \quad (1)$$

La cybersécurité est l'enchaînement opéré, organisé, documenté, piloté, optimisé de trois environnements d'actions :

- ▶ **Protéger** l'environnement par les mesures et solutions technologies adaptées au niveau de risque que l'entreprise est prête à prendre ;
- ▶ **Défendre** les actifs les plus sensibles de l'entreprise en surveillant et combattant la menace (y compris l'image de l'entreprise) ;

4. Opérateur d'Infrastructures Vitales (OIV) et Opérateur de Services Essentiels (OSE)

5. Lanceurs d'alertes, comportements déviants des utilisateurs légitimes



- assurer **la continuité et la reprise d'activité** de l'entreprise face à tout incident rendant indisponible tout ou partie d'une fonction essentielle de celle-ci.

La Cybersécurité, est donc, avant-tout, le déploiement de mécanismes de protection des biens et des processus numériques sensibles. C'est avec cette première dynamique que l'entreprise déploie en premier lieu des solutions de sécurité.

Toutefois, malgré ce niveau de protection et souvent les lourds investissements réalisés dans des composants de sécurité périmétrique, l'entreprise peut se faire surprendre avec des attaques contournant ces mesures. Face à ces attaques, l'entreprise découvre que la solidité de l'entreprise n'est pas directement liée aux investissements sur les systèmes de protections. Il lui faut anticiper les menaces, les détecter non seulement sur son périmètre mais aussi dans l'écosystème de l'environnement des menaces potentielles. Ces menaces exploitent des vulnérabilités qu'il convient de détecter en amont.

Malheureusement, malgré ces mesures de protection et de défense qui permet de réagir vite et efficacement, il arrive que des attaques informatiques arrivent à leurs fins. La capacité de l'entreprise à revenir à une situation normale, avec un contexte assaini est un critère dont un chef d'entreprise appréciera la valeur **qu'après un incident**.

Il fut une époque pas si lointaine, ou dans l'évaluation de la probabilité d'une attaque, l'analyste consacrait du temps. Aujourd'hui bien que ce paramètre continue quand même à être pris en compte, l'analyste positionne cette probabilité ou vraisemblance à 100%. (cf. figure 3)

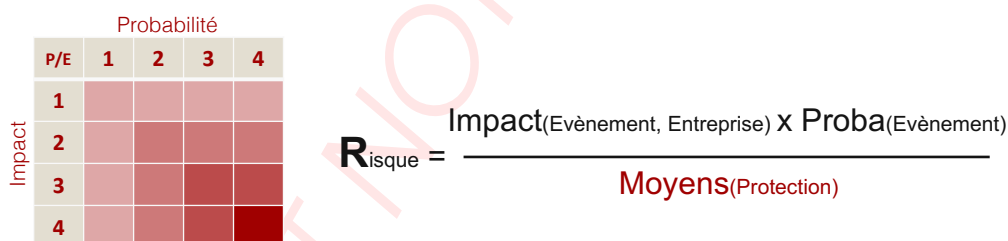



FIGURE 3. le cyber-risque

L'ensemble des experts du domaine est globalement en accord sur la posture que doivent prendre les entreprises et les organisations : « Le temps n'est plus de savoir si on sera attaqué ou pas, mais plutôt de savoir quand et comment on le sera », qui concrètement se résume à la certitude que tout incident de sécurité peut se produire.

Dans les modèles d'analyse de risque et d'évaluation de la cybersécurité, l'analyste se positionne aujourd'hui du point de vue de l'attaquant. Ce regard lui permet de mieux comprendre la menace comme équation duale du risque, mais vu de l'énergie dépensée par l'attaquant et du risque qu'il prend. (cf. figure 4)





$$M_{\text{ menace }} = \frac{\text{Valeur}_{(\text{Cible})} \times \text{Fragilités}_{(\text{Entreprise})}}{\text{Moyens}_{(\text{Attaque})} \times \text{Risques}_{(\text{Attaquant})}}$$

FIGURE 4. La menace : une vision de l'attaquant

3. Sécurité du système d'information

Le système d'information est au coeur de ce « monde digital », et il est le lieu d'activités humaines très denses, permettant à des utilisateurs de réaliser leurs activités, professionnelles ou privées, à l'aide de processus informatiques et de services.

Ces activités doivent de plus en plus faire face à tout un système d'agression orchestré par des attaquants non seulement humains mais aussi « automatiques ». On observe aujourd'hui une multitude de situations critiques, incertaines dont l'occurrence quasi quotidienne provient de phénomènes variés, humains (isolés, en réseau, ...), physiques et/ou technologiques. Parmi ces difficultés qui profitent aux pirates informatiques il y a de nombreuses failles ou fragilités que nous découvrirons, provenant des systèmes du SI sans lesquelles ils ne pourraient exploiter leurs attaques. Ces phénomènes sont une menace pour les conditions de sécurité du système d'information.

3.1 Gouvernance et conformité

⚙️ chapitre en cours de rédaction, DRAFT non publiable ⚙️

3.2 SECOPS et lutte contre la malveillance

⚙️ chapitre en cours de rédaction, DRAFT non publiable ⚙️

3.3 Les fonctions SSI de gouvernance

Au sein des grandes entreprises, il existe de nombreuses fonctions ou missions pour gouverner, piloter cette sécurité numérique.

Nous ne présentons rapidement ici que ceux qui seront utilisés directement dans ce document et qui sont fortement en liaison avec la sécurité des systèmes d'information.

3.3.1 Les DSSI et RSSI

Au sein de l'entreprise, il est important que quelqu'un porte la charge de suivre ces conditions de sécurité. C'est le rôle du RSSI (Responsable de la sécurité des systèmes d'information), ou DSSI (Directeur de la sécurité des systèmes d'information). La mission de ce RSSI d'entreprise est de protéger son Système d'Information (SI), de le mettre dans une posture d'amélioration continue tant de son système de protection que de son système de



défense. Le RSSI n'est pas seul pour assumer ces missions, à tous les niveaux de l'entreprise, s'organise des fonctions de sécurité tant au sein de la DSI (auquel est souvent rattaché le RSSI), qu'au sein d'autres activités de l'entreprise.

3.3.2 Le DPO

A partir de mai 2018, une responsabilité plus juridique liée à la protection des données a été rendue plus visible avec la nécessité de disposer d'un Data Protection Officer (DPO) en entreprise (Data Protection Officer) héritier en France *Correspondant Informatique et Liberté (CIL)*. Nous n'aborderons pas la fonction, les missions et la dynamique de responsabilité du DPO ici. Il faut toutefois que cette fonction possède de nombreux recouvrements dans la chaîne de gouvernance du risque « informatique » auprès des directions d'entreprise. Orienté vers la protection des données à caractère personnel, le tropisme de la fonction DPO peut conduire certaines structures à oublier des pans importants des risques numériques comme :

- ▶ la protection du patrimoine informationnel. (Espionnage industriel).
- ▶ la protection des systèmes d'information contre les risques de ruptures de services (Continuité d'activité)

3.3.3 L'officier de sécurité de défense

Pour les entreprises traitant des informations classifiées de défense ou liées aux contraintes de la classification de l'état, il est indispensable de se doter d'une fonction Officier de sécurité (OS) de défense. Son rôle est de s'assurer de la conformité à l'Instruction Générale Interministérielle IGI 1300 pour le « Confidentiel Défense » et l'Instruction Interministérielle II901 pour le « Diffusion Restreinte ».

Nous resterons donc dans le cadre fonctionnel de la Cybersécurité dans son volet protection des Systèmes d'information et gestion des risques numériques. Quand nous aborderons des sujets en forte adhérence avec les dynamiques de la General Data Protection Regulation ou RGPD Règlement général sur la protection des données (GDPR) nous donnerons les liens et les indications adaptés pour les DPO. Par exemple, nous aborderons l'usage des données nominatives collectées et traitées dans les System Incident and Event Management (SIEM), ou celles recueillies sur le DarkWeb etc ...

Consulter le site www.cnil.fr pour parfaire ses connaissances en matière de réglementation européenne sur la protection des données personnelles.

3.3.4 Responsabilités SSI

Le maintien des conditions de sécurité du système d'information des grandes entreprises nécessite un Responsable de la sécurité des systèmes d'information (RSSI) Central ou une fonction semblable rattachée à un niveau plus global de l'entreprise. On découvre ainsi des RSSI rattachés à la direction des risques, la direction générale, au contrôle interne ... Il n'y a pas de rattachement bien défini. La couverture de responsabilité dépend grandement de la taille et de l'activité de l'entreprise, mais aussi de la maturité de celle-ci en matière



de gestion de risque et de gouvernance. Il peut y avoir des RSSI par entité, par projet à l'intérieur d'une entreprise. Leur mandat est fixé en fonction des enjeux sécurité de ces entités ou ces projets.

Le fin mot de l'histoire est le « R » de RSSI. Son domaine de responsabilité dépendra de son mandat pour assumer ce rôle de garant d'un environnement « possédant » des bonnes conditions de sécurité. La gouvernance de la sécurité, est au coeur du métier du RSSI. Cette discipline que ce dernier pilote dans l'entreprise se nomme Gouvernance Risques et Conformité (GRC).

La notion de système d'information a profondément évoluée ces dernières années. Le périmètre des risques digitaux inclut maintenant des systèmes et services externes à l'entreprise. Beaucoup d'entre eux sous la forme de réseaux sociaux, de services cloud ouvrant par ailleurs le domaine de supervision à la téléphonie avec les smartphones et leurs applications professionnelles ou non.

Bien entendu en fonction de la taille de l'entreprise et de ses enjeux, on peut disposer au sein de l'entreprise de nombreuses personnes ayant une fonction de RSSI.

Le métier est riche et dispose d'un spectre de responsabilité et d'activité très large en terme de poste on y trouve par exemple :

- ▶ **RSSI d'entreprise** : Responsable de la sécurité de sa structure.
- ▶ **RSSI d'un département, d'une organisation intermédiaire** : A l'image d'un RSSI d'entreprise, il assure toute les tâches de gouvernance, il applique et fait appliquer les directives et politique de sécurité aux équipes du département / division / structure intermédiaire, il déploie les actions décidées dans la chaîne fonctionnelle sécurité
- ▶ **RSSI d'un contrat, d'un projet contractualisé (Security Manager)** : Responsable de la sécurité du déroulement d'un contrat. Souvent lié à un plan d'assurance sécurité, le RSSI contrat se doit d'assurer pour le client ou pour le fournisseur le suivi des exigences de sécurité du contrat.
- ▶ **RSSI Projet** : La responsabilité sécurité couvre le projet, on parle souvent de « security by design ». La responsabilité dans ce type de poste recouvre l'intégration de la sécurité dans le système, le suivi des indicateurs définis (contractuels, ou réglementaires), la remontée des indicateurs de suivi de sécurité à la MOA (Maitrise d'ouvrage), la prise de décision autour des choix de sécurité
- ▶ **RSSI Produit / Service** : Au delà de ce qui est fait pour un projet, le RSSI produit a en charge de gérer la sécurité opérationnel c'est à dire Maintenir la sécurité de son produit ou de son service.
- ▶ **RSOP** : Le responsable sécurité opérationnelle, est souvent un RSSI dépendant d'une DSI, il est généralement et dans beaucoup de d'entreprise de taille moyenne le RSSI technique. Il assure opérationnellement la mise en place technique des politiques de sécurité et maintien en condition de sécurité l'ensemble de l'environnement informatique. Il est aujourd'hui au coeur de la sécurité opérationnelle face aux attaques et aux crises cyber.



3.4 Maintien en condition de sécurité

Les conditions de sécurité représentent les propriétés fondamentales du SI, appelées : Disponibilité, Intégrité, Confidentialité, Traçabilité (DICT) , qui favoriseront le fonctionnement optimisé du SI et éviteront l'avènement d'incidents de sécurité irréversibles ou même gênants pour son fonctionnement. D'un certain point de vue, les conditions de sécurité représentent le paramétrage du SI pour lequel le système fonctionne bien dans des conditions de sécurité « connues et approuvées ».

Ces fameux critères **DICT** ou propriétés de sécurité des systèmes d'information visent les objectifs suivants :

👁 **DISPONIBILITE** : le système doit fonctionner sans faille (arrêt, ou dégradation) durant les plages d'utilisation prévues et garantir l'accès aux services et ressources définies et installées avec le temps de réponse attendu.

👁 **INTEGRITE** : Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

👁 **CONFIDENTIALITE** : Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

👁 **TRACABILITE** : (ou preuve) : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité tels que :

👁 **AUTHENTICITE** : l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange. On voit aussi dans la littérature la terminologie « critères Authentification, Confidentialité, Intégrité, Disponibilité (ACID) (Authentification, Confidentialité, Intégrité, Disponibilité) ».

👁 **NON-REPUDIATION** : La non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Dans un contexte d'activité économique dense et en perpétuel renouvellement, les conditions de sécurité sont aussi en perpétuelle évolution, c'est pourquoi nous parlons d'un cycle de vie vertueux au cours duquel les nouveaux paramètres tirent profit des expé-



riences passées. Ainsi, l'amélioration continue également appelée « lean management » dans d'autres domaines (industrie, ...) travaille elle sur le cycle de vie des conditions de sécurité souvent appelé Plan, Do, Check, Act (Roue de Deming) (PDCA). Ce cycle de vie doit néanmoins être maîtrisé par le RSSI en place avec ses équipes, il faut co-produire ces conditions de sécurité, cette maîtrise est complexe, fortement dépendante du contexte de l'entreprise, c'est pourquoi elle doit être accompagnée d'une méthodologie rigoureuse et partagée qui constitue le savoir-faire de base du RSSI et de son équipe. Par ailleurs, parmi ces conditions, certaines sont universelles et d'autres propres à chaque entreprise. Comme le montre le diagramme 5, il est possible aussi d'utiliser un cycle de vie sécurité de type projet, qui se rapproche par ailleurs de la manière dont nous avons structuré ce document.

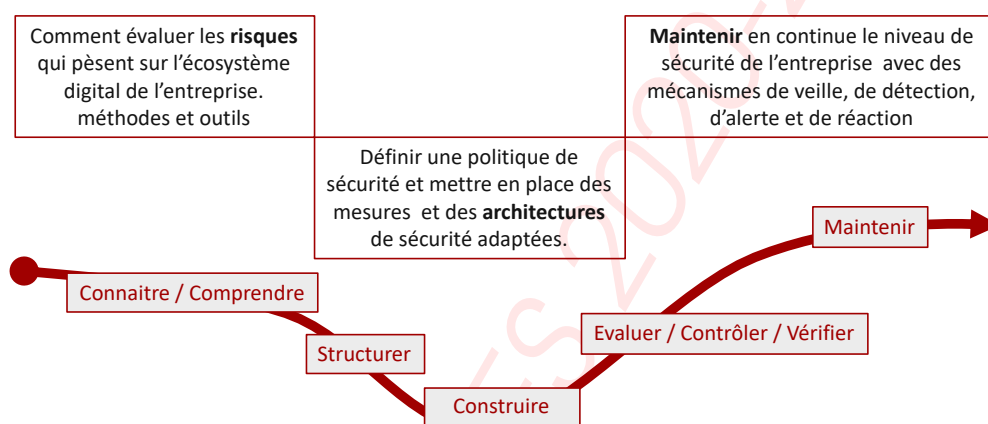


FIGURE 5. Cycle de vie sécurité dans les projets

Dans cette optique, ce cadre méthodologie a été défini par le sous-comité 27 de l'ISO, par l'ensemble de normes ISO 27x. Il s'agit également d'un ensemble de bonnes pratiques, qu'un RSSI peut suivre au travers de trois volets fondamentaux qui constituent les référentiels utilisés pour ce cours sur la cybersécurité. La norme 27001 est en particulier un cadre pour organiser la dynamique de la mise en condition de sécurité de l'entreprise et son maintien dans le temps. Cet environnement que le « RSSI » doit bâtir est le système de management de la sécurité (« SMSI »). Notre dynamique méthodologique est soutenue dans ce document, par trois cadres normatifs :

- ▶ Identifier ses cyber-risques sur la base de méthodologies que l'on retrouve dans l'environnement ISO/CEI 27001/27005 mais aussi sur la méthodologie Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) de l'ANSSI (Méthode EBIOS RM en particulier) ;
- ▶ Elaborer une politique de cybersécurité sur la base des cadres ISO/CEI 27001 et 27002, en n'oubliant pas les architectures de sécurité et la sécurité des architectures associées ;
- ▶ Détecter en amont des attaques et savoir réagir à ses cyber-incidents en se basant sur ISO 27035 et sur la continuité d'activité avec l'ISO 22301 et 27031.



👁 **Pourquoi des normes dans ce document ?** : L'objectif de ce document, n'est pas de présenter en détail un cadre normatif, mais bien de les utiliser pour ce qu'elles sont : des langages communs permettant d'appréhender une terminologie, des méthodologies, des outils. L'ISO 27001 comporte un grand nombre de normes (plus de 50...) qu'il convient de connaître comme outils terminologiques et de référence. Leur maîtrise nécessite une spécialisation le plus souvent demandée pour des métiers de conseil ou d'implémentation pour une certification.

Ces documents définissent un cadre méthodologique et normatif pour définir, créer, élaborer maintenir, améliorer les conditions ou les critères de sécurité pour le fonctionnement du système protégé et surveillé. Ils permettent aux acteurs de l'entreprise évoluant autour du métier RSSI un cadre méthodologique ainsi qu'un « how to » du maintien en conditions de sécurité. C'est en particulier au travers de ces trois axes que la mission de RSSI repose. Le nombre d'entreprises prêtes à accueillir des spécialistes de ce savoir-faire est en forte augmentation car les PME/PMI ont pris conscience que la sécurisation de l'entreprise est devenu primordiale pour « survivre » dans l'écosystème digital de nos sociétés modernes. Les contraintes légales issues de la Loi de Programmation Militaire (Loi de programmation militaire), de la Règlementation pour la Protection des Données Personnelles (RGPD), de la directive NIS nécessitent de disposer d'une vision globale et transverse tant technique, qu'organisationnelle ou humaine de la cybersécurité.

Nous tenterons donc dans le suite du cours, de vous donner des contextes d'usages de ces cadres normatifs indispensables pour aborder la cybergdéfense d'entreprise.

4. Enjeux légaux

Beaucoup d'environnements normatifs sont issus de la pression des différents cadres législatifs sur le marché. Que ce soit avec la pression du grand public ou avec les enjeux stratégiques et économiques des pays, ces lois organisent profondément les modes de gouvernance de la sécurité en entreprise.

4.1 Quelques cadres législatifs d'influence


Parmi les grandes lois qui ont influencées le monde de la sécurité des entreprises ces dix dernières années :

- ▶ En France, le cybergdéfense est largement orientée par les différentes « Lois de programmation militaire » avec des directives nationale de sécurité par grands domaines d'infrastructures vitales.
- ▶ En Europe deux grandes directives ont donné plus de responsabilités aux entreprises dans l'engagement sécurité avec GDPR et NIS qui sont déclinés en droits français via la CNIL, et l'ANSSI. On notera par ailleurs la montée en puissance dans la confiance numérique avec le cadre de certification européen.
- ▶ Aux Etats Unis, le *Cloud security Act*, a bouleversé la vision des risques numériques des états avec les potentielles nuisances liées à l'extraterritorialité de lois américaines




- ▶ En Russie et en Chine, plusieurs lois autour de l'usage d'internet interpellent les entreprises et en particulier celles du numérique sur la protection des données de leurs clients ou utilisateurs de leurs services.

4.2 Le cadre de certification européen

Le règlement établit un cadre européen de certification ⁶ de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification, au sein duquel l'ENISA trouve toute sa place. Les certificats délivrés bénéficieront d'une reconnaissance mutuelle au sein de l'Union européenne (UE).

4.3 Cyberdéfense et loi de programmation militaire

Pour ceux intéressés par les contraintes et cadre généraux de la cyberdéfense au sein des lois de programmation successives (2008, 2013, 2019 ...) il est conseillé d'aller voir sur le site de l'ANSSI. Les différentes LPM ont fait évoluer le cadre réglementaire pour assurer à la France une capacité de défendre la continuité de l'état et des infrastructures vitales du pays (Cf. Opérateurs d'infrastructures vitales) ⁷.

5. Quelques organismes de référence

Pour l'entreprise la cybersécurité est un domaine de nombreux cadres normatifs et réglementaires soutenus bien souvent par contraintes législatives propres à chaque pays.

Cette normalisation et ses réglementations sont riches mais certaines fois complexes. Le plus simple pour s'enrichir de ces savoirs et surtout pour disposer des meilleures informations à la sources autant « fréquenter » les sites internet institutionnels des organismes qui sont et continuent à être les points de référence dans le domaine de cybersécurité.

De nombreux services étatiques et de normalisation possèdent des activités dites Cyber dans leur structures :

- ▶ Organismes français : AFNOR, Cert FR, CNIL, HADOPI, ANSSI, DGSE, DGSI, DGA/MI, Commandement de la cyberdéfense, C3N, OCLCTIC, BEFTI ...
- ▶ Organismes internationaux : ISO, ETSI, CERT, Europol, Interpol, ENISA, FIRST ...
- ▶ Organismes étrangers : FBI, CIA, NSA, GCHQ, Unité 8200, Fapsi, The SANS institute, CISA ...

Je vous propose de donner quelques pointeurs par portée sur des organismes de référence du point de vue occidental.

5.1 International et Etats-Unis

Au niveau international, on ne peut éviter les Etats-Unis, un pays qui oeuvre fortement dans le domaine des standards.

6. <https://www.ssi.gouv.fr/entreprise/reglementation/cybersecurity-act-2/le-cadre-de-certification-europeen>

7. <https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/>




5.1.1 Le NIST

Le National Institute of Standards and Technology, ou NIST est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards avec l'industrie.

- ▶ NIST COMPUTER SECURITY RESOURCE CENTER ⁸
- ▶ NIST INFORMATION TECHNOLOGY LABORATORY ⁹

On notera en particulier les référentiels cryptographiques du NIST et ceux liées à la cyberdéfense en particulier avec le *CyberSecurity Framework*

5.1.2 SEI : Université de Carnegie Mellon

Le Software Engineering Institute (SEI) est un centre de recherche-développement financé par des fonds fédéraux et placé sous le parrainage du département de la Défense des États-Unis; son fonctionnement incombe à Carnegie Mellon University. Le SEI travaille avec des organisations pour apporter des améliorations significatives à leurs capacités d'ingénierie logicielle en leur fournissant le leadership technique afin de faire progresser la pratique de l'ingénierie logicielle. Le CERT Division du SEI est l'entité qui fait autorité et cherche à améliorer la sécurité et la résilience des systèmes et réseaux en particulier dans le domaine du logiciel (Carnegie Mellon University - Cybersecurity research ¹⁰).

5.1.3 l'ISO : International Organization for Standardization

L'ISO est une Organisation Internationale participant à l'élaboration de Standards. En ce sens la conformité à une norme a l'avantage d'être reconnue internationalement.

Les normes de la famille ISO 27000 permettent d'organiser et structurer la démarche de la gestion de la sécurité des systèmes d'information, une grande famille de normes avec des positionnements sur l'ensemble du spectre de la sécurité des systèmes d'information :

- ▶ ISO 27001 décrit les processus permettant le management de la sécurité de l'information (SMSI);
- ▶ ISO 27002 présente un catalogue de bonnes pratiques de sécurité;
- ▶ ISO 27003 décrit les différentes phases initiales à accomplir afin d'aboutir à un système de Management tel que décrit dans la norme ISO 27001;
- ▶ ISO 27004 permet de définir les contrôles de fonctionnement du SMSI;
- ▶ ISO 27005 décrit les processus de la gestion des risques;
- ▶ ISO 27006 décrit les exigences relatives aux organismes qui auditent et certifient les SMSI des sociétés.

Nous aborderons dans le chapitre sur les politiques de sécurité, l'usage de ce cadre normatif dans la gouvernance globale de la cybersécurité au sein de l'entreprise


8. <https://csrc.nist.gov/>

9. <https://www.nist.gov/itl/fips-general-information>

10. <https://www.sei.cmu.edu/research-capabilities/cybersecurity/>



5.2 Europe


Au niveau européen, le règlement (CE) 460/2004 du Parlement européen et du Conseil du 10 mars 2004 a institué l'Agence européenne chargée de la sécurité des réseaux et de l'information Agence européenne chargée de la sécurité des réseaux et de l'information ENISA ¹¹. Son rôle est de :

- ▶ Conseiller et assister la Commission et les États membres en matière de sécurité de l'information et les aider, en concertation avec le secteur, à faire face aux problèmes de sécurité matérielle et logicielle.
- ▶ Recueillir et analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents.
- ▶ Promouvoir des méthodes d'évaluation et de gestion des risques afin d'améliorer notre capacité de faire face aux menaces pesant sur la sécurité de l'information.
- ▶ Favoriser l'échange de bonnes pratiques en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées.
- ▶ Suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information.

5.3 France

En France, la Cybersécurité est pilotée par un organisme dépendant des services du 1er Ministre, l'Agence National des Systèmes d'information (Agence Nationale de la Sécurité des systèmes d'information (ANSSI)). L'ANSSI possède plusieurs rôles de fait. C'est un « régulateur » c'est à dire qu'elle définit des cadres réglementaires pour les entreprises mais c'est aussi une agence qui édicte des préconisations et des guides.

Le site de l'agence ¹² est riche en information et guide sur la cybersécurité.

Dépendant aussi de l'état, la CNIL ¹³ (Commission National Informatique et Liberté) est une autorité dont la mission est de protéger le citoyen. Avec l'avènement du règlement de protection des données personnelles, la Commission National Informatique et Liberté (CNIL) a vu son pouvoir étendu.

Il faut aussi citer l'AFNOR Association Française de Normalisation (AFNOR), qui relaie en France la normalisation internationale dont l'ISO au delà de ses actions de normalisation purement françaises.

11. <https://www.enisa.europa.eu>






12. <https://www.ssi.gouv.fr/agence/cybersécurité/ssi-en-france/>

13. <https://www.cnil.fr/>



6. Quelques associations et groupements professionnels

A titre d'information, vous trouverez en France aussi quelques clubs et associations historiques de la sécurité de systèmes d'information qui offrent à leurs adhérents des lieux d'échanges très intéressants et publient régulièrement :

- ▶ **Observatoire de la Sécurité des Systèmes d'Information et des Réseaux** (Technique) OSSIR ¹⁴, association plutôt technique, qui propose de nombreux échanges sur la cybersécurité et existant depuis les années 90.
- ▶ **Club de la sécurité de l'information Français** (Gouvernance) CLUSIF ¹⁵, association qui propose de nombreux échanges sur la cybersécurité.
- ▶ **Club CyberEdu** (Education) CyberEdu ¹⁶, issu des travaux sur la formation des enseignants en cybersécurité de l'ANSSI, l'association regroupe les écoles et les utilisateurs des travaux de CyberEdu.
- ▶ **Club HexaTrust** (Editeurs de produits et services de cybersécurité Français) HexaTrust ¹⁷, regroupe les éditeurs et fournisseurs de services français en cybersécurité.
- ▶ **Club des Experts de la sécurité de l'Information et du Numérique**. (Club de RSSI) le CESIN ¹⁸ est une association regroupant les RSSI d'entreprises, l'adhésion à cette association nécessite un parrainage et vous devez être RSSI.

14. <https://www.ossir.org/>

15. <https://clusif.fr>

16. <https://www.cyberedu.fr>

17. <https://www.hexatruster.com/le-club/>

18. <https://www.cesin.fr>



7. Contributions

7.1 Comment contribuer

Les notes et les présentations sont réalisées sous \LaTeX .

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- ▶ Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- ▶ Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) ¹⁹. Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes. Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

7.2 Les contributeurs/auteurs du cours

7.2.1 co-auteurs

(2019-2020) **David BATANY** - Cnam SEC101 : *Architecture et fonctionnement des Botnets*

7.2.2 contributeurs

(2020) **Céline JUBY** - Orange Cyberdefense : *Contributions d'amélioration et relectures*

¹⁹. <https://github.com/edufaction/CYBERDEF>



Table des matières

1	Avant propos	2
2	Aborder la cybersécurité	3
2.1	Politiques versus stratégies	4
2.2	Transformation numérique	5
3	Sécurité du système d'information	8
3.1	Gouvernance et conformité	8
3.2	SECOPS et lutte contre la malveillance	8
3.3	Les fonctions SSI de gouvernance	8
3.3.1	Les DSSI et RSSI	
3.3.2	Le DPO	
3.3.3	L'officier de sécurité de défense	
3.3.4	Responsabilités SSI	
3.4	Maintien en condition de sécurité	11
4	Enjeux légaux	13
4.1	Quelques cadres législatifs d'influence	13
4.2	Le cadre de certification européen	14
4.3	Cyberdefense et loi de programmation militaire	14
5	Quelques organismes de référence	14
5.1	International et Etats-Unis	14
5.1.1	Le NIST	
5.1.2	SEI : Université de Carnegie Mellon	
5.1.3	l'ISO : International Organization for Standardization	
5.2	Europe	16
5.3	France	16
6	Quelques associations et groupements professionnels	17
7	Contributions	18
7.1	Comment contribuer	18
7.2	Les contributeurs/auteurs du cours	18
7.2.1	co-auteurs	
7.2.2	contributeurs	

Table des figures

