PÔLE D'EXCELLENCE

CYBER

RÉFÉRENTIEL CYBER

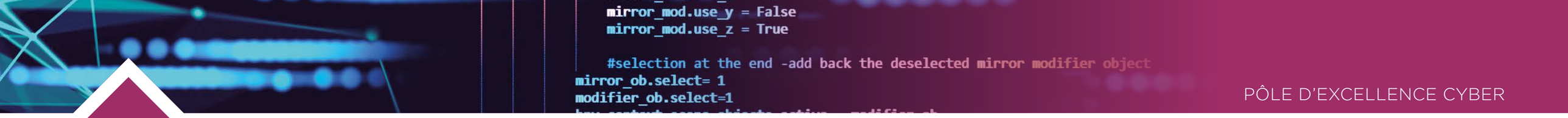
V5.0

NOVEMBRE 2019

Région BRETAGNE

MINISTÈRE DES ARMÉES

CYBER DÉFENSE



Sommaire

Editorial

Lors de son discours de Rennes en date du 3 octobre 2019 la ministre des Armées, a rappelé les ambitions de la France dans le domaine de la cyberdéfense et le rôle dévolu au Pôle d'excellence Cyber (PEC) dans le dispositif global.

Le Pôle poursuit son travail de fédération, d'animation et de décloisonnement pour répondre à trois enjeux principaux : le développement des formations, la structuration d'une filière, l'accompagnement de l'innovation dans les offres de service et les produits de confiance.

Ces enjeux mobilisent l'ensemble des membres et partenaires du Pôle d'excellence cyber, instituts de recherche, de formation, PME, grands groupes industriels, ministère des Armées et région Bretagne.

Leur rencontre fait naître des opportunités et des synergies, porteuses de projets concrets.

Le Pôle d'excellence cyber présente par ce document le fruit d'un de ces groupes de travail en charge de proposer et de maintenir à jour un référentiel pour le domaine de la cyberdéfense.

Élaboré par un panel d'experts privés et étatiques, du monde de la recherche, de la formation, de la défense ou de l'industrie, ce document décrit, en particulier, les différentes composantes de la cybersécurité, que ce soit pour les technologies et services, les domaines fonctionnels ou les cas d'usage et permet d'y entrevoir les enjeux associés.

Il se veut pragmatique et utile aux différents acteurs du domaine pour leur permettre de se positionner dans ce paysage en recomposition permanente et d'identifier les enjeux et les opportunités de développement associés.

Outil de dialogue et de concertation, il a vocation à évoluer régulièrement, tant pour tenir compte des nouvelles technologies et des nouveaux usages que pour s'enrichir des remarques et des propositions de tous ses lecteurs.

Il est un document essentiel de partage au sein du Pôle pour permettre aux acteurs par nature très différents de se comprendre et ainsi de pouvoir travailler ensemble.

Il est un bien commun, mis à la disposition de la communauté nationale et européenne de cyberdéfense, pour contribuer à l'ambition d'un développement d'une « cyber vallée européenne » souhaitée par la ministre des Armées.

Philippe Verdier
Président du Pôle d'excellence cyber

Remerciements

Le Pôle d'excellence cyber tient à remercier les personnes suivantes qui ont contribué à la préparation et à l'élaboration de ce référentiel en fournissant soutien, expertise et conseils clés :

Michel Corriou
Directeur des Opérations
b<>com

Patrick Erard
Délégué général adjoint du Pôle d'excellence cyber

Jean-Marc Jezequel
Directeur de l'IRISA
Professeur à l'Université de Rennes I

Jean-Pierre Lebee
Direction générale de l'armement

Gérard Le Bihan
Directeur général du pôle Images et réseaux

Gilles Michalon
Direction Technique Critical Information Systems and Cybersecurity
Thales

Jean-Charles Nicolas
Ex-Délégué général du Pôle d'excellence cyber

Stéphane Paquelet
Responsable du laboratoire Intelligence Artificielle
b<>com

Jean Picco
Direction Technique Critical Information Systems and Cybersecurity
Thales

Frédéric Pierre
Directeur Scientifique
Systancia
Membre du Comité de Direction
Systancia Management

Paul-André Pincemin
Délégué à la cybersécurité et aux restructurations militaires
Rennes Métropole/Ville de Rennes

Frédéric Rémi
Directeur Général
AMOSSYS

Didier Virlogeux
Direction Marketing Critical Information Systems and Cybersecurity
Thales

PRÉAMBULE _

A.1 Introduction

Le Pôle d'excellence cyber a, depuis sa création, contribué à développer l'activité de recherche, l'offre de formation et à dynamiser le tissu industriel.

Ce référentiel qui a constitué une de ses premières productions a pour objectif de déterminer ce que recouvre le terme générique de « cyber », aujourd'hui largement répandu.

Il vise à dépasser la seule taxonomie technique en s'intéressant aussi aux cas d'usages, reflétant ainsi un des grands objectifs du Pôle d'excellence cyber.

Bien entendu, ce document a vocation à être partagé et diffusé largement, et cette nouvelle version, qui intègre des retours de l'ensemble des acteurs, sera amenée à évoluer régulièrement.

Pour atteindre ces objectifs, ce document s'articule autour de trois grandes parties :

- La première partie du document permet d'identifier le périmètre du domaine et d'identifier les enjeux techniques qui y sont associés.
- La deuxième traite des domaines fonctionnels qui utilisent les technologies, les méthodes et les services listés dans la première partie.
- La troisième contient un premier exemple d'analyse suivant une structuration basée sur la taille des entreprises clientes, et propose des exemples de structuration par métiers.

A.2 Définitions

Même s'il existe quelques définitions des termes « cyberdéfense » ou « cybersécurité » (par exemple l'ITU (International Télécommunication Union) fournit une définition dans le document IUT-T X.1205 (04/2008)), celles-ci ne permettent pas de délimiter clairement le contenu de ces domaines.

Au sein des entités en charge de la normalisation (CEN, CENELEC, ETSI), il existe un groupe de coordination sur la cyber, le Cyber Security Coordination Group (CSCG).

Ce groupe a émis la recommandation suivante:

> The European Council should establish a clear and common understanding of the scope of Cyber Security, based on an initiative the CSCG plans to launch to clarify the key terms and definitions used in the standardization of and communication related to Cyber Security within the European Union.

La préoccupation de clarifier le périmètre de la cybersécurité est donc assez généralement partagée par les acteurs concernés, et correspond à des actions qui sont en cours.

Au niveau national, il convient de retenir les définitions suivantes :

ANSSI

Cybersécurité :

> État recherché pour un système d'information lui permettant de résister à des événements issus du cyber-espace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.
> La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cyber-criminalité et sur la mise en place d'une cyberdéfense.

Cyberdéfense :

> Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels pour le pays.

Ministère des Armées

Les grands constitutifs de la cybersécurité :

1. Volet cyber-protection

   Ensemble des mesures techniques, physiques et organisationnelles mises en place pour bâtir les architectures les plus robustes possibles face aux menaces portant sur la disponibilité, la confidentialité et l'intégrité des informations ou des services.

2. Volet cyber-résilience

   Capacité des systèmes à continuer à fonctionner éventuellement en mode dégradé lorsqu'ils sont soumis à des agressions.

3. Volet cyberdéfense

   Ensemble des mesures techniques ou organisationnelles permettant la surveillance, l'appréciation de la sécurité et la réaction face à des attaques.

4. Volet cyber-renseignement

   Ensemble des opérations de collecte, d'enrichissement sémantique (traitement, analyse, fusion, interprétation) et de diffusion des informations, issues ou à destination (*) du cyber espace.

   (*) Il est d'origine ou/et d'intérêt cyber (ROC/RIC) selon qu'il est issu ou à destination du cyberespace.

5. Volet cyber-engagement

   Actions sur les systèmes numérisés adverses et opérations d'influence numérique à des fins de soutien de la supériorité militaire.

La stratégie Française de cyberdéfense est synthétisée dans les documents de référence :

- La revue stratégique de cyberdéfense[1] ;
- La politique ministérielle de lutte informatique défensive[2].

Le synoptique qui suit permet de visualiser simplement les différents regroupements d'activités.

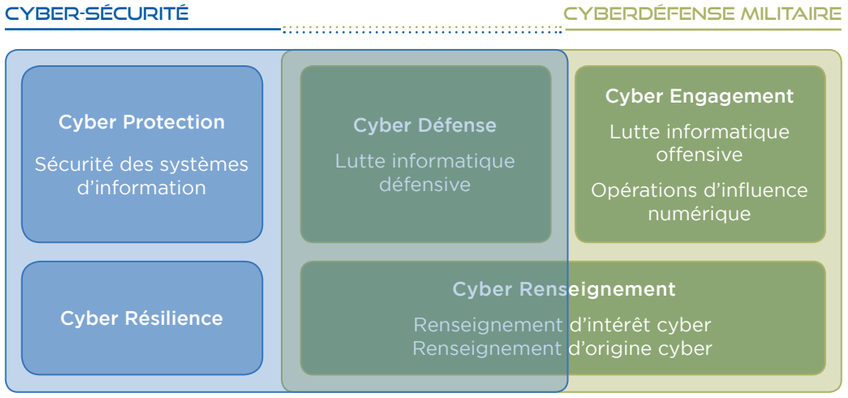


Figure 1 : Regroupements des activités de cybersécurité

Nota bene : excluant les activités purement militaires, le terme cybersécurité, du périmètre cerclé de bleu sur la figure 1, est celui qui va nous intéresser dans le reste du document, l'engagement cyber étant réservé aux Armées.

1 http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

2 https://www.defense.gouv.fr/content/download/551530/9394277/Politique%20MINARM%20de%20lutte%20informatique%20DEFENSIVE.pdf

B

TECHNOLOGIES ET SERVICES _

Plusieurs catégorisations existent pour structurer ce domaine. Celle proposée ci-dessous s'articule autour d'une déclinaison en trois thématiques : produits & technologies, services, méthodes & outils métiers.

Dans cette découpe thématique, la notion de service désigne les services opérationnels et non des services techniques ou des fonctionnalités administrées par un opérateur tiers.

Les quatre schémas synoptiques suivants présentent la structuration générale de la cybersécurité suivant ces différentes thématiques.

En première approche et sans présager des analyses de marchés qui seront réalisées ultérieurement par les acteurs nationaux de la filière, la suite du document explicite, sans rechercher l'exhaustivité, l'importance stratégique de certaines de ces thématiques.

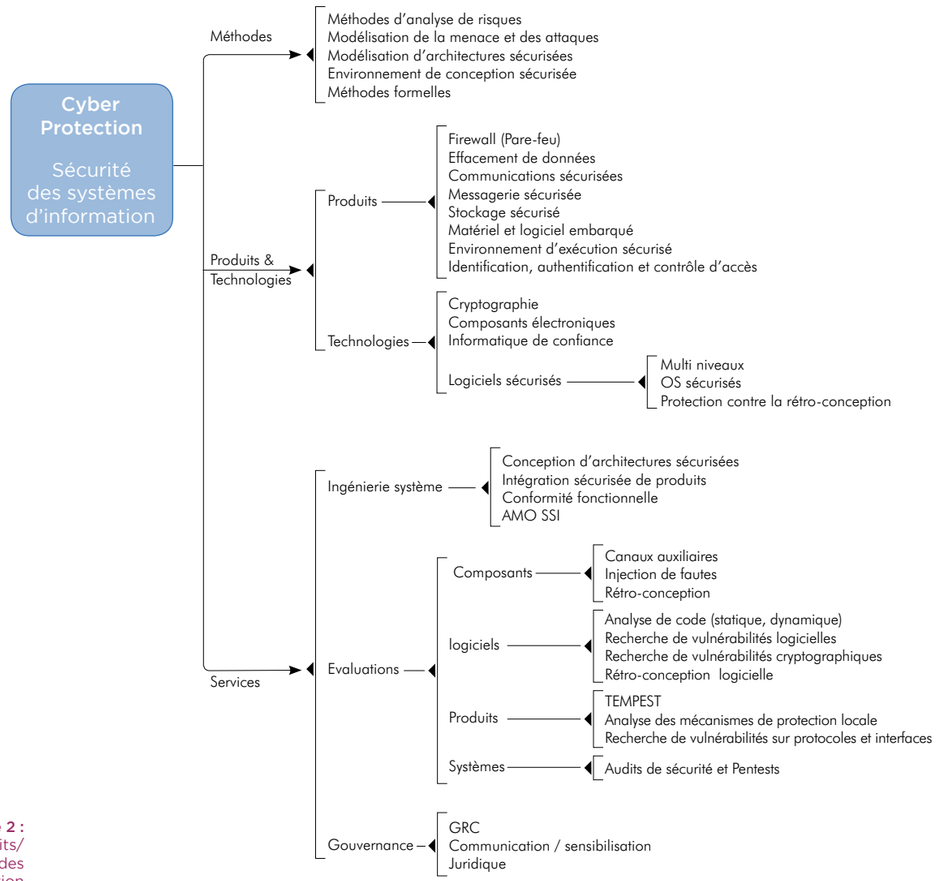


Figure 2 :
Besoins en produits/ services/méthodes de cyber-protection

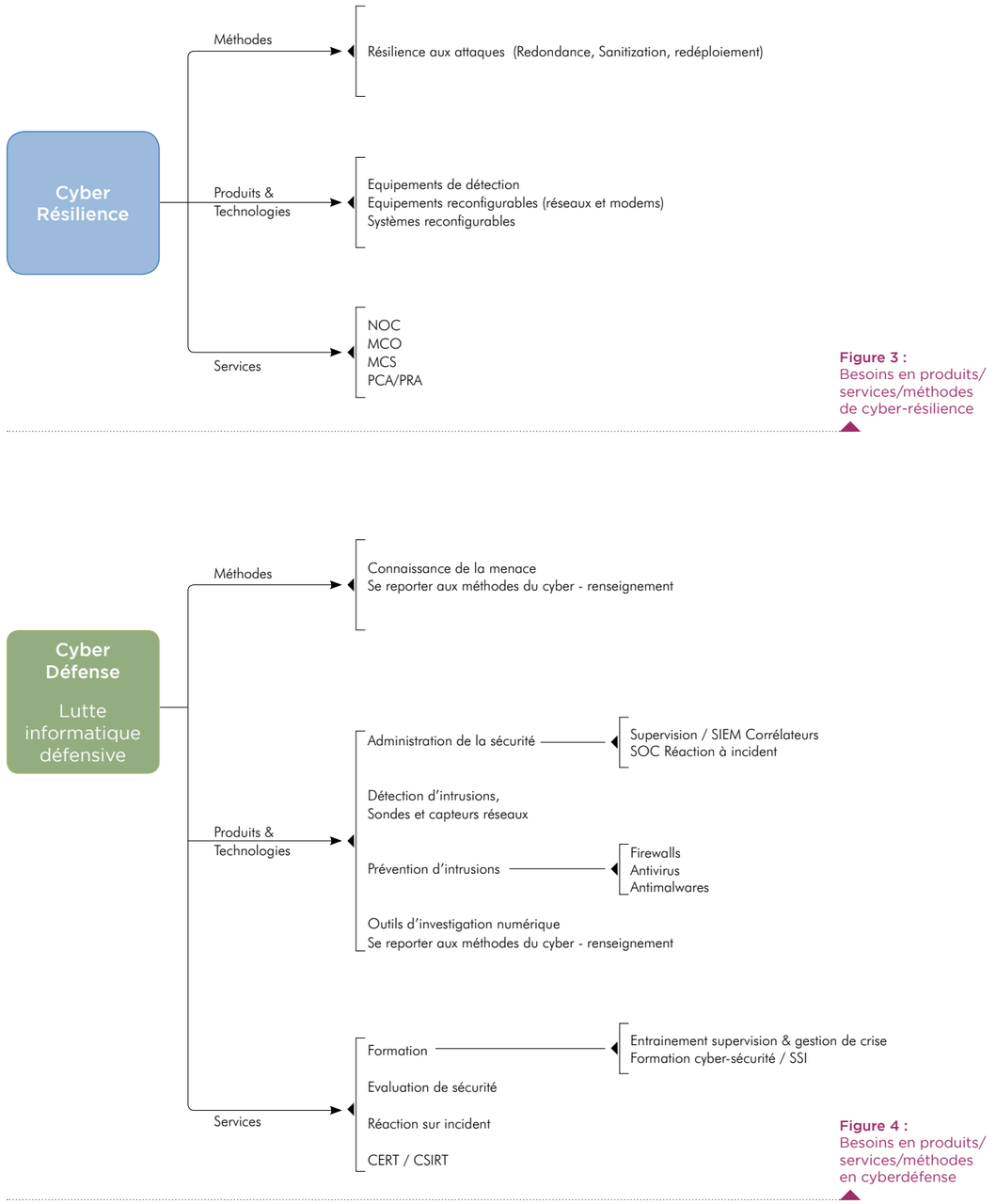


Figure 3 :
Besoins en produits/ services/méthodes de cyber-résilience

Figure 4 :
Besoins en produits/ services/méthodes en cyberdéfense

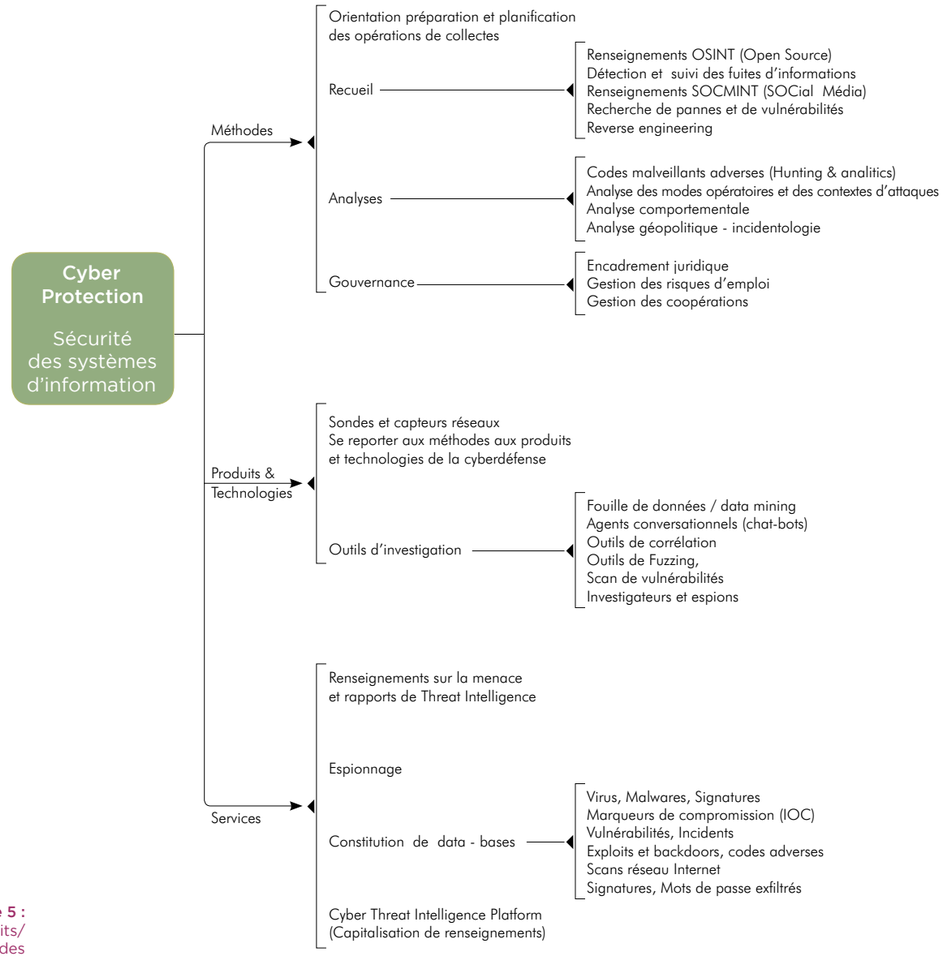


Figure 5 :
Besoins en produits/ services/méthodes en cyber-renseignement

Ces schémas servent de support à l'identification des besoins sectoriels et opérationnels liés à la cybersécurité pour la défense et le secteur civil.

L'engagement et le renseignement militaire étant des activités de nature régalienne, les rubriques associées ne sont pas développées dans ce document. Les sections suivantes exposent un certain nombre de thématiques critiques en termes de positionnement de la filière.

B.1.1 _Méthodes

B.1.1.1 _Analyse de risques

L'analyse de risque est l'outil de base de toute activité de cybersécurité. En effet, avant de mettre en place des solutions, il est impératif de bien identifier les enjeux, les besoins en sécurité, les menaces et scénarios de menaces contre lesquels il convient de se protéger. Ensuite, un processus d'analyse de risques doit être intégré à toutes les décisions d'évolutions d'un système.

L'ISO/IEC 27005 « Gestion des risques en sécurité de l'information » décrit les grands principes de cette analyse de risque.

La méthode de référence française EBIOS[3], proposée par l'ANSSI, permet par exemple d'accompagner les organisations dans l'identification et la compréhension des risques numériques qui leurs sont propres.
Cette méthode permet de déterminer les mesures de sécurité adaptées à la menace et de mettre en place le cadre de suivi et d'amélioration continue à l'issue d'une analyse de risque partagée au plus haut niveau.

B.1.1.2 _Modélisation de la menace et des attaques

La modélisation de la menace peut être vue comme l'une des briques des méthodes d'analyse de risques. Il apparaît également opportun de réaliser des bibliothèques de menaces et d'attaques qui pourraient être utilisées au sein de plateformes de test ou d'entraînement et mises à jour en fonction de la capitalisation sur le sujet. Dans les deux cas, il est nécessaire de définir des modèles partagés pour décrire les différents éléments et des outils pour les réaliser et les valider. L'équilibre entre la sensibilité potentielle de ces éléments et la nécessité de partage au sein de la communauté pour l'amélioration du niveau de sécurité doit être recherché entre les différents acteurs.

B.1.1.3 _Modélisation d'architectures sécurisées

Il existe de nombreux outils de modélisation système utilisés dans l'industrie. L'expérience a montré qu'il était difficile de les utiliser directement pour des analyses de sécurité. En effet, l'intérêt de la modélisation d'architectures sécurisées est de pouvoir utiliser ce modèle pour, par exemple, simuler l'impact de la menace ou d'un scénario d'attaque.
Il faut donc pouvoir intégrer des modèles d'attaques (cf. ci-dessus), des attributs de sécurité, prendre en compte l'aspect non probabiliste des attaques informatiques, … des choses aujourd'hui indisponibles dans les outils standards.

B.1.1.4 _Environnement de conception sécurisé

Pour limiter les failles de sécurité dans les produits de cyberdéfense, mais aussi de manière générale dans l'ensemble des produits logiciels ou intégrants du logiciel, il est indispensable de disposer de méthodes et d'outils adaptés.

3 https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

Les environnements de conception sécurisés doivent garantir l'intégrité des codes générés (par exemple en s'assurant que les bibliothèques sont bien issues d'une source sûre, ...) et offrir des outils pour limiter le risque d'erreurs de codage.

Quels que soient les méthodes ou les cycles de développement adoptés, et en particulier pour les méthodes agiles, la prise en compte des problématiques de sécurité est à considérer tout au long du cycle de développement, et notamment sur les phases amont.

Les organisations qui évoluent vers le modèle « DevOps » pour favoriser les retours des équipes opérationnelles vers les équipes de développement, doivent aussi intégrer la sécurité de façon continue sur l'ensemble du cycle de vie des applications et des infrastructures.

Les processus liés à la sécurité ne sont plus isolés et les équipes en charge de la sécurité sont bien immergées au sein de l'équipe projet pour mettre en place la sécurité dès le démarrage et prendre en compte les enjeux liés à l'automatisation spécifique à l'approche « DevOps ». Cette tendance a donné naissance à l'expression « DevSecOps ».

B.1.1.5 _Méthodes formelles

Les méthodes formelles (au sens large) sont, d'un point de vue haut niveau, des techniques basées sur des fondements mathématiques permettant de représenter une « problématique » et/ou une « solution » sous une forme clairement définie et non-ambiguë, puis au besoin de raisonner avec justesse (et de façon plus ou moins automatique) pour vérifier la satisfaction de la problématique par la solution. Les méthodes formelles peuvent être par exemple utilisées pour obtenir une preuve formelle de sécurité à partir d'un modèle, vérifier la cohérence d'un modèle par rapport à son implémentation, générer automatiquement du code ou des tests à partir d'un modèle, ...

Il existe un très large spectre d'utilisation et de nombreux travaux de recherche et d'industrialisation sont nécessaires pour disposer de méthodes et d'outils accessibles au plus grand nombre et qui apportent un maximum d'automatisation.

B.1.2 _Produits et technologies de sécurité

B.1.2.1 _Produits

La thématique des produits de sécurité est très vaste. Elle englobe les produits de chiffrement (réseau, téléphonie, messagerie, poste de travail, ...), les produits de contrôle d'accès et d'authentification (Gestion des Identités et des Accès (GIA), annuaires, certificats, ...), les produits de filtrage (pare-feu, diodes, ...), les anti-virus, les systèmes d'exploitation et composants de confiance et bien d'autres encore.

Quelques éléments peuvent être particulièrement mis en avant :

- L'importance des besoins liés à la confiance numérique : gestion des identités, de l'anonymat, de la résilience. Il s'agit notamment de la protection de la vie personnelle et des données privées ;
- L'adaptation des technologies de sécurité (cryptographie, identification, ...) aux architectures de type Cloud ;
- La capacité de construire une informatique de confiance par assemblage de protections aux différents niveaux : matériel, logiciel applicatif, systèmes d'exploitation, réseau, poste de travail, serveur, Cloud, ...
- L'importance de briques de base sans lesquelles la confiance ne peut être établie (voir le chapitre B.1.2.2 ci-après) :
  - Langages sécurisés, règles de programmation ;
  - Compilateur « de confiance »;
  - Machine virtuelle et OS « de confiance » ;
  - Implémentation sûre (logiciel et matériel) ;
  - Cryptographie sûre.
- Le domaine émergent des objets communiquant renforce ce besoin de bases matérielles et logicielles de confiance.

L'importance de produits de confiance ou souverains est bien entendu critique pour cette catégorie de produits.

Au niveau organisationnel aussi bien que technique, l'absence de standards permettant la mise en place de chaines de confiance entre différents acteurs est aussi une problématique.

B.1.2.2 _Technologies

B.1.2.2.1 _Cryptographie

La cryptographie est une des bases de la cybersécurité. Il est indispensable de maîtriser les algorithmes de chiffrement, de signature, d'authentification, ... mais aussi les protocoles associés et bien entendu tous les services nécessaires à la génération, à la distribution et au stockage sécurisé des clés.

Ce domaine fait l'objet de nombreux travaux académiques et de nombreux verrous restent à lever, comme par exemple :

- La cryptographie à très haut débit ;
- La cryptographie à bas coût énergétique pour les objets connectés ;
- La cryptographie adaptée au Cloud et au travail collaboratif ;
- La gestion de clés pour des systèmes comportant des millions d'utilisateurs ;
- L'intégrité et l'authenticité dans des systèmes purement logiciels ;
- La cryptographie post-quantique ;
- Les technologies de type blockchain ;
- La cryptographie homomorphe ;
- ...

B.1.2.2.2 _Composants électroniques

Comme la cryptographie à laquelle ils sont souvent associés, les composants de sécurité constituent une brique de base indispensable.

Il convient de bien comprendre et savoir évaluer les fonctions de sécurité intrinsèques des composants sur étagères. Il est aussi important de pouvoir disposer de capacités de réalisation de composants spécifiques.

L'existence de catalogues d'IP sécurisées ou apportant des services de sécurité est dans ce cadre une voie intéressante.

B.1.2.2.3 _Informatique de confiance

Indépendamment des initiatives mondiales comme le Trusted Computer Group (TCG) qui peuvent poser des problèmes de maîtrise ou de gestion de la vie privée, il existe un besoin réel de pouvoir garantir des transactions sûres, assurer la gestion de droits pour la diffusion de produits numériques, et globalement protéger les systèmes informatiques contre les agressions et les utilisations frauduleuses. Les techniques faisant intervenir un tiers de confiance, les DRM, la stéganographie (watermarking, ...) ou la blockchain font partie des éléments utilisables pour répondre à ce besoin.

La confiance est aussi nécessaire dans les outils de développement et de production du logiciel afin de garantir que le produit final est bien à l'image du code source fourni en entrée. La maîtrise des outils de développement est dans ce cadre un autre axe d'intérêt.

B.1.2.2.4 _Logiciel sécurisé

› B.1.2.2.4.1 _Multi-niveaux

Le multi niveau est un besoin prégnant dans le domaine de la défense où coexistent des niveaux de classification et de sensibilité très divers. Il existe aussi au sein des entreprises dans lesquelles il est possible de trouver conjointement des informations ouvertes, des informations confidentielles liées aux personnels, des informations financières, stratégiques, relevant du secret industriel, ... Il apparaît également cohérent de vouloir séparer des réseaux de type bureautique de réseaux de type industriels, ou des systèmes accessibles par des clients de systèmes internes à l'entreprise.

Le besoin de multi-niveaux peut s'exprimer suivant plusieurs modalités :

- Interconnecter des réseaux et systèmes de niveaux différents en permettant des échanges selon une politique de sécurité définie (par exemple connecter un réseau contenant des informations sensibles et des informations ouvertes à l'Internet pour échanger de l'information non sensible) ;
- Mettre à disposition sur un serveur, une base de données, ... des informations de différents niveaux de sensibilité et permettre à des utilisateurs d'y accéder selon des droits d'accès qui leurs sont propres ;
- Permettre à un utilisateur d'accéder depuis le même poste de travail à des environnements de niveaux de sensibilité différents.

Tous ces sujets ont été étudiés depuis longtemps et des produits commerciaux ont même été mis sur le marché. Leur diffusion a jusque-là toujours été freinée, à la fois par une difficulté d'exploitation certaine, mais aussi par l'incapacité d'arriver à concilier un niveau de sécurité en adéquation avec un niveau fonctionnel acceptable pour les utilisateurs. Il existe donc dans ce domaine un vaste champ de recherche et de réalisations de produits.

Les produits de type DLP (Data Leak/Loss Prevention) peuvent être rattachés à cette catégorie car ils utilisent sensiblement les mêmes concepts : identification de l'information sensible, contrôle des flux selon le niveau de sensibilité.

› B.1.2.2.4.2 _OS sécurisé

Les systèmes industriels souverains déploient des solutions intégrant des OS sécurisés reposant sur des noyaux de tailles limitées pour en faciliter leurs évaluations et en permettre leur maitrise.

Les systèmes informatiques grand public utilisent en revanche des systèmes d'exploitation qui sont, non maîtrisés pour les OS propriétaires, et difficiles à maîtriser pour les systèmes ouverts, à cause de leur taille et de leur complexité. S'il parait aujourd'hui illusoire de vouloir développer un OS de type Windows ou IOS entièrement maîtrisé, la recherche de solutions à base de virtualisation, par exemple, peut permettre de reporter une partie du problème sur un logiciel de plus petite taille susceptible d'être maîtrisé. Toutes les techniques de cloisonnement, de bac à sable (sand boxing), d'hyperviseurs, etc sont donc d'un intérêt certain. Elles sont notamment mises en œuvre pour bâtir des architectures multi-niveaux, chaque niveau de sécurité fonctionnant dans une « cage » étanche, sauf pour des échanges plus critiques qui passent alors par l'hyperviseur.

L'application de ces techniques peut concerner le monde bureautique au sens large mais aussi les systèmes embarqués, les terminaux mobiles et les objets connectés. Sans maîtrise des OS, il est en effet difficile de prétendre à une maîtrise des produits qui les utilisent.

En complément, il est nécessaire d'acquérir une bonne compréhension du fonctionnement de ces différents OS afin de pouvoir les configurer de la manière la plus sûre possible en fonction des besoins applicatifs. Ceci peut se concrétiser par la publication de guides de sécurisation ou bien par la réalisation d'outils de vérification ou de configuration automatiques.

› B.1.2.2.4.3 _Protection contre la rétro-conception

La protection contre la rétro-conception est une étape indispensable pour la protection de droits (des licences d'utilisation, par exemple) mais aussi pour la protection de savoir-faire industriels. Il est nécessaire de disposer de méthodes et d'outils facilement utilisables pour qu'ils soient mis en œuvre par les industriels dans le but de mieux protéger leurs produits. Ils doivent pouvoir s'adapter aux différents langages de programmation aux différents environnements d'exécution et s'insérer dans les processus de développement. Les techniques peuvent être purement logicielles ou faire appel à des éléments matériels. Il reste un vaste champ de recherche tant pour les techniques de protection (obfuscation de code, par exemple) que pour les outils qui les mettent en œuvre.

B.1.3 _Services

B.1.3.1 _Outils et techniques d'évaluation

L'obtention d'un niveau de confiance sur les produits de sécurité passe par une évaluation de leur résistance face à une large palette d'attaques. À cet effet, Il convient donc de préciser l'importance de la mise en place d'un schéma d'évaluation reconnu par l'ensemble des acteurs de la filière. Ce schéma se déclinera en méthodologies d'évaluation ad hoc par typologie de produits.

Les outils et méthodes d'évaluation sont donc indispensables pour garantir le niveau de confiance des produits cyber. Parmi les thématiques afférentes au schéma d'évaluation, il est possible de citer :

- L'évaluation de la sécurité du logiciel (audit de code, de configuration ou d'architecture) ;
- La génération de tests ;
- Les techniques de recherche de vulnérabilités ;
- Les attaques physiques intrusives ou non intrusives sur les composants (canaux cachés, injection de fautes, ...) ;
- Outils et méthodes de tests d'intrusion ;
- Outils et méthodes d'analyse de risques.

B.1.3.1.1 _Evaluation composant

L'évaluation de composants a pour objectif de déterminer le niveau de sécurité apporté par un composant matériel. Il existe dans ce domaine des techniques invasives et non invasives. Les moyens techniques nécessaires sont relativement conséquents (surtout pour les techniques invasives) et dans tous les cas une expertise de haut niveau est indispensable. Ces moyens et techniques sont surtout aujourd'hui maîtrisés par les CESTI spécialisés dans l'évaluation hardware. Ce domaine fait l'objet de nombreuses publications notamment dans les domaines de l'injection de fautes ou de l'analyse de canaux auxiliaires. La recherche dans le domaine peut déboucher sur des produits destinés aux CESTI, elle profite aussi aux concepteurs de composants pour leur permettre d'améliorer le niveau de sécurité de leurs produits.

B.1.3.1.2 _Evaluation logicielle

La recherche de vulnérabilités dans les logiciels est une activité complexe et extrêmement coûteuse. Même s'il existe de bonnes méthodes d'ingénierie, l'utilisation d'environnement de conception sécurisés, le choix de langages et de règles de programmation appropriés, peuvent permettre de réduire le nombre de défauts. Ces bonnes pratiques sont encore assez peu répandues et elles ne permettent pas à moyen terme de pouvoir garantir l'absence de vulnérabilités. Les méthodes et outils d'évaluation logicielle sont donc indispensables tant pour les entreprises spécialisées dans l'évaluation de sécurité (CESTI) que pour les développeurs, cela afin de vérifier au plus tôt dans les cycles de conception le niveau de qualité et de sécurité des logiciels qui sont produits. Les deux notions sont en effet assez liées : un logiciel d'un bon niveau de qualité ne sera pas forcément exempt de vulnérabilités SSI, et, à l'inverse, un logiciel de mauvaise qualité aura sans aucun doute un grand nombre de vulnérabilités.

Les outils et les techniques intéressants dans ce domaine sont notamment :

- Les outils d'analyse de code statiques et dynamiques ;
- Les outils de recherche de vulnérabilité, par test à données aléatoires (fuzzing), injection de code, ...
- Les outils de rétro-conception logicielle.

Ces différents outils peuvent être utilisés quels que soient les domaines d'application des logiciels à évaluer. Par contre, certaines catégories de logiciels (comme par exemple les logiciels de cryptographie) nécessitent des compétences spécifiques et éventuellement quelques outils complémentaires pour faire une recherche de vulnérabilités pertinente.

Il faut aussi pouvoir intégrer ces outils dans un environnement de test permettant autant que faire se peut la génération automatique de tests, leur gestion en configuration ou leur rejeu pour améliorer la productivité de cette activité.

B.1.3.1.3 _Evaluation produit

Même si la plupart des produits contient une grande proportion de logiciel, certaines fonctions de sécurité peuvent être rendues par le matériel (par exemple, les mécanismes de protection locale anti-intrusion sur les boitiers). Par ailleurs, en complément d'une évaluation logicielle, ou si on ne dispose pas du code source, il est important de pouvoir évaluer un produit en sollicitant ses interfaces externes (évaluation en boîte noire ou grise). Dans ce cas, les techniques de tests à données aléatoires (fuzzing) appliquées aux interfaces et protocoles, les outils de tests de l''interface homme-machine, vont être indispensables.

Un dernier sujet concerne l'analyse des signaux compromettants. En dehors de l'activité TEMPEST très spécifique aux produits classifiés, l'utilisation de plus en plus massive de protocoles radio et la disponibilité sur le marché de plateformes de radio-logicielles à faible coût, de l'existence de moyens d'analyse numériques performants et accessibles, ouvrent un large champ de vulnérabilités qu'il est utile de corriger.
Les travaux d'évaluation (de protocoles radio, TEMPEST), ou plus généralement, d'activités classifiées nécessitent l'utilisation de cages de Faraday.

B.1.3.1.4 _Evaluation système

B.1.3.1.4.1 _Audit de sécurité et Pentests

L'audit de sécurité permet d'obtenir une photographie de l'état de sécurité d'un système ou d'une organisation, par rapport à des référentiels SSI ou un état de l'art du domaine. Il comporte en général une partie technique et une partie organisationnelle (procédures, personnels, ...). Il existe différents référentiels pour mener à bien ces audits. La certification d'entreprises peut être recherchée pour faciliter le choix de prestataires compétents par les clients.

Il convient de ranger dans cette catégorie les prestations de type « test d'intrusion » (« pentest »), qui sont plus ciblées et purement techniques.

Ces activités nécessitent un encadrement juridique précis (chartes d'audit ou de test d'intrusion) et peuvent nécessiter des outils spécifiques.

B.1.3.2 _Ingénierie système

B.1.3.2.1 _Assistance à maîtrise d'ouvrage (AMO) SSI

Les prestations d'AMO SSI sont des prestations de services destinées à apporter un soutien SSI sur des projets. Elles recouvrent des prestations :

- D'analyse de risques ;
- De rédaction d'exigences ;
- D'animation de GT SSI ;
- De pilotage de travaux industriels ;
- De réalisation de synthèses au profit des décideurs ;
- ...

Elles nécessitent des experts de haut niveau et peuvent s'appuyer sur des outils d'ingénierie classiques (clausiers d'exigences, outils de gestion de traçabilité, ...) ou spécifiques au domaine (outils d'analyse de risque, modélisation de la SSI, ...).

B.1.3.2.2 _Conception d'architectures

La conception d'architecture sécurisée est une prestation de haut niveau qui nécessite une bonne maîtrise de l'analyse de risques et doit s'appuyer sur des outils de modélisation ou de simulation. L'objectif est de définir l'architecture capable à la fois de satisfaire aux besoins fonctionnels tout en garantissant le meilleur niveau de sécurité, et cela dans le respect des contraintes techniques et financières du donneur d'ordre.

B.1.3.2.3 _Intégration sécurisée de produits

Ce type de prestation fait souvent suite à la précédente. Une fois l'architecture définie et le choix des différents produits effectués, il s'agit de les configurer et de les intégrer dans un système fonctionnel et exploitable. Ici encore des outils de modélisation peuvent être utiles pour préparer le travail. Des moyens de tests permettant de vérifier le bon fonctionnement de l'ensemble sont aussi nécessaires.

B.1.3.2.4 _Conformité fonctionnelle

La conformité fonctionnelle vise à s'assurer qu'un produit réponde bien à son cahier des charges. C'est une étape nécessaire, y compris pour les produits de sécurité. Ce travail nécessite une forte automatisation, la complexité fonctionnelle des produits rendant les cas de tests extrêmement nombreux. Les techniques évoquées au chapitre B.1.3.1 sont indispensables pour fournir un service pertinent.

B.1.3.3 _Gouvernance

B.1.3.3.1 _GRC (Governance Risk Compliance)

Il existe un besoin de services autour de la gouvernance, gestion des risques et conformité (Governance Risk Compliance) de manière à disposer notamment d'un pilotage et de tableaux de bord de suivi des risques et de la conformité, notamment réglementaire, en fonction de l'avancement des plans d'actions.

B.1.3.3.2 _Communication et sensibilisation des utilisateurs

Les services liés à la communication et à la sensibilisation des utilisateurs sont essentiels, sachant que la vulnérabilité se situe « entre la chaise et l'ordinateur ». Les hommes et les femmes sont à la fois la plus grande vulnérabilité pour l'organisation et la solution aux problèmes de cybersécurité.

B.1.3.3.3 _Services juridiques

Le recours à des prestataires externes dans le domaine de la cybersécurité peut nécessiter une expertise juridique, afin de sécuriser l'organisation contre les risques liés à des défaillances ou au non-respect des contrats.

Cette dimension juridique doit aussi être prise en compte dans les contrats avec les clients ou pour l'organisation des processus en interne (chartes de sécurité, règlement intérieur, ...).

B.2 Cyber-résilience

B.2.1 _Méthodes

Une partie des fonctions de cyber-résilience est apportée par les architectures de systèmes. Les méthodes identifiées au B.1.3.2 seront donc utilisées pour bâtir des architectures incluant des redondances au niveau réseau ou au niveau services.

Dans le cas où une attaque a réussi il est bien entendu important de pouvoir remettre au plus vite le système dans un état opérationnel et sûr. Cela signifie qu'il faut pourvoir remettre à zéro les systèmes pour effacer toute trace des malwares (après avoir effectué, bien entendu, les copies nécessaires aux actions d'investigation post-incident (forensic), puis réinstaller à partir d'archives saines l'ensemble du système).
Les outils d'administration offrent les fonctions de base pour ce type d'action, mais il est nécessaire de définir des méthodes appropriées pour prendre en compte le contexte d'agression.

B.2.2 _Produits et technologies

De nombreux produits, notamment ceux liés à l'administration des systèmes permettent de contribuer à la résilience, en permettant une reconfiguration manuelle ou semi-automatique.

Au niveau des produits eux-mêmes, des fonctions d'auto-configuration en cas de détection d'agression peuvent être mises en œuvre : passage dans des modes de communication plus sécurisés au détriment du débit ou des services offerts, recherche de chemins alternatifs, voire coupure de services.

Ces fonctions doivent être gérées avec précaution pour ne pas induire de déni de service disproportionné par rapport aux attaques détectées, et, bien entendu, la détection d'attaques doit être pertinente pour éviter les faux positifs.

B.2.3 _Services

Les services permettant d'améliorer la cyber-résilience sont tout d'abord les services de surveillance de réseau, qui permettent de détecter les attaques et éventuellement de prendre des mesures de défense pour s'en prémunir. Ensuite, il est possible d'identifier les services de maintien en condition opérationnelle (MCO) et de maintien en condition de sécurité (MCS). En effet, de nombreuses attaques informatiques peuvent se diffuser à cause de la mauvaise configuration des systèmes : versions obsolètes, bases antivirales non mises à jour, ...
Le MCS de systèmes enfouis ou de systèmes industriels, dont il est parfois difficile d'interrompre le fonctionnement, pose de nombreuses difficultés qu'il est nécessaire d'étudier.

La réalisation de PCA/PRA (plans de continuité d'activité, plans de reprise d'activité) constitue aussi un volet important pour identifier les services essentiels, et la manière dont l'organisation peut fonctionner en cas d'attaque puis revenir à un mode de fonctionnement nominal.

Pour l'ensemble de ces activités, il est nécessaire de disposer de méthodes et d'outils qui permettent d'évaluer les niveaux de résilience d'un SI et d'une architecture, notamment par l'évaluation des niveaux de risque et l'identification des points de panne unique.

B.3 Cyberdéfense

B.3.1 _Méthodes de Lutte Informatique Défensive (LID)

B.3.1.1 _Connaissance de la menace

Pour connaître la menace externe, il est nécessaire de la mesurer par une veille active, notamment sur les sites d'information non officiels (Internet clandestin ou dark Web). L'exploration du Web profond (deep Web) via des techniques de « crawling » est à ce titre pertinente.

Pour connaître la menace sur le SI, il est nécessaire de disposer d'outils de collecte et de traitement d'informations en sources ouvertes et en sources fermées, sur les technologies, produits ou systèmes des technologies de l'information, mais aussi de systèmes connexes, comme par exemple les systèmes de contrôle industriel.

L'exploitation de ces données peut nécessiter des compétences dans les domaines des bases de données, du « big data », du « DATA mining », ...

Les méthodes et outils dédiés à la connaissance de la menace sont détaillés au paragraphe B.4 dédié au cyber-renseignement.

B.3.2 _Produits et technologies de LID

B.3.2.1 _Administration de la sécurité

B.3.2.1.1 _SIEM (Security Information and Event Management)

Les SIEM sont des outils qui intègrent des fonctions de collectes d'événements générés par des sondes (voir ci-après), de normalisation de ces informations, d'agrégation et de corrélation, puis de visualisation vers un opérateur. Les SIEM peuvent ensuite être connectés à un SOC (Security Operation Center, voir ci-après).

B.3.2.1.2 _SOC / Réaction à incident

Des fonctions basiques peuvent être intégrées dans les SIEM, mais elles sont plus généralement identifiées dans les SOC (Security Operation Center).

Le SOC a pour rôle d'agréger les données issues des sondes, de les analyser, puis d'en donner une vue pertinente au regard des décisions à prendre pour assurer la sécurité du SI et du processus qu'il sous-tend.

Par ordre de difficulté croissante, les techniques d'aide à la décision sont :

- La présentation de solutions techniques possibles vers un opérateur (de type fiche réflexe par exemple) ;
- La présentation de solutions techniques priorisées selon les impacts métier ou processus ;
- La réaction automatique sur scénarios : possibilité de basculer dans des modes de repli en fonction de conditions préétablies ;
- La réaction automatique par système expert.

Ces fonctions de réaction sont très critiques, une réaction inappropriée ou disproportionnée pouvant entraîner des conséquences désastreuses pour le fonctionnement de l'entreprise ou de l'organisme concerné.

B.3.2.2 _Produits de détection d'intrusion (sondes et capteurs réseaux)

Les produits de détection d'intrusion désignent des sondes qui vont capter l'information alimentant ensuite le reste de la chaîne de LID.
Il convient de citer :

- Les capteurs basiques qui enregistrent l'activité du système (journalisation des événements) ;
- Les sondes réseaux, qui analysent le trafic pour identifier des événements anormaux ;
- Les sondes hôtes qui vont analyser le fonctionnement d'un poste de travail ou d'un serveur pour identifier les comportements anormaux ;
- Les sondes métiers qui vont analyser un processus (process) pour identifier des déviations par rapport à un comportement normal ou acceptable.

Ces sondes relèvent des données qu'il est nécessaire de faire remonter par un réseau. Ce réseau de collecte peut être soit confondu avec le réseau opérationnel, soit dédié. Ces flux sont à sécuriser en eux-mêmes.

Les sondes peuvent fonctionner par détection de signatures ou suivant une analyse comportementale (les sondes métiers sont plutôt exclusivement dans cette seconde catégorie).

La détection d'intrusion peut être considérée selon un axe domaine d'emploi afin de s'adapter à des catégories de systèmes différentes (SI, systèmes d'armes, systèmes industriels). Elle peut aussi être considérée selon un axe technique avec les différents types de sondes (réseaux, systèmes) et différents modes de détection, notamment la détection comportementale (déviance par rapport à un usage normal).

B.3.2.3 _Prévention d'intrusion (Firewalls, Anti-virus, Anti-malwares)

Les anti-virus ou les firewalls se présentent souvent comme des outils de prévention d'intrusion. Ils peuvent se placer au niveau réseau ou au niveau système et ont comme caractéristique de détecter et de bloquer les attaques.

Les anti-virus peuvent être classés comme des outils de prévention ou de défense (ils protègent contre les agressions en éliminant les logiciels malveillants détectés et ils génèrent des alertes). Il existe globalement deux grandes familles : ceux utilisant des bases de signatures et les anti-virus comportementaux.
Les deux modes peuvent être mixés et sont parfois associés à des fonctions de type Cloud pour des estimations de risques (réputation de logiciels, ...). Pour ces produits, il s'agit de conserver une capacité à identifier de nouvelles menaces toujours plus complexes sans trop pénaliser le fonctionnement des postes ou des serveurs.

Concernant les malwares, pour en comprendre le fonctionnement et les éradiquer il est nécessaire de disposer d'outils spécifiques. En effet, pour des raisons évidentes, l'analyse de ces logiciels ne peut être réalisée que dans un environnement maîtrisé afin d'éviter leur propagation. Par ailleurs, le degré de sophistication avancée de ces malwares commande d'effectuer leur analyse dans des environnements hautement réalistes, au risque qu'ils ne déploient pas l'ensemble de leurs fonctionnalités.

L'analyse de ces logiciels peut aussi demander des outils évolués de rétro-conception pour comprendre le détail de leur fonctionnement.

Une description des méthodes et outils est proposée en complément au sein du chapitre consacré au cyber-renseignement.

B.3.2.4 _Outils d'investigation numérique

Les outils d'investigation numérique sont utilisés pour rechercher les traces laissées par une agression informatique et reconstruire la chronologie des événements, ou encore pour reconstruire des données effacées.

Certains de ces outils peuvent être utilisés dans le cadre d'actions judiciaires et doivent donc garantir une forte intégrité et une parfaite traçabilité des actions.

L'évolution des technologies et des usages conduit à réaliser des investigations numériques non seulement sur des supports physiques et des postes de travail, mais aussi sur des réseaux, des systèmes ou des architectures de type Cloud. Les volumes de données à traiter sont de plus en plus considérables (investigation numérique et big data). Cette évolution demande de nouvelles méthodes et de nouveaux outils.

Une description complémentaire de méthodes et outils d'investigation numérique est proposée au sein du chapitre dédié au cyber-renseignement.

B.3.3 _Services

B.3.3.1 _Formation

B.3.3.1.1 _Formation cybersécurité

L'ANSSI propose sur son site[4] une liste de profils. Cette liste est résumée au chapitre E. Des formations initiales ou continues doivent être proposées afin d'être en mesure de disposer de ressources humaines en quantité et de qualité pour tenir les postes qui sont à pouvoir dans les sphères privée ou étatique. Ce besoin en formation nécessite des outils et systèmes de formation à la cyberdéfense, à la supervision de la sécurité, et à la gestion de crise.

Ces moyens doivent servir à la formation de personnels de différents niveaux (utilisateurs, techniciens, ingénieurs, experts), civils ou militaires et dans ce dernier cas pour des systèmes en métropole ou sur les théâtres d'opérations extérieures.

B.3.3.1.2 _Entrainement supervision et gestion de crise

Ces formations plus spécifiques doivent permettre de disposer de personnels de différents niveaux, aptes à réagir efficacement en cas de crise cyber. Ces formations peuvent aussi inclure la dimension juridique liée à la cyber-défense (quels sont les droits en cas d'attaque, quelles limites à la réaction, ...), des aspects éthiques, et prendre en compte des aspects psychologiques, telle la gestion du stress. Afin de mieux spécifier les contrats de service ou de développement de produits, les aspects contractuels doivent aussi être abordés.

B.3.3.2 _Evaluation de sécurité

Il est vital de pouvoir estimer le niveau de sécurité des outils ou services de LID. Leur évaluation par des entreprises de confiance est donc indispensable. Les outils et enjeux sont identiques à ceux développés pour les outils de protection (cf. B.1.3.1).

4 http://www.ssi.gouv.fr/entreprise/formations/profils-metiers/

B.3.3.3 _Services juridiques

Les services juridiques interviennent de manière transverse sur les différentes activités, soit pour borner et sécuriser les différentes prestations de services, soit pour définir le cadre d'emploi de certains outils, ou pour encadrer la mise en place de procédures ou d'outils de cybersécurité au sein des entreprises.

B.3.3.4 _Réaction aux incidents

Dans le cas où une attaque a atteint son but, la remise en service du système d'information de l'organisation attaquée peut demander des ressources humaines conséquentes à la fois en quantité (s'il faut par exemple une intervention physique sur un grand nombre d'équipements) et en qualité (préservation des traces, expertise technique pour l'éradication des malwares, ...). Ces équipes peuvent être internes ou externes à l'organisation mais doivent être formées et entrainées.

B.3.3.5 _CERT[5] / CSIRT

Les CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team) sont des entités publiques ou privées qui assurent le traitement des alertes informatiques, l'entretien et la diffusion de bases de vulnérabilités et la diffusion de messages d'alertes ou de prévention.

B.4 Cyber-renseignement

Le cyber-renseignement désigne l'ensemble des opérations de collecte, d'enrichissement sémantique (traitement, analyse, fusion, interprétation) et de diffusion des informations issues ou à destination du cyberespace.

Il est d'origine cyber lorsqu'il est issu du cyberespace. Il est d'intérêt cyber lorsqu'il est à destination du cyberespace.

B.4.1 _Méthodes

B.4.1.1 _Orientation préparation et planification des opérations de collecte

L'orientation consiste à identifier la nature et les supports des informations à recueillir, à définir la suite des opérations nécessaires au recueil, et à inventorier les moyens à mettre en œuvre.

Les capacités matérielles et humaines et leur préparation préalable conditionnent la réussite des opérations de recueil.

B.4.1.2 _Le recueil d'informations

Le recueil d'informations concerne l'ensemble des activités permettant d'agglomérer les informations et d'en tirer profit.

Le renseignement technique couvre des formes très variées, liées à la nature de l'information et à son mode de recueil.

Si nous excluons le renseignement au profit des activités de la Défense Nationale et sans prétention d'exhaustivité, nous citerons comme principales sources de renseignement technique :

- L'OSINT (Open Source INTelligence) qui concerne les informations accessibles au grand public en source ouverte. Ces sources incluent les journaux, l'Internet, les écrits, les diffusions, les fuites d'information quelle que soit leur origine ;
- Le SOCMINT (SOCial Media INTelligence) qui fait référence aux méthodes et moyens dédiés à la surveillance des médias sociaux, de manière à anticiper ou agir sur les besoins et les comportements des utilisateurs ;
- La recherche de vulnérabilités sur les logiciels et les équipements. Que ce soit en provoquant l'apparition de défauts ou de pannes par des tests tous azimuts hors du champ d'utilisation de l'équipement (tests à données aléatoires (fuzzing)), ou par la recherche de voies d'infiltration et d'exploitation de failles ; ces activités ont pour but d'identifier les vulnérabilités afin d'organiser la défense des infrastructures ;
- La rétro-ingénierie ou le reverse engineering. Consiste à étudier et à décortiquer un objet pour en déterminer son fonctionnement ou sa méthode de fabrication. Ces études peuvent être, par exemple, l'analyse d'un binaire malicieux, d'un virus, la recherche de vulnérabilités en vue de leur éradication, ou l'étude d'un objet (physique ou logique) pour lutter contre la copie et les contrefaçons.

B.4.1.3 _Analyses

Les analyses ont pour vocation d'apporter une compréhension rapide et exhaustive sur le déroulement d'un événement (campagnes d'attaque), sur le mode opératoire d'un groupe déterminé, ou sur le fonctionnement d'un malware et/ou sur son évolution.

Sur le plan technique, elles apportent les informations sur la structure d'un malware et/ou sur des indicateurs de compromission (Indicators of compromise (IoC)). Les descriptions techniques issues des analyses amènent à l'écriture de règles de détection et permettent d'avoir une démarche proactive et non pas uniquement réactive.

Les descriptions techniques sont complétées par une analyse contextuelle et stratégique, qui, à partir des éléments techniques obtenus grâce à l'investigation, vise à déterminer la motivation réelle de l'attaquant. Pour cela, la compréhension de l'écosystème international qui entoure l'attaque (juridique, financier, social, culturel) est essentielle pour saisir les tendances stratégiques qui expliquent l'événement.

L'analyse du contexte stratégique permet une compréhension accrue des facteurs déclencheurs des événements et donc la mise en place de démarches proactives.

Idéalement les rapports d'analyse contiennent une description des secteurs industriels et géographiques touchés, l'origine de l'attaquant, ses Tactiques, Techniques et Procédures (TTP), et ses motivations.

5 Le terme CERT est une marque déposée de l'université Carnegie Mellon et ne peut être utilisé sans leur accord

B.4.1.4 _La gouvernance

Le renseignement militaire est une activité de nature régalienne, sa gouvernance n'est pas détaillée dans ce document[6].

B.4.2 _Produits et technologies

B.4.2.1 _Sondes et capteurs réseaux

Se reporter au paragraphe B 3.2.2.

B.4.2.2 _Outils d'investigation

Les outils d'investigation ont pour objectif d'identifier les vulnérabilités résiduelles des systèmes d'information, les menaces qui leurs sont associées, ils aident à caractériser les attaques que ces systèmes pourraient subir ou subissent.

Les outils d'investigation sont de natures très variées, ils dépendent du support de stockage, de transport, ou d'exploitation des informations qui sont à protéger.

Leur terrain d'application est extrêmement étendu (depuis les couches matérielles jusqu'aux applications), protéiforme et mouvant.

À titre d'exemple nous avons cité : les fouilles de données, les agents conversationnels, les outils de corrélation et de classification, les tests à données aléatoires (fuzzing), les scanners de vulnérabilités, liste loin d'être exhaustive.

Le lecteur pourra s'adresser pour plus de détails aux services et agences de l'État, tels que la DGSI ou l'ANSSI en France, ou vers des sociétés privées spécialisées dans ce domaine.

B.4.3 _Services

B.4.3.1 _Renseignements sur la menace et rapports de Threat Intelligence

Le renseignement sur la menace consiste à caractériser la menace sous ses différents aspects :

- Son origine : de qui provient-elle ?
- Pourquoi ? Dans quel contexte ?
- Qui en est la cible ?
- Quels sont les lieux concernés par la menace ?
- Quand peut-elle être exercée ?
- Sous quelles formes peut-elle s'exprimer ?
- Quels sont les moyens et les modes opératoires de l'attaquant ?
- Quelles sont les solutions pour s'en protéger ?

Le renseignement sur la menace fait l'objet de rapports de Threat Intelligence (TI) ou Cyber Threat Intelligence (CTI) synthétisant tout ou partie des réponses aux questions adressées.

Le monitoring des activités souterraines de la cybercriminalité et des trafiquants et la surveillance du cyberespace pour la lutte contre le terrorisme illustrent l'importance de l'activité de suivi des cyber-menaces.

B.4.3.2 _Lutte contre l'espionnage

Le cyber espionnage consiste à récupérer des données sensibles ou des droits afin d'obtenir un avantage sur une entreprise ou une entité gouvernementale.

Le site gouvernemental dédié à la lutte contre l'espionnage[7] en expose les risques et les moyens de prévention. Le Service de l'Information Stratégique et de la Sécurité Economique (SISSE) propose 26 fiches autour de la sécurité économique[8]. L'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ) a également publié un kit de sensibilisation des atteintes à la sécurité économique[9].

La règlementation pour la cybersécurité des entreprises est évoquée au chapitre H.3

B.4.3.3 _Constitution de bases de données

La constitution de bases de données permet de capitaliser les connaissances issues du renseignement, de les représenter sous différents angles de vues selon les problématiques à adresser, et de les rendre disponibles pour une exploitation numérique par un calculateur et ses logiciels.

Divers types d'objets peuvent être capitalisés et mis en base ou en catalogue pour être réemployés à des fin de lutte informatique défensive (LID) ou offensive (LIO). Sans exhaustivité nous pouvons citer :

- Les logiciels malveillants (vers, chevaux de Troie, portes dérobées, spywares, keyloggers, rootkits, ransomwares, ...) ;
- Les signatures de logiciels malveillants ;
- Les indicateurs de compromission ;
- Les vulnérabilités matérielles, logicielles, ou des systèmes ;
- Les incidents observés ;
- Les scans réseau via l'Internet ;
- Les certificats et les mots de passe interceptés ou décryptés.

B.4.3.4 _Cyber Threat Intelligence Platform (Capitalisation de renseignements)

Un service de CTI performant utilise une plateforme pour pouvoir :

- Agréger plusieurs sources de données sur une même plateforme ;
- Corréler, qualifier et valider les informations, via des processus ou par investigation ;
- Disséminer l'information via des capacités d'interfaçage avec l'environnement.

Dans un environnement interconnecté, complexe et changeant, il est essentiel de comprendre l'évolution rapide des menaces afin d'adapter les processus et les opérations de cyberdéfense.

6 Pour plus d'informations, les éléments publics figurent à l'adresse : https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf

7 https://www.gouvernement.fr/risques/espionnage
8 https://sisse.entreprises.gouv.fr/fr/outils/la-securite-economique-au-quotidien-26-fiches-thematiques
9 https://inhesj.fr/kit-de-sensibilisation-des-atteintes-la-securite-economique

Défendre une infrastructure contre des vulnérabilités inconnues du plus grand nombre, qualifiées de zero-day, lutter contre des menaces persistantes complexes (Advance Persistent Threat (APT)) est un défi majeur qui nécessite une compréhension des objectifs et du mode de fonctionnement de l'adversaire.

Une plateforme Cyber Threat Intelligence permet d'améliorer la résolution des incidents de sécurité en évoluant d'une défense réactive et partielle à une réponse proactive et adaptée. Les formats d'échange d'informations sur les menaces peuvent prendre plusieurs formes, mais les analystes se tournent presque toujours vers l'échange d'indicateurs de compromission (Indicators of Compromise (IOC). Les opérations de collecte, partage et échange d'informations en sont les étapes clés.

B.5 Cyber-engagement

Le cyber-engagement désigne les actions sur les systèmes numérisés des adversaires et les opérations d'influence numérique qui visent à soutenir la supériorité militaire des Armées.

L'engagement étant une activité de nature régalienne, la rubrique n'est pas développée dans ce document[10].

B.6 Zoom sur l'utilisation de l'Intelligence Artificielle (IA) en cybersécurité

B.6.1 _Introduction et principales méthodes et algorithmes

Dans ce document, nous adoptons une définition volontairement large de la notion d'intelligence artificielle (IA) dans laquelle tout système informatique capable d'analyser son environnement pour décider de ses actions et interagir est considéré comme intelligent.

Pour une discussion approfondie à ce sujet, on renverra le lecteur à :

Russel, S., Norvig, P., 2010. Artificial Intelligence: a modern approach. 3nd Edition. Prentice Hall, Pearson Education Inc.

Cette définition de l'intelligence artificielle ne se limite pas, à celle d'apprentissage (machine learning), voire d'apprentissage profond (deep learning).

Ces notions ne sont pas équivalentes, mais bien imbriquées : l'intelligence artificielle englobe l'apprentissage, qui lui-même englobe l'apprentissage par réseaux de neurones, qui lui-même englobe l'apprentissage profond.

L'IA englobe aussi plusieurs autres types de techniques logicielles, comme les moteurs de règles (systèmes experts), et de même l'apprentissage englobe de nombreuses techniques qui ne font pas appel à des réseaux de neurones (par exemple les forêts aléatoires, Support Vector Machine (SVM), etc.) dont certaines ont par exemple l'avantage de l'explicabilité des raisonnements par construction.

Une analyse méthodologique avec modélisation de la problématique et des données afférentes facilite la mise en évidence des notions d'explicabilité et de fiabilité qui sont clés pour la certification des solutions incorporant ces techniques.

Une telle approche doit être encouragée par rapport à une approche de type « boite noire » de l'intelligence artificielle qui permet une résolution rapide de certains problèmes mais au prix bien souvent de biais de représentativité, de robustesse et fiabilité des résultats proposés.

De nombreuses thématiques scientifiques relèvent traditionnellement de l'IA. Elles peuvent être classées en quelques grandes familles : résolution de problèmes ; connaissance et raisonnement, notamment en environnement incertain ; planification ; apprentissage ; communication, perception et action.

Nous allons dans les chapitres qui suivent nous concentrer sur les liens entre IA et cybersécurité, selon quatre points de vue :

- Les cas d'usage de l'IA en cybersécurité ;
- La cybersécurité des systèmes intégrant de l'IA ;
- L'évaluation des systèmes intégrant de l'IA ;
- Les données et les plateformes nécessaires pour développer des systèmes à base d'IA.

B.6.2 _Cas d'usage de l'IA pour la cybersécurité

Les applications de l'IA pour la cybersécurité sont potentiellement infinies si on considère que cette technique peut être utilisée dans tous les systèmes numériques.

Quatre grandes catégories d'applications où l'IA peut apporter un gain particulièrement significatif peuvent être identifiées :

- L'aide au développement sécurisé : l'IA pourrait aider à la modélisation et à la simulation de systèmes complexe, à la détection d'erreurs de conception ou de codage, permettant ainsi le développement de produit sûrs par conception ;

10 Pour plus d'informations, les éléments publics figurent à l'adresse : https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf

- L'évaluation de sécurité : l'IA peut permettre la recherche de vulnérabilités sur des logiciels mêmes complexes ou volumineux, mais aussi sur des composants avec la capacité d'analyser des images de puces électroniques. L'IA montre aussi d'ores et déjà sa capacité à la caractérisation de menaces DPA permettant d'aider à la sécurisation de composants. Enfin, l'IA peut permettre d'assister des équipes de pentest en réalisant des tests automatisés permettant de démultiplier les capacités des équipes ;
- La détection d'attaques : ce sujet a probablement été un des premiers où l'IA a été utilisée en cybersécurité. Il s'agit ici de détecter des signaux faibles dans des masses de données importantes (des logs, par exemple), de détecter des comportements anormaux d'individus ou de processus qu'ils soient métiers ou informatiques, d'effectuer des analyses de corrélation entre des multitudes d'évènements, et de détecter des logiciels malveillants complexes ;
- La réaction aux attaques : ce sujet reste aujourd'hui majoritairement à défricher mais une IA pourrait : aider à proposer des mesures de réaction face à une attaque, voire prendre automatiquement ces mesures, aider à l'identification de la source de la menace et à développer des contre-mesures.

B.6.3 _Sécurité de l'IA

Les algorithmes d'IA, comme tous les algorithmes peuvent être la cible d'attaques informatiques. C'est aussi le cas des machines qui les hébergent mais en première hypothèse on considérera que ce point est adressé par les techniques classique de sécurisation de l'IT.

Les systèmes d'IA devront donc être sécurisés depuis leur phase de conception. Cette sécurité devra être évaluée lors des phases de qualification et la sécurité réévaluée durant tout le cycle de vie du système. De manière synthétique, quatre grands types de vulnérabilités pour les systèmes d'IA sont à prendre en considération :

- L'empoisonnement de données : introduction dans le jeu de données de données erronées choisis pour affecter le comportement des systèmes ;
- La porte dérobée : introduction d'un biais dans le modèle qui va déclencher un certain comportement face un événement choisi par l'attaquant (ex : marque sur un panneau STOP qui le fera considérer comme un autre panneau) ;
- La reconstruction de données d'apprentissage : cette vulnérabilité consiste à mener des actions de rétro-conception, elle permet de remonter aux données qui ont servi à entrainer le modèle. Ces données peuvent être sensibles, voire classifiées pour des applications défense ;
- Le leurrage : il s'agit d'introduire une perturbation dans les données d'entrée pour modifier la réponse du système en ajoutant du bruit dans une image ou sur un son (one pixel attack par exemple), bruit choisi pour être indétectable par un humain mais spécifiquement conçu pour provoquer une erreur du système.

Les techniques de sécurisation vont dépendre du type d'IA utilisé. Pour les IA utilisant massivement des données (apprentissage automatique), leur qualité intrinsèque et la qualité des traitements associés (mise en forme, filtrage, annotations, ...) vont être prépondérantes pour que l'apprentissage se déroule correctement. D'autres propriétés doivent aussi être étudiées, comme leur intégrité, pour être sûr que l'apprentissage de déroule bien avec les données sélectionnées à cet effet.

Des méthodes algorithmiques peuvent aussi être employées pour éliminer les menaces, elles sont listées plus haut. Certains moyens de détection permettent aussi d'identifier des attaques (par leurre notamment), ce qui vient renforcer la sécurité de l'ensemble.

B.6.4 _Agrément et homologation des solutions à base d'IA

L'évaluation de produits de sécurité « traditionnels » (pare-feu, IDS, chiffreurs, etc.) restait jusqu'à présent cantonnée à l'utilisation de techniques déterministes. L'intégration progressive d'algorithmes d'apprentissage et de prise de décision dans les nouvelles familles de produits de sécurité nécessite de facto une adaptation des méthodes d'évaluation afin notamment de renforcer l'efficacité intrinsèque de ces produits de sécurité.

À l'instar des usages de l'IA en cybersécurité (détection d'intrusion, filtrage de spams, analyse de malwares, détection d'exfiltration de données, authentification biométrique,...), les méthodes utilisées (classification, partitionnement de données (clustering), détection d'anomalies, régression linéaire et prédictions,...) sont de plus en plus nombreuses, ce qui induit forcément :

- Des limitations d'ordre opérationnel (complexité du paramétrage, prise en compte du modèle de menace, ...) ;
- Des limitations liées à l'efficacité des algorithmes face aux attaques complexes et/ou nouvelles ;
- Des limitations liées à la robustesse des algorithmes (résistance à l'empoisonnement, résistance à l'évasion, ...).

Dans ce contexte, la spécification d'une démarche d'évaluation / de certification de produits de sécurité intégrant de l'IA devra reposer sur :

- L'analyse du modèle de menace du produit (exposition du produit à l'empoisonnement, intérêt de l'attaquant à évader le mécanisme cible, confidentialité des entrées, ...) ;
- L'analyse de l'adaptabilité du produit à l'environnement (adaptation des paramètres au contexte opérationnel, capacité d'assistance au paramétrage, ...) ;
- L'analyse de l'efficacité du produit dans un environnement réaliste ;
- L'utilisation d'une plateforme Cyber Range générant du trafic d'attaque et du trafic de vie pertinent ;
- La confrontation du produit à un catalogue d'attaques ;
- La construction de scénarios réalistes et variés ;
- L'analyse de la robustesse des algorithmes retenus (« empoisonnement » des données d'entrainement, évasion du moteur de test, inversion du modèle, extraction du modèle et de ses paramètres / seuils, ...).

La normalisation d'une démarche d'évaluation / certification opérationnelle de ce type devrait voir le jour d'ici quelques années sous l'impulsion de l'ENISA et des Agences Nationales de Sécurité qui vont multiplier les investissements autour de cette thématique.

B.6.5 _Big data et infrastructures et technologies dédiées à l'implémentation de solutions d'IA

Aujourd'hui branche phare de l'IA, l'apprentissage statistique (Machine Learning, Deep Learning) requiert massivement un accès aux données. Or, ces données sont souvent la propriété de quelques acteurs et leur accès peut être complexe, notamment pour des domaines sensibles tels que la cybersécurité. Précisons ci-dessous les enjeux spécifiques à la constitution, au transport et à l'exploitation de ces jeux de données.

Sans préjuger de la solution adoptée, un besoin en traitement numérique se décomposera systématiquement en questions élémentaires associées aux catégories suivantes :

- Estimation de paramètres dans un système ;
- Classification (appariement à des classes prédéterminées) et partitionnement de données (clustering) (classes non prédéterminées) ;
- Prédiction pour anticipation de séries temporelles ;
- Commande optimale (planification de suite d'opérations).

En s'appuyant sur les performances atteintes par les processeurs, l'apprentissage statistique a connu ces dernières années des progrès spectaculaires dans toutes ces catégories : détermination de paramètres physiologiques, reconnaissance d'images, traitement du langage naturel, transport autonome, cybersécurité. Les techniques utilisées reposent toutes sur l'exploitation de données massives. Ces données sont soit issues du terrain, ce qui est nécessaire en l'absence de modèle descriptif, soit synthétisées quand un modèle descriptif permet des simulations extensives.

S'agissant de la constitution de bases de données terrain, il est crucial de disposer d'une capacité de collecte et de création de données dans les domaines d'application visés. Dans cette perspective, l'Internet des Objets (IoT), qui présente une complémentarité symbiotique avec l'IA, pourra permettre la capture, la numérisation et la centralisation des données physiques alimentant les algorithmes de prédiction et de prise de décision.

Concernant la génération de données synthétiques, des capacités de calcul sont requises dès la phase de simulation ainsi que des capacités de stockage pour les données générées.

Dans les deux cas, l'exploitation nécessite des capacités réseaux pour l'acheminement des données vers des plateformes disposant de capacités de stockage et de calcul intensif. Ces plateformes devront répondre aux enjeux de confidentialité et de souveraineté des projets demandeurs et les offres de « Clouds privés » fournies par des acteurs de confiance sont à privilégier.

Ces plateformes doivent s'appuyer sur des architectures matérielles et logicielles à l'état de l'art. Au niveau matériel, l'infrastructure doit être dimensionnée pour héberger plusieurs centaines de téraoctets de données et fournir du traitement sur différents types de processeurs (CPU, GPU, FPGA,...).

Au niveau logiciel, le volume de données visé privilégie des bases de données de type NoSQL avec, par exemple, des canevas logiciels issus de l'open source comme Hadoop, ElasticSearch,...

L'offre de service de ces plateformes doit également inclure l'instanciation à la demande de pipeline de traitement de données se basant sur des librairies d'apprentissage statistique à l'état de l'art comme Spark, TensorFlow, PyTorch, Scikit-Learn,...

DOMAINES D'ACTIVITÉ DE LA CYBER

(OU SEGMENTATION MARCHÉS)

Les différentes technologies et services décrits au paragraphe précédent n'ont pas d'intérêt en eux-mêmes, mais comme briques intégrées dans des solutions.

Il est donc nécessaire de définir une classification ou segmentation de niveau supérieur par grands domaines d'activité cyber, ou par grands secteurs du marché de la cyber.

Dans les domaines des télécommunications ou des réseaux informatiques ou de communications, les classifications usuellement adoptées sont des classifications par couches (layers), comme pour le modèle OSI (Open System Interconnection).

À titre d'exemple, dans le domaine des TIC, il est fréquemment utilisé la segmentation suivante :

- Management
- Applications
- Communications
- Réseaux
- Terminaux

Cette segmentation n'est pas applicable dans l'état car elle est incomplète pour le domaine cyber. Il est donc nécessaire d'en définir une plus précise couvrant l'ensemble des domaines concernés tout en restant dans une approche par couche (couches basses, couches hautes) comme pour le modèle OSI. La liste ci-dessous présente les grands domaines du monde cyber. Cette liste pourra évoluer en fonction de l'évolution de ces marchés.

Services	Services
Intelligence Artificielle	Artificial Intelligence
Authentification et identité numérique	Authentication & Identity management
Analyseurs, gestion et supervision	Analysers, management & supervision
Cloud	Cloud
OS et applications	OS & applications
Communications et transactions	Communications & transactions
Réseaux industriels	Industrial networks
Réseaux	Networks
Terminaux et objets connectés	End point & IoT
Composants et hardware	Chipset & hardware

Ces domaines peuvent ensuite être appliqués à des secteurs d'activité comme indiqué au chapitre D : cas d'usage.

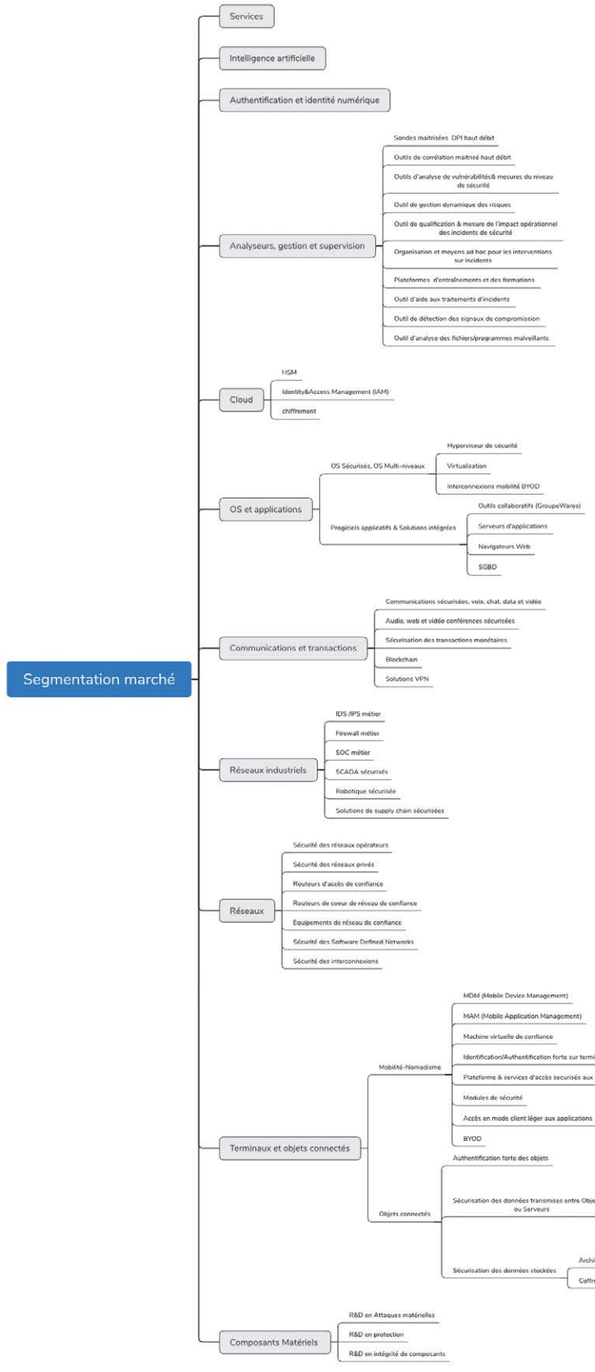


Figure 6 : Segmentation marché

C.1 Services

Les différents services du domaine cyber sont décrits au chapitre B (B.1.3 pour la cyber-protection, B.2.3 pour la cyber-résilience, B.3.3 pour les services liés à la cyberdéfense, et B.4.3 pour les services liés au cyber-renseignement).

C.2 Intelligence Artificielle

Se reporter au paragraphe B.6 qui propose un zoom sur l'utilisation de l'Intelligence Artificielle en cybersécurité.

C.3 Authentification et identité numérique

Chacun utilise une ou plusieurs identités numériques pour accéder aux différents services offerts sur l'Internet. La gestion de ces identités pose des problèmes techniques, par exemple autour de l'identification et de l'authentification et des supports ou techniques associés (support d'identité numérique, biométrie, certification, ...), mais aussi des problèmes juridiques (respect de la vie privée, droit à l'image, droit à l'oubli, usurpation d'identité, ...). Le sujet de l'identité numérique intègre aussi celui de l'anonymat qui pose lui aussi des problèmes techniques et juridiques complexes.

En particulier, le volet juridique de la gestion des identités numériques est extrêmement sensible en ce qu'il touche à la réglementation des données à caractère personnel. Ces données font l'objet d'un cadre juridique d'inspiration européenne avec l'entrée en vigueur du RGPD en mai 2018, complété par la loi informatique et libertés modifiée par la loi du 20 juin 2018.

Les textes placent la prévention des risques d'atteintes aux données personnelles comme une obligation, par la mise en place du concept de protection de la vie privée dès la conception (privacy by design). Il s'agit de la prise en compte des données personnelles au stade de la conception des produits et services, mais aussi de l'actualisation des processus au cours de l'exploitation de ceux-ci.

En complément, c'est tout un système de recueil et de conservation des données personnelles qui est imposé, du consentement de la personne concernée à la suppression des données, en passant par le stockage en Europe ou en dehors. Sur cette dernière obligation, le RGPD favorise le stockage des données personnelles au sein de l'Union Européenne, même s'il prévoit la possibilité de conclure des accords pour garantir le même niveau de sécurité avec un pays non-membre de l'UE (à titre d'exemple, le privacy shield avec les Etats-Unis).

Cette réglementation n'est pas seulement incitative puisqu'elle prévoit des amendes administratives dissuasives en cas de non-respect des principes liées à la protection des données personnelles. Ces sanctions peuvent se cumuler avec une action pénale voire une demande de dommages et intérêts.

C'est pour toutes ces raisons, que, à titre d'exemple, l'arrêté du 8 novembre 2018 relatif au fonctionnement de la solution d'accès universel aux administrations en ligne, FranceConnect[11], précise le périmètre des données à caractère personnel, les acteurs qui en sont destinataires et les modalités de leur conservation.

La croissance fulgurante de la dématérialisation des services, qu'ils soient étatiques (impôts, Assurance Maladie, ...) ou privés (gestion de ses comptes bancaires, réservations en ligne, achats en ligne, ...) accroit la criticité et les enjeux de l'identité numérique.

En alternative à la suprématie des GAFAM (Google Apple Facebook Amazon Microsoft) principaux fournisseurs d'identité, l'Union Européenne et les états se préoccupent de la problématique, avec l'objectif de promouvoir la mise en place d'une identité numérique européenne ou nationale respectueuse des lois adoptées pour la protection des citoyens.

11 https://franceconnect.gouv.fr/

C.4 Analyseurs, gestion et supervision

On va retrouver dans ce domaine l'ensemble des produits, technologies et services décrits au chapitre § B.1 ci-dessus.

Leurs besoins et leurs enjeux découlent donc directement de ceux-ci.

C.5 Cloud

Le Cloud public pose un ensemble de problèmes de sécurité notamment pour le contrôle de l'accès aux données. La protection de ces données en confidentialité ou intégrité vis-à-vis de tiers, que ceux-ci soient au sein du fournisseur de service ou qu'ils soient externes et non autorisés, est bien entendu une préoccupation constante.

Pour cette raison, les techniques de chiffrement pourront être utilisées aux niveaux transport, stockage ou applicatif. Les contraintes particulières du cloud pourront nécessiter le développement de nouvelles techniques cryptographiques (chiffrement homomorphe, par exemple).
À la croisée d'autres domaines, il existe également la gestion des identités pour garantir un accès sécurisé quels que soient le lieu ou le moyen d'accès aux données.

Le contrôle des organisations ou des personnes et des moyens qui administrent ou exploitent les données est en particulier nécessaire si l'on souhaite préserver les intérêts d'un état, assurer la protection de ses citoyens ou encore éviter l'espionnage industriel.

Précisément sur ce point l'extraterritorialité du droit états-unien prolongée avec le Cloud ACT du 23 mars 2018 (Clarifying Lawful Overseas Use of Data) renforce l'intérêt pour les états de disposer de services Clouds souverains.

En effet, cette loi contraint, sur simple réquisition judiciaire, tous fournisseurs de services de communications électroniques, dont les fournisseurs de services d'hébergement dans le Cloud, soumis à la juridiction états-unienne, indépendamment de leur localisation physique ou de leur nationalité, à fournir les données de communications en leur possession et contrôle, pouvant inclure des données stratégiques d'entreprise ainsi que des données à caractère personnel de leurs clients.

Compte tenu des critères d'appréciation étendus de soumission au droit états-unien (nature, degré de contact avec les États-Unis, etc.), cette disposition fait légitimement craindre que des données à caractère personnel hébergées par un fournisseur européen de services Cloud puissent être communiquées aux autorités judiciaires états-uniennes, hors de tout contrôle des clients dudit prestataires de services cloud.

De plus, ce texte pose la question de la licéité des transferts de données d'un fournisseur européen vers les autorités états-uniennes, au regard du droit de l'Union européenne, à travers l'article 48 du RGPD, établissant que « toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international », lequel n'existe pas encore.

C.6 OS et applications

C.6.1 _OS Sécurisés et OS Multi-niveaux

Le paragraphe B.1.2.2.4.4 détaille cette rubrique.

C.6.2 _Progiciels applicatifs & Solutions intégrées

Dans ce domaine, il est nécessaire d'accompagner les évolutions des architectures applicatives afin de les sécuriser au juste niveau :

- Travail collaboratif ;
- Serveurs applicatifs ;
- Clients légers ;
- Applicatifs Java ;
- ...

En complément, il reste de gros enjeux autour de la sécurisation des bases de données, tant pour la protection de leurs contenus que du contrôle de leurs accès.

C.7 Communications et transactions

Sécuriser les réseaux n'est pas suffisant pour contrer l'ensemble des menaces sur les communications. Il est très souvent nécessaire de sécuriser les flux audio, vidéo, de messagerie instantanée (chat) ou de données. De même, le développement de la visio-conférence pour du travail collaboratif à haute valeur ajoutée nécessite la mise en place de solutions adaptées. Les solutions VPN (Virtual Private Network) utilisées notamment pour l'accès à distance à des réseaux d'entreprises par des postes nomades sont également à prendre en compte dans cette catégorie.

Les nouvelles technologies dites de « blockchain » qui permettent de sécuriser les transferts d'information ou les transactions sans tiers de confiance ou organe central de contrôle vont jouer un rôle majeur dans les années à venir dans un certain nombre de domaines. Elles viennent compléter les solutions plus historiques, qui restent toutefois indispensables pour la sécurisation des transactions monétaires.

C.8 Réseaux industriels

Les réseaux industriels ou plus généralement les systèmes de contrôle industriel (SCI), parfois improprement appelés SCADA (Supervisory Control and Data Acquisition, le logiciel du système de contrôle industriel), se retrouvent dans une infinité de domaines que ce soit pour le pilotage de processus industriels, la gestion technique bâtimentaire, ou de nombreux systèmes d'armes.

Leur positionnement à l'interface entre un domaine informatique (des applications métiers) et un système physique via des ensembles de capteurs et d'actionneurs, en font des systèmes particulièrement sensibles en terme de sécurité.

Comme l'ont prouvé des exemples médiatisés (Stuxnet, Flame, ...), une attaque informatique sur des systèmes de ce type peut avoir des conséquences dans le monde physique, provoquant des pertes de services (coupure électrique, perturbation de l'alimentation en eau potable, ...) voire des accidents entrainant des pertes humaines (blocage de la manœuvrabilité d'un navire dans un port ou en mer, ...).

Ce domaine pose de nombreux défis, dus notamment aux spécificités de ce milieu :

- Systèmes souvent temps réel ;
- Difficultés de mise à jour des équipements (coût de l'arrêt d'une ligne de production, accessibilité, ...) ;
- Protocoles parfois spécifiques ;
- ...

Ce domaine inclut également la sécurisation des solutions de robotique et des solutions de chaine logistique (supply chain).

Les solutions informatiques existantes, dites « sur étagères », ne sont donc pas capables de répondre à tous les besoins. Ce domaine est très vaste et encore peu exploré, même si la profusion d'articles scientifiques sur le sujet et les productions des grands fournisseurs de solutions évoluent rapidement.

C.9 Réseaux

Ce chapitre concerne l'ensemble des équipements et des solutions qui constituent les réseaux de transmissions et de communications, du niveau 1 au niveau 3. Il regroupe les équipements de transmission électriques ou optiques, les commutateurs des réseaux locaux (Local Area Network (LAN) de niveau 2 ainsi que les routeurs d'accès, d'agrégation et de cœur de réseau de niveau 3.

La sécurité des réseaux est un domaine historique de la SSI. En dehors du chiffrement des liaisons qui est bien maîtrisé, se pose la question de la maîtrise des équipements, des protocoles et des services qui constituent le cœur des réseaux des opérateurs. Le fonctionnement global de notre société repose sur la disponibilité des services de communication, et les conséquences d'un arrêt général ces services aurait un impact considérable, tant sur le fonctionnement de l'Etat que celui des entreprises. L'évolution vers des architectures réseau dites SDN (Software Defined Networking), la virtualisation et donc potentiellement la délocalisation de fonctions intelligentes des réseaux) va engendrer des problèmes de sécurité et de confiance d'un genre nouveau.

Dans un autre registre, l'interconnexion de réseaux de sensibilités différentes, la connexion entre un Intranet et Internet, entre un réseau industriel et un réseau bureautique, les nouveaux usages (par exemple Bring Your Own Device (BYOD), en français Apportez Votre Equipement personnel de Communication (AVEC)) génèrent de nouveaux problèmes: fuite des données sensibles de l'entreprise, intégrité des données, pollution du SI par des logiciels malveillants, déni de service, ...

C.10 Terminaux et objets connectés

C.10.1 _Mobilité-Nomadisme

Le domaine du nomadisme va concerner plusieurs types de préoccupations :

- La sécurité des terminaux :
  Outils de travail au quotidien, les smartphones ou tablettes contiennent des informations sensibles pour les entreprises et sont particulièrement susceptibles d'être perdus ou volés. Par ailleurs ils ont souvent un usage mixte (privé/professionnel) qui les rend vulnérables à de multiples problèmes de sécurité. La généralisation des comportements de type BYOD ne font qu'augmenter les risques encourus ;
- La gestion des terminaux et des applications :
  Les flottes de terminaux peuvent compter des centaines voire des milliers d'objets qu'il faut pouvoir gérer, tracer, mettre à jour, ... Le problème est identique pour les applications métiers ;
- Les accès aux systèmes d'information de l'entreprise :
  Les terminaux mobiles doivent se connecter au(x) SI de l'entreprise. Il faut se prémunir contre les usurpations, les connexions suite à un vol ou à une perte d'un terminal ou des données qu'il contient, des intrusions via ces points d'accès externes.

C.10.2 _Objets connectés

Le domaine des objets connectés connait une explosion considérable avec des milliards d'objets produits, que ce soit dans les domaines industriels, dans celui du commerce et de la distribution, dans le médical ou pour une utilisation personnelle.

Jusqu'à aujourd'hui, la sécurité a rarement été prise en compte, tant au niveau des connexions, qui sont en généralement assurées via des connexions sans fils, qu'au niveau des applications qui gèrent ces masses de données. Les risques concernent par exemple la vie privée, via la collecte de milliers d'informations sur les habitudes de vie, la santé ou la vie sociale, émises par des objets autonomes.

Ces données sont susceptibles d'être écoutées par des tiers non autorisés (collecte d'images, informations sur la présence ou l'absence de personnes dans un lieu, ...). Leur prise de contrôle à distance qui pourrait provoquer des accidents graves (dispositifs médicaux implantés, matériels hospitaliers, ...).

Dans tous les cas, des masses de données issues de capteurs différents peuvent être agrégées et corrélées pour caractériser des comportements individuels.

C.11 Composants et hardware

Les composants matériels sont les briques de base des outils numériques. Dès que l'on souhaite un haut niveau de sécurité, il est indispensable de maîtriser le matériel sous-jacent. Les composants peuvent être une source de menaces, s'ils contiennent des vulnérabilités ou des pièges qui peuvent permettre à un agresseur de contourner les mesures de protection logicielles misent en œuvre par ailleurs.

D'un autre côté, ils peuvent aussi renforcer considérablement la sécurité d'un objet en rendant inopérantes les modifications du logiciel en vue de mener une attaque.

Par exemple, il est beaucoup plus facile de protéger un logiciel contre la copie en s'appuyant sur un élément matériel qu'en se basant uniquement sur une solution logicielle.

CAS D'USAGE _

Les chapitres précédents ont abordé le sujet via une approche technologique. Il est maintenant utile de croiser cette approche avec une analyse des cas d'usage, c'est-à-dire des domaines métiers où ces technologies, produits et services peuvent être utilisés. Pour ce faire, il nous semble intéressant d'identifier des critères qui peuvent être dimensionnant pour les solutions ou les produits.

Dans un premier temps, nous nous proposons d'utiliser deux critères :

- Son domaine d'activité, et donc les risques devant être adressés ;
- La taille de l'entité utilisatrice des produits ou services de cybersécurité.

D'autres critères différenciant peuvent être envisagés, comme par exemple l'implantation internationale qui peut entrainer l'obligation de répondre à des législations ou des directives nationales de sécurité différentes. Les retours d'expériences de l'utilisation des différents cas d'usages conduiront à introduire si nécessaires d'autres critères.

Chaque produit ou service cyber pourra au final être caractérisé selon :

- Ses briques technologiques (chapitre B) ;
- Son domaine fonctionnel (chapitre C) ;
- Son (ou ses) cas d'usage(s) (chapitre D).

Cette analyse peut permettre d'identifier la nécessité d'adaptation de produits existants, de développement de nouveaux produits, ou de travaux de R&D :

- Adaptation à un nouveau cas d'usage pour un produit existant ;
- Déclinaison en gamme d'outils ou de services pour répondre aux moyens techniques susceptibles d'être financés selon le type de client ;
- ...

D.1 Analyse des cas d'usage selon le secteur d'activité

Chaque secteur d'activité a ses propres contraintes, techniques, organisationnelles, réglementaires voire culturelles. Il est donc crucial que les produits et services proposés soient en adéquation avec ces réalités.

L'analyse détaillée des cas d'usage et donc des besoins afférents devra être réalisée en collaboration avec les acteurs concernés, qui seuls peuvent exprimer un besoin pertinent. À titre d'exemple, voici une première liste de cas d'usages liés à des activités essentielles :

- Transports :
  - Automobile et infrastructure routière connectée ;
  - éronautique ;
  - Navires et navigation maritimes ;
  - Infrastructures ferroviaires ;
  - Production et distribution d'énergie (smart energy, y compris smart grids) ;
- Gestion de l'eau (distribution et retraitement) ;
- Santé ;
- Systèmes de communication ;
- Domotique / gestion technique bâtimentaire ;
- Banques / assurances ;
- Usine du futur :
  - Industries agro-alimentaires ;
  - Cobotique et robotique industrielle ;
  - Industries culturelles et créatives ;
- Drones et robots ;
- Protection de la vie privée ;
- Villes intelligentes (smart cities).

D.1.1 _Transports

Le domaine des transports se caractérise par un nombre d'opérateurs très importants (c'est un peu moins vrai pour le ferroviaire) et donc une organisation extrêmement distribuée. Cette structure apporte de manière générale une meilleure résilience que dans d'autres domaines.
Par contre, il est possible d'identifier un risque commun pour tous les acteurs, le risque de pertes humaines et de dysfonctionnement majeur de la société dans le cas d'un accident lié à une cyber-attaque.

D.1.1.1 _Automobile connectée

L'automobile devient un objet connecté, que ce soit dans le cadre d'une utilisation personnelle ou professionnelle (gestion de flotte, suivi de trajets, hyper-connectivité, ...). De nombreux articles ont montré la vulnérabilité potentielle des architectures actuelles et des travaux ont été lancés pour les sécuriser. Les risques sont liés à la multiplication des calculateurs, à la connexion entre des bus temps réels pour les fonctions de conduite et de sécurité (ABS, ESP, gestion moteur, ...) et des bus utilisés pour des fonctions de confort ou de divertissement.
L'arrivée de ports de type USB permettant la connexion de supports amovibles courants et la généralisation de l'intégration de fonctions de téléphonie mobile offrent tout à la fois des portes d'entrées pour l'introduction de logiciels malveillants, et des liens pour les activer ou les piloter à distance. Il convient alors d'imaginer des attaques ciblées ou aléatoires pouvant causer des dommages matériels pouvant aller jusqu'à des pertes humaines.

Les travaux qui sont menés sur les véhicules autonomes (fonctionnement automatique sans intervention du conducteur) renforcent bien évidemment le besoin de disposer de solutions de sécurité éprouvées. Cette dynamique suppose que le niveau de sécurité exigé se rapproche de celui des applications aéronautiques critiques.

D.1.1.2 _Aéronautique

Le domaine aéronautique est très vaste et recouvre à la fois les aéronefs, les infrastructures aéroportuaires et la gestion du trafic aérien.

La sureté de fonctionnement est une préoccupation permanente dans ce domaine, notamment en ce qui concerne les aéronefs, avec des règles de certification très poussées. La prise en compte de menaces cyber s'effectue progressivement, à mesure que l'évolution des techniques et des usages augmente les risques potentiels.

Pour exemple, il convient de citer les réseaux de divertissement à bord, qui permettent aux passagers de connecter leurs propres équipements, sachant qu'il existe des liens potentiels entre ces réseaux et les réseaux liés au pilotage de l'appareil.

Par ailleurs, les aéronefs disposent de multiples moyens de connexion vers l'extérieur, qu'ils soient liés à la navigation (liens radio avec le contrôle aérien), à la maintenance (liens vers le constructeur de l'appareil) ou aux services offerts aux passagers (connexions internet, téléphones mobiles en vol).
Ces liaisons constituent des portes d'entrées potentielles pour des attaquants.

En termes d'infrastructures aéroportuaires, la logistique des aéroports et le contrôle aérien sont assurés par de nombreux systèmes informatiques.

Pour le premier point, le risque principal à identifier concerne l'indisponibilité des services qui peut entraîner un blocage du trafic par l'incapacité à gérer les flux de passagers ou le ravitaillement des avions.

Pour le second, l'indisponibilité doit aussi être considérée pour les mêmes raisons, mais on peut y ajouter les risques sur l'intégrité des informations liées aux vols. À cet égard, des solutions protégeant les radars de surveillance aérienne contre les risques de cyber attaques (par exemple, ajout ou suppression de pistes radars) sont d'ores et déjà proposées.

D.1.1.3 _Navires et navigation maritime

Les navires modernes intègrent de multiples systèmes numériques pour la gestion de l'ensemble des fonctions du bord : propulsion, navigation, production d'énergie, gestion de l'eau douce, contrôle du fret, … Ces systèmes mixent de l'informatique classique et des systèmes de contrôle industriels. Par ailleurs, la réduction des équipages entraîne une forte dépendance des liaisons vers la terre pour assurer la maintenance de ces systèmes embarqués.

Le risque principal concerne la disponibilité et l'intégrité des systèmes, avec des conséquences très variées, qui vont de l'immobilisation d'un navire à sa prise de contrôle à distance avec des effets potentiels graves (collisions entre navires, échouage, pollution maritime, ….

Concernant les systèmes de navigation maritime, la situation est proche de celle du transport aérien.

Les infrastructures portuaires sont elles aussi très dépendantes de l'informatique. Une indisponibilité pourrait conduire à un blocage progressif du trafic commercial ou des passagers, avec des impacts rapides sur l'économie.

En effet une grande part du trafic international utilise la voie maritime. La confidentialité et l'intégrité des échanges est aussi un aspect à prendre en compte.

Comme l'a montré une cyber attaque sur le port d'Anvers il y a quelques années, des trafiquants ayant accès aux systèmes portuaires peuvent réaliser des vols de grande envergure.

D.1.1.4 _Infrastructures ferroviaires

Les infrastructures ferroviaires sont sensibles aux risques liés à la disponibilité, qui peuvent conduire à de graves perturbations du trafic. Leur intégrité doit aussi être protégée, cela pour éviter qu'une prise de contrôle n'ait de conséquences sur la sécurité des passagers ou des riverains (déraillement ou collisions de trains de passagers ou de matières dangereuses).

D.1.2 _Production et distribution d'énergie (y compris smart grids)

L'énergie électrique est vitale pour assurer le fonctionnement de l'ensemble de la société. Par ailleurs, les usines de production d'électricité notamment celles basées sur l'énergie nucléaire sont des sites particulièrement sensibles. La production doit être protégée contre les cyber-attaques, l'intégrité des systèmes d'information et la disponibilité des systèmes industriels doit être garantie. Quant à l'absence de connexion directe entre les réseaux critiques et les réseaux ouverts, elle ne doit pas être considérée comme une barrière absolue, la diffusion de l'attaque Stuxnet illustre cela.

Au niveau de la distribution, une mise en indisponibilité globale ou partielle du réseau aurait des conséquences économiques et sociétales très importantes si elle devait durer quelques heures si la coupure est totale, voire quelques jours.

Les réseaux intelligents (smarts grids) élargissent la dimension sécuritaire en multipliant les points d'accès au système d'information, en agrandissant donc la surface d'attaque, en ouvrant une inter-connectivité entre la sphère de distribution et celle de la consommation. D'autres vulnérabilités de nature plus commerciales (masquage de consommation, …) peuvent aussi apparaitre avec des impacts financiers ou d'image.

D.1.3 _Gestion de l'eau (distribution et retraitement)

L'eau potable est une ressource importante pour de nombreux secteurs et pour le grand public. L'accès aux systèmes de traitement de l'eau potable pourrait entraîner des risques sur la santé. L'arrêt de la distribution imposerait des mesures complexes de distribution d'eau potable vers la population et des impacts pour certains secteurs d'activités.

Au niveau des systèmes de traitement, une prise de contrôle de stations d'épuration pourrait impliquer des pollutions des milieux naturels. En revanche, la gestion de l'eau étant essentiellement locale, les impacts seront dans tous les cas limités à une zone géographique de faible extension, la mise en place d'une attaque de grande ampleur étant complexe à réaliser.

D.1.4 _Santé

Le domaine de la santé comprend de grands systèmes de dimension Nationale, comme ceux de l'assurance maladie et des systèmes plus décentralisés pour la gestion des hôpitaux ou de structures résidentielles / personnelles dotées de dispositifs médicaux assistés. Des risques d'indisponibilité ou d'intégrité des données peuvent être à l'origine de fraudes qui occasionnent des impacts financiers, une responsabilité pénale de l'organisation, ou une perte de confiance des patients et des personnels.

La multiplication des dispositifs implantés ou d'auto diagnostic fait apparaitre d'autres risques pouvant avoir des impacts plus directs sur la santé, voire sur la vie des patients.

D.1.5 _Systèmes de communication

Sans systèmes de communication l'activité de la plupart des entreprises s'arrête ou est au moins fortement ralentie. Il existe donc des besoins forts sur la disponibilité globale des grandes infrastructures de communication.
Il est aussi important de garantir la protection des données échangées, que ce soit pour la protection de la vie privée, le secret des affaires ou la propriété intellectuelle.

D.1.6 _Domotique / gestion technique de bâtiments

Après un démarrage poussif, la domotique est pleine croissance grâce à la généralisation de l'Internet, qui permet des accès à distance simplifiés avec des débits maintenant compatibles la vidéo mais aussi d'autres services ; la miniaturisation et à la baisse de coût des capteurs et l'utilisation des protocoles sans fils de type WiFi facilitent leurs connexions. Du point de vue des particuliers ou des entreprises utilisateurs de solutions domotiques, il est important que ces systèmes, qui assurent notamment la protection contre le vol, ne puissent pas être neutralisés ou détournés de l'usage pour lequel ils ont été conçus (capture de flux vidéo de caméras de surveillance, par exemple).

D.1.7 _Banques / assurances

Dans le domaine des banques et assurances, figurent des préoccupations autour de la disponibilité des services, mais surtout des craintes sur l'intégrité des échanges ou des données qui pourrait avoir de graves conséquences. Pour exemple, il convient de relever les fraudes sur les mouvements bancaires, mais aussi les attaques potentielles contre les marchés financiers qui pourraient conduire, à cause de l'automatisation très poussée de ce domaine, à des mouvements incontrôlables : crise boursière, manipulation des cours, ...

Des incidents, même de moindre importance mais largement médiatisés peuvent aussi avoir des conséquences fortes sur les entreprises concernées en termes de dégradation de leur image.

D.1.8 _Usine du futur

D.1.8.1 _Industrie et agro-alimentaire

L'industrie agroalimentaire utilise des systèmes de contrôle industriels pour la réalisation des produits. Un accès frauduleux à une chaîne de fabrication pourrait conduire à des produits dangereux pour la santé humaine (ou animale) : mauvais dosage de certains ingrédients, mauvais contrôle de température, mauvais stockage, ... Les conséquences en termes d'image ou de santé publique pourraient être très lourdes pour les entreprises qui seraient touchées.

D.1.8.2 _Cobotique et robotique industrielle

L'automatisation de plus en plus forte de la production peut entraîner des risques soit visibles (par exemple l'arrêt d'une activité suite à une cyberattaque) soit insidieux (telle la modification malveillante du processus industriel, un sabotage).

D.1.8.3 _Industries culturelles et créatives

Pour des industries culturelles et créatives, les attaques de plusieurs médias français montrent qu'une vulnérabilité sur le réseau informatique interne peut conduire à un impact immédiat sur la « production » (ici les programmes diffusés par la chaîne). Les impacts financiers directs (pertes de revenus publicitaires, ...) ou indirects (perte d'image) peuvent être très importants.

D.1.9 _Drones et robots

L'usage de drones et de robots télécommandés est en pleine explosion que ce soit pour des applications ludiques ou professionnelles. Les cas récemment médiatisés de survol de sites sensibles par des drones montrent les risques potentiels liés à ces objets. Des risques qui peuvent être liés à une prise de contrôle à distance d'un drone en vol, et à l'utilisation de drone comme projectile, emportant une charge explosive ou une arme. Ce sujet est très dual compte tenu des applications militaires des drones.

Cette problématique sera encore renforcée avec l'apparition de drones ou robots de plus en plus autonomes.

D.1.10 _Protection de la vie privée

La multiplication des applications numériques, des réseaux sociaux et des usages associés constituent un véritable défi qui peut potentiellement remettre en cause la notion même de vie privée. Il est nécessaire de disposer de solutions permettant à chacun de maîtriser les informations numériques qu'il souhaite diffuser ou celles qu'il souhaite garder dans un cercle maîtrisé.

À cet égard, un équilibre entre cette protection de la vie privée et la nécessaire imputabilité des actions est à trouver pour éviter que ces outils ne soient utilisés à des fins commerciales (données médicales revendues aux assureurs), délictueuses ou criminelles

D.1.11 _Villes intelligentes (Smart cities)

Le concept de ville intelligente (smart city) recouvre un domaine assez vaste et certains termes abordés plus haut pourraient en faire partie. La caractéristique de la ville intelligente est la surface d'attaque due à l'étendue géographique des villes et la multiplicité des capteurs et actionneurs qui permettent de rendre les nombreux services.

Les dysfonctionnements possibles en cas de cyber attaque sont potentiellement conséquents, ils peuvent être utilisés pour renforcer l'effet d'attaques physiques concomitantes (par exemple, la désorganisation du trafic qui provoque un engorgement de la circulation juste avant un attentat afin de bloquer l'arrivée des secours).

D.2 Analyse des cas d'usage selon la taille des entreprises

Trois grandes catégories sont ici considérées :

- Le grand public et les TPE, auxquels on pourra aussi raccrocher les petites collectivités territoriales (mairies ou communautés de communes rurales) ;
- Les PME/PMI et ETI, ainsi que les collectivités territoriales plus conséquentes (villes, départements, régions) ;
- Les grands groupes, les OIV et les administrations d'Etat ou les métropoles.

Par rapport à l'analyse du marché cyber, ces différents groupes se caractérisent par leurs capacités diverses en termes d'expertise interne ou de moyens financiers et humains.

Les produits ou les services pour le groupe 1 doivent être simples d'utilisations, quasi autonomes ou administrés par des tiers, car les entités concernées n'ont pas les capacités techniques, humaines ou financières pour mettre en œuvre ces systèmes complexes.

A contrario, les OIV ou les grandes administrations pourront vouloir être autonomes, et elles auront besoin de solutions pour gérer des milliers de systèmes hétérogènes.

De même, le niveau de confiance dans les produits, qui est lié aux types de menaces contre lesquelles on veut se prémunir, sera différent entre une TPE, un OIV et une entité gouvernementale. Les PME ou ETI, selon leur activité, pourront se rattacher à l'un ou l'autre groupe. Ainsi, apparaît la nécessité de créer des gammes de produits et de services adaptés à ces différents types de marchés.

Les modes de commercialisation pourront aussi être différents avec :

- Des marchés de masse et des produits plutôt génériques lorsqu'on adresse le groupe 1 ;
- Du produit spécifique ou une intégration particulière pour le groupe 3 avec un marché beaucoup plus restreint en nombre.

E

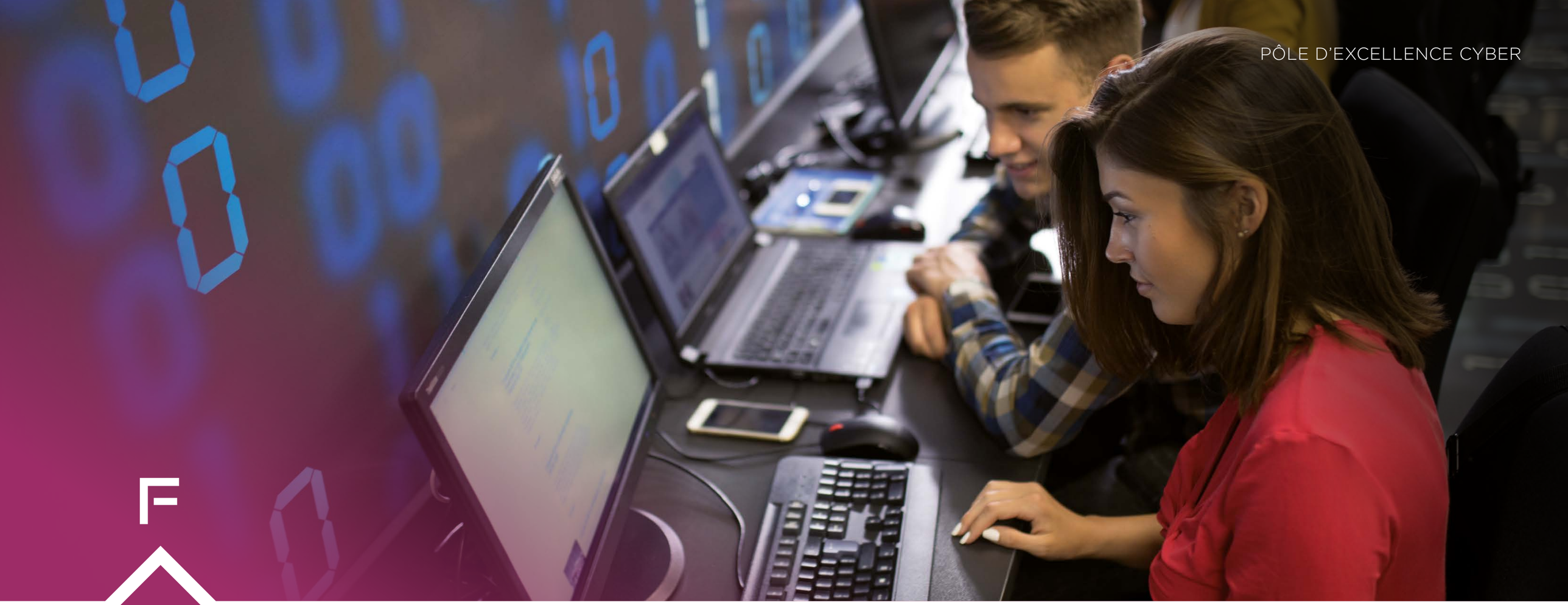
LES RESSOURCES HUMAINES _

La disponibilité de ressources compétentes et formées reste un enjeu stratégique pour le développement de la filière du numérique en France. Dès sa création, le Pôle d'excellence cyber s'est inscrit dans la démarche de l'ANSSI pour créer un groupe de travail dédié à l'élaboration d'une liste de profils métiers dans le domaine de la sécurité du numérique.

Ce groupe de travail, composé de représentants de l'enseignement supérieur et du monde industriel, a établi une liste de métiers[12] qui sont détaillés sur le site de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Nous présentons dans le tableau ci-dessous les cinq grandes classes de métiers.

DOMAINE	MÉTIERS
Pilotage, Organisation et Gestion des risques (POG)	Responsable de la Sécurité des Systèmes d'Information (RSSI)
	Correspondant sécurité
	Spécialiste en gestion de crise cyber
	Responsable du plan de continuité d'activité (RPCA)
Management de Projets et Cycle de vie (MPC)	Chef de projet sécurité
	Développeur sécurité
	Intégrateur de sécurité
	Architecte sécurité
Operation et Maintien en Condition Operationnelle (OMCO)	Administrateur sécurité
	Technicien sécurité
Support et Gestion des Incidents (SGI)	Analyste SOC
	Expert réponse à incident
Conseil, Audit, Expertise (CAE)	Consultant sécurité «organisationnel».
	Consultant sécurité «technique».
	Cryptologue
	Juriste spécialisé en cybersécurité
	Évaluateur sécurité
	Analyste de la menace
	Délégué à la Protection des Données (DPD)

12 https://www.ssi.gouv.fr/particulier/formations/profils-metiers-de-la-cybersecurite/



LES DOMAINES DE RECHERCHE ACADÉMIQUE _

Les domaines académiques de recherche en cybersécurité couvrent un large spectre dont la combinaison est la condition du succès. Ces domaines sont structurés selon la typologie de l'ACM (Association for Computing Machinerie).

Cette association américaine à but non lucratif, éditrice de nombreuses revues de référence, met à jour régulièrement une taxonomie de la recherche en informatique comprenant un volet sécurité, qui constitue un standard de facto de classification de la recherche en informatique. Pour cette raison, il est utile de présenter ici une table de correspondance entre les deux approches.

Cette première correspondance entre ces axes de recherche académique et les produits, technologies et domaines fonctionnels permet de mettre en évidence l'apport potentiel de la communauté académique au développement de la filière.

Taxonomie de l' « Association for Computing Machinerie »	Référentiel PEC
Cryptography	
Key management	Cyber-protection-Produits & technologies-technologies-cryptographie
Public key (asymmetric) techniques	Cyber-protection-Produits & technologies-technologies-cryptographie
Digital signatures	Cyber-protection-Produits & technologies-technologies-cryptographie
Public key encryption	Cyber-protection-Produits & technologies-technologies-cryptographie
Symmetric cryptography and hash functions	Cyber-protection-Produits & technologies-technologies-cryptographie
Block and stream ciphers	Cyber-protection-Produits & technologies-technologies-cryptographie
Hash functions and message authentication codes	Cyber-protection-Produits & technologies-technologies-cryptographie
Cryptanalysis and other attacks	Cyber-protection-Produits & technologies-technologies-cryptographie
Information-theoretic techniques	Cyber-protection-Produits & technologies-technologies-cryptographie
Mathematical foundations of cryptography	Cyber-protection-Produits & technologies-technologies-cryptographie
Formal methods and theory of security	
Trust frameworks	Cyber-protection-méthodes-environnement de conception sécurisé
Security requirements	Cyber-protection-services-ingénierie système
Formal security models	Cyber-protection-méthodes-méthodes formelles
Logic and verification	Cyber-protection-méthodes-méthodes formelles
Security services	
Authentication	Cyber-protection-produits & technologies
Biometrics	Cyber-protection-produits & technologies
Graphical / visual passwords	Cyber-protection-produits & technologies
Multi-factor authentication	Cyber-protection-produits & technologies
Access control	Cyber-protection-produits & technologies
Pseudonymity, anonymity and untraceability	Cyber-protection-produits & technologies
Privacy-preserving protocols	Cyber-protection-produits & technologies
Digital rights management	Cyberprotection-produits & technologies-technologies-informatique de confiance
Authorization	Cyber-protection-produits & technologies
Intrusion/anomaly detection and malware mitigation	
Malware and its mitigation	Cyberdéfense-produits &technologies de LID-analyse de malware
Intrusion detection systems	Cyberdéfense-produits &technologies de LID-détection d'intrusion
Social engineering attacks	Méthodes de LID-connaissance de la menace
Spoofing attacks	Méthodes de LID-connaissance de la menace
Phishing	Méthodes de LID-connaissance de la menace
Vulnerability management	Cyber-protection-services-évaluation-évaluation système
Penetration testing	Cyberdéfense-produits &technologies de LID
Vulnerability scanners	Cyberdéfense-produits &technologies de LID
File system security	Cyber-protection-produits & technologies-produits
Network security	
Security protocols	Cyber-protection-produits & technologies-produits
Web protocol security	Cyber-protection-produits & technologies-produits
Mobile and wireless security	Domaines fonctionnels-mobilité-nomadisme
Denial-of-service attacks	Cyber-résilience-méthodes-résistance aux attaques
Firewalls	Cyber-protection-produits & technologies-produits
Database and storage security	
Data anonymization and sanitization	Domaines fonctionnels-progiciels applicatifs & solutions intégrées
Management and querying of encrypted data	Domaines fonctionnels-progiciels applicatifs & solutions intégrées
Information accountability and usage control	Domaines fonctionnels-progiciels applicatifs & solutions intégrées
Database activity monitoring	Domaines fonctionnels-progiciels applicatifs & solutions intégrées
Software and application security	
Software security engineering	Cyber-protection-produits & technologies-technologies-informatique de confiance
Web application security	Domaines fonctionnels-progiciels applicatifs & solutions intégrées
Social network security and privacy	Cas d'usage-sécurité de la vie privée
Domain-specific security and privacy architectures	Cas d'usages
Software reverse engineering	Cyber-protection-services-évaluation-évaluation logicielle
Human and societal aspects of security and privacy	
Economics of security and privacy	Cas d'usage-sécurité de la vie privée
Social aspects of security and privacy	Cas d'usage-sécurité de la vie privée
Privacy protections	Cas d'usage-sécurité de la vie privée
Usability in security and privacy	Cas d'usage-sécurité de la vie privée
Security in hardware	
Tamper-proof and tamper-resistant designs	Cyber-protection-produits & technologies-technologies-composants électroniques
Embedded systems security	Cyber-protection-produits & technologies-produits-matériel et logiciel embarqué
Hardware security implementation	Cyber-protection-produits & technologies-technologies-composants électroniques
Hardware-based security protocols	Cyber-protection-produits & technologies-technologies-composants électroniques
Hardware attacks and countermeasures	Domaines fonctionnels-composants matériels
Malicious design modifications	Domaines fonctionnels-composants matériels
Side-channel analysis and countermeasures	Cyber-protection-services-évaluation-évaluation composant
Hardware reverse engineering	Cyber-protection-services-évaluation-évaluation composant
Systems security	
Operating systems security	Cyber-protection-produits & technologies-technologies-logiciel sécurisé
Mobile platform security	Cyber-protection-produits & technologies-technologies-logiciel sécurisé
Trusted computing	Cyber-protection-produits & technologies-technologies-logiciel sécurisé
Virtualization and security	Cyber-protection-produits & technologies-technologies-logiciel sécurisé
Browser security	Domaines fonctionnels-progiciels applicatifs & solutions intégrées
Distributed systems security	Domaines fonctionnels-progiciels applicatifs & solutions intégrées
Information flow control	Cyber-protection-produits & technologies-produits
Denial-of-service attacks	Cyber-résilience-méthodes-résistance aux attaques
Firewalls	Cyber-protection-produits & technologies-produits

LES PLATESFORMES _

L'ensemble des éléments présentés dans les précédents chapitres de ce document peut nécessiter à un moment ou à un autre l'utilisation de plateformes. Un des objectifs du pôle d'excellence est donc de s'assurer que la disponibilité de plateformes adaptées (incluant aussi celles intervenant sur des données) permette le développement des actions des partenaires du Pôle d'excellence cyber, et, plus généralement, de la filière cybersécurité et cyberdéfense.

Au sens du Pôle d'excellence cyber, une plateforme de cybersécurité (et de cyberdéfense) est un environnement maîtrisé constitué de moyens techniques, humains, organisationnels, permettant d'appréhender de manière générale différents aspects liés à la cybersécurité.
Une plateforme de cybersécurité est considérée comme un ensemble de « ressources », un « magasin » de moyens (techniques, services, contenus, humains) permettant de répondre à des enjeux (montée en compétence, qualification de produit, capitalisation de savoir et de données, ...). C'est un socle, un collectif de plusieurs ressources permettant de bâtir des projets, des usages ou des services.

Cinq types de plateformes ont été identifiés au sein du GT plateforme du Pôle d'excellence cyber[13] :

- Recherche et développement en cybersécurité (R&D) ;
- Formation et entraînement à la sécurité numérique ;
- Validation et certification de produits ;
- Industrialisation de produits de sécurité ;
- Plateforme en contexte opérationnel.

G.1 Recherche et développement en cybersécurité (R&D)

Une plateforme de recherche en cybersécurité est une plateforme fournissant un environnement et des moyens d'expertiser des systèmes, de mettre en lumière les vulnérabilités de ces systèmes et de proposer des solutions ou des recommandations permettant d'améliorer leur sécurité. Ces plateformes adressent à la fois la recherche académique et la recherche industrielle.

Une plateforme de développement fournit les moyens techniques permettant de mettre en œuvre des produits ou des solutions de cybersécurité. Elle concerne de fait plus particulièrement la production industrielle mais peut aussi faire l'objet de développements dans un contexte académique. Elle peut par exemple, sans être limitative, permettre le développement d'outils ou de scénarios pour les besoins d'expertise en cybersécurité.

G.2 Formation et entraînement à la sécurité numérique

Une plateforme de formation constitue un support permettant principalement de répondre aux besoins de sensibilisation, d'enseignement et d'apprentissage. Elle fournit des moyens techniques, organisationnels, humains, ainsi que des contenus (cours, exercices, etc.) permettant de répondre à ces besoins.

La formation peut être dispensée en présentiel sur des équipements physiques mettant à disposition les cours et les exercices et permettant de réaliser des travaux pratiques sur des configurations matérielles et/ou logicielles. Elle peut également être dispensée en ligne.

L'entraînement se distingue de la formation de par son objectif, qui est de mettre en situation réelle des personnels afin de leur permettre d'acquérir des automatismes et des savoir-faire sur la base de leurs connaissances.

Deux aspects de l'entraînement sont à distinguer :

- L'entraînement au sens «répétition de procédure» (training) permettant d'acquérir des automatismes ;
- L'entraînement au sens « exercice en situation inconnue », permettant notamment d'évaluer les compétences en situation inattendue, en situation de crise.

G.3 Validation et certification de produits

Une plateforme de validation fournit des moyens de tests permettant d'une part de valider la conformité fonctionnelle d'un produit par rapport à ses spécifications et à la documentation associée, et d'autre part de tester sa fiabilité et sa robustesse de fonctionnement dans un environnement représentatif d'une configuration réelle y compris au-delà du domaine d'emploi spécifié. Les validations peuvent par exemple être réalisées par des tiers de confiance qui ont pour mission d'éprouver une configuration proposée par un fournisseur à un client.

La certification s'appuie sur une évaluation généralement réalisée par des centres d'évaluation de la sécurité des technologies de l'information (CESTI ou ITSEF) agréés par l'ANSSI et qui possèdent les moyens matériels, logiciels et humains nécessaires à cette évaluation.

Dans ce contexte, l'évaluation est réalisée suivant des critères normalisés, tels que, par exemple, les critères communs (CC) (norme internationale) ou la Certification de Sécurité de Premier Niveau (CSPN) à l'issue de laquelle une certification est délivrée par l'ANSSI.
Les plateformes de certification nécessitent des compétences d'experts permettant d'élaborer des tests de vulnérabilités (connus ou spécifiques au produit) en vue de rédiger un rapport technique d'évaluation (RTE ou ETR).

G.4 Industrialisation de produits de sécurité

Une plateforme de pré-production peut par exemple permettre de pré-configurer et de qualifier une solution ou un produit vis-à-vis des autres composants d'une architecture. Cela permet notamment de vérifier et contrôler l'impact de l'intégration de ces nouveaux composants dans un environnement technique opérationnel réel.

Les plateformes de démonstration ont pour principal objectif de montrer les vulnérabilités potentielles des systèmes et de promouvoir les produits et les solutions de cybersécurité permettant d'y faire face. Elles permettent de montrer la faisabilité des solutions et les bénéfices que ces dernières peuvent apporter. Elles contribuent de fait au développement industriel et commercial des produits de sécurité.

G.5 Plateforme en contexte opérationnel

Les plateformes dites d'« usage » sont des plateformes techniques réelles (matérielles) et opérationnelles dans lesquelles des solutions de cybersécurité peuvent être intégrées.

Ces plateformes sont soit des environnements de fonctionnement nécessitant des moyens de sécurisation, soit des environnements qui vont assurer la sécurité d'une infrastructure. Ces plateformes d'usage ne sont pas nécessairement des plateformes de cybersécurité, mais peuvent contribuer au développement de la filière en tant que support de validation de produits ou de solutions de cybersécurité.

Plateformes d'audit ou de pentest : Dans un contexte opérationnel, il peut être nécessaire de contrôler et valider la sécurité des infrastructures qui sont déjà en place. Les tests peuvent alors être réalisés en mode in-situ (sur des plateformes réelles en fonctionnement) ou ex-situ (sur des plateformes indépendantes reproduisant des environnements réels).

13 https://www.pole-excellence-cyber.org/wp-content/uploads/2018/02/Typologie-de-plateformes-V1.4.pdf

NORMALISATIONS EUROPÉENNES _

H.1 RGPD

Le Règlement Général de l'UE sur la Protection des Données (RGPD[14] et GDPR[15] en anglais) dont les sanctions sont entrées en vigueur le 25 mai 2018 renforce et harmonise la protection des données à caractère personnel[16] pour l'ensemble des citoyens de l'UE. Il remplace la directive sur la protection des données personnelles de 1995. Contrairement à une directive qui fait l'objet d'une transposition inévitablement différente dans chaque droit national, une règlementation s'impose ex abrupto dans tous les Etats Membres de façon homogène à quelques exceptions près. Le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou en tant que sous-traitant, dès lors qu'elle est établie sur le territoire de l'Union européenne ou que son activité cible directement des résidents européens.

Ce règlement impose des exigences entièrement nouvelles quant à la façon dont les organisations doivent traiter ces données, ce qui implique, pour les entreprises, d'accroitre leurs efforts dans la gestion de la sécurité des informations et les investissements associés. Il est important de noter que le règlement (qui est déjà en application, seule l'application des sanctions est différée à mars 2018) s'impose à toutes les entreprises, européennes ou extra-européennes, ayant une activité qui accède à des données personnelles de citoyens de l'UE (art.3).

Le changement le plus important dans le cadre du RGPD est probablement l'accent mis sur la responsabilisation, une combinaison de contrôles opérationnels sur les systèmes et les données et la transparence de ces contrôles, y compris la « protection des données par conception » (en tenant compte de la protection de la vie privée lors de la conception des systèmes et des produits), la sécurité appropriée des données, l'exécution d'analyses d'impact sur la vie privée et la tenue de dossiers sur les activités de traitement.

Pour atteindre ces objectifs, le RGPD pose les principes suivants relatifs à la collecte, la conservation et la manipulation des données à caractère personnel (art. 5) :

- Principe de licéité, loyauté et transparence : tous les traitements d'une donnée à caractère personnel doivent correspondre à ce qui a été décrit à la personne concernée ;
- Principe de limitation des finalités : la collecte des données à caractère personnel doit être effectuée pour des motivations « déterminées, explicites et légitimes » ;
- Principe de minimisation des données : au regard des traitements réalisés, les données traitées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire » ;
- Principe d'exactitude : les données à caractère personnel doivent être « exactes et, si nécessaire, tenues à jour » ;
- Principe de limitation de la conservation : les données à caractère personnel doivent être « conservées [...] pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées » ;
- Principe d'intégrité et de confidentialité : les données à caractère personnel doivent être « traitées de façon à garantir une sécurité appropriée ».

14 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees
15 https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/
16 Une « donnée à caractère personnel » est une information se rapportant à une personne physique identifiée ou identifiable.

Maîtrise des risques

Les atteintes à la protection des données à caractère personnel ont donné lieu, par le passé, à des situations désastreuses à la fois pour les entreprises et pour les personnes touchées, avec pour conséquences des pénalités parfois élevées.

Avec l'activation prochaine des sanctions prévues par le RGPD, la conformité est devenue cruciale puisque des pénalités allant jusqu'à 4 % du chiffre d'affaires mondial pourront être prononcées à l'encontre des entreprises défaillantes (art. 83, 84 du RGPD et article 65 de la loi n°2016-1321 du 7 octobre 2016).

À mesure que la complexité des systèmes d'information des entreprises augmente, les risques liés à la gestion des accès augmentent. De plus, l'ubiquité d'Internet a imposé d'une part le partage généralisé d'informations entre les sociétés et leurs partenaires et prestataires et, d'autre part, la pervasivité des accès aux ressources de l'entreprise.

De ce fait, si les fuites d'informations les plus retentissantes (Sony, Yahoo!, ...) sont souvent l'œuvre d'acteurs extérieurs à l'entreprise, la majorité (en nombre et probablement en valeur) des brèches de sécurité proviennent de l'intérieur de l'organisation, où les conséquences d'un comportement négligent ou malfaisant peuvent être démultipliées si une gestion rigoureuse des permissions et des accès n'est pas opérationnelle. La protection des données se trouve au cœur du RGPD (art.5).

Volatilité des permissions

Au sein du SI d'une entreprise, les données sont continuellement importées, stockées, transférées vers et depuis des référentiels structurés (base de données, annuaires...) ou non-structurés (messageries, fichiers...), voire hors du périmètre physique de la société dans le Cloud.

Cette hétérogénéité ne permet pas, en général, aux responsables du SI (DSI), de la sécurité (RSSI) et au Délégué à la Protection des Données (Guidelines on Data Protection Officers, G29 2017) d'avoir la vision d'ensemble nécessaire pour vérifier et valider que les employés aient les droits d'accès et les autorisations strictement nécessaires à l'accomplissement de leurs missions. La validation de la conformité de l'entreprise aux exigences du RGPD est alors une mission impossible.

De plus, ces mêmes employés peuvent être amenés à changer de rôle au sein de l'organisation, en cas de mutation ou de promotion interne par exemple. Cela signifie qu'ils acquièrent de nouveaux droits et accèdent à de nouveaux ensembles de données, sans obligatoirement perdre les accès précédemment acquis (en tout cas immédiatement).

Cette distorsion du modèle de droits initial peut constituer une menace en ce qui concerne la légalité du traitement des données à caractère personnel puisque la base juridique du traitement des données peut ne plus s'appliquer au nouveau rôle du salarié (art.4). Ce serait alors une violation du RGPD puisque le principe de responsabilité sous-jacent au RGPD impose à tout responsable d'être capable de démontrer qu'il se conforme aux obligations du règlement (art.24).

Limitations des référentiels d'entreprise

La forme la plus simple du contrôle des accès au SI peut être réalisée grâce aux fonctionnalités des annuaires d'entreprise : par exemple, la solution Microsoft Active Directory permet de structurer les ressources de l'entreprise dans des groupes disposant de droits d'accès spécifiques.

Cependant, ces méthodes sont trop complexes et trop statiques pour prendre en compte la mobilité et l'hétérogénéité des cas d'usage actuels. De plus, la vue d'ensemble des droits et permissions des personnes est tout simplement impossible à consolider compte tenu de l'imbrication des différentes structures ; la différence entre les droits apparents et les droits réels d'un employé peut engendrer des risques graves de violations de règle du RGPD si toutes les relations ne sont pas correctement interprétées.

En effet, la prise en compte des principes de protection des données à caractère personnel dès la conception et par défaut[17] sont partie intégrante de l'évaluation de la conformité (art.25).

Par ailleurs, les autorisations attribuées à un employé à travers les fonctionnalités de l'annuaire central ne reflètent pas forcément les droits de cette personne dans une application donnée si la correspondance est réalisée « manuellement ». L'automatisation du processus est la seule façon de garantir que les droits attribués sont correctement et immédiatement appliqués (à un delta temporel près lié à la fréquence de synchronisation des référentiels, le cas échéant).

Enfin, il existe de nombreux cas d'usage dans lesquels il est essentiel de garantir, à tout moment, que des ensembles de droits toxiques, c'est-à-dire incompatibles entre eux, ne sont pas simultanément attribués à une personne ou un groupe de personnes[18]. Si tel était le cas, ce serait à nouveau un cas de violation des règles du RGPD.

En résumé

Le RGPD définit les objectifs qui doivent être atteints en termes de protections des données à caractère personnel, sans imposer de méthodes ou de technique spécifique. Cette protection que le RGPD définit et encadre exige que les organisations contrôlent et restreignent l'accès aux données personnelles.

Aussi, étant donné la complexité inhérente aux volumes et à l'hétérogénéité de ces données ainsi qu'au nombre de demandes d'accès à traiter, l'authentification des personnes et des objets qui accèdent aux données ainsi que la supervision et la traçabilité des droits d'accès sont fondamentaux pour respecter les exigences du RGPD, ce que la gestion - es fonction - des accès à privilège doit garantir.

17 « privacy by design » et « privacy by default » en anglais.
18 Voir http://www.rfi.fr/asie-pacifique/20151016-vanuatu-president-parlement-arrestation-auto-amnistie-deputes-grace pour un exemple amusant.

H.2 Certifications (Cyber Act)

La certification est un enjeu stratégique pour les entreprises et pour les pays.

Le projet de règlement Cyber Act propose de mettre en cohérence les certifications nationales de et créer un schéma européen harmonisé de certification.

Il répond à l'attente des différents acteurs de la cybersécurité, industriels comme autorités nationales et doit être un outil essentiel pour la mise en place de la réglementation RGPD.

Le cadre de certification européen[19] est détaillé sur le site de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).Le lecteur pourra également affiner sa compréhension des enjeux et objectifs en consultant le site de l'Alliance pour la Confiance Numérique[20] (ACN).

H.3 Règlementations pour la cybersécurité des entreprises

Les différentes catégories de réglementation dont l'ANSSI a la mission d'assurer l'exécution figurent dans la rubrique dédiée du site de l'ANSSI[21].

Ces catégories réunissent les thèmes relatifs à la protection des systèmes d'information, de l'administration électronique ainsi que plus spécifiquement à la cryptographie ou à d'autres réglementations techniques.

19 https://www.ssi.gouv.fr/entreprise/reglementation/cybersecurity-act-2/le-cadre-de-certification-europeen/
20 https://www.confiance-numerique.fr/
21 https://www.ssi.gouv.fr/entreprise/reglementation/

ANNEXES _

I.1 Table des abréviations

ACM – Association for Computing Machinerie
ACN – Alliance pour la Confiance Numérique
ANSSI – Agence nationale de la sécurité des systèmes d'information
APT – Advanced Persistent Threat
BYOD – Bring Your Own Device
CC – Critères communs
CEN – European Committee for Standardization
CENELEC – European Committee for Electrotechnical Standardization
CERT – Computer Emergency Response Team
CESTI – Centre d'évaluation de la sécurité des technologies de l'information
CSIRT – Computer Security Incident Response Team
CSPN – Certification de Sécurité de Premier Niveau
CTI – Cyber Threat Intelligence
DevSecOps – Développement-Sécurité-Opérations
DLP – Data Leak/Loss Prevention
DSI – Directeur des systèmes d'information
ENISA – Agence européenne chargée de la sécurité des réseaux et de l'information
ETI – Entreprise de taille intermédiaire
ETSI – European Telecommunications Standards Institute
GAFAM – Google, Apple, Facebook, Amazon, Microsoft
GT – Groupe de travail
IA – Intelligence artificielle
IoC – Indicators of compromise
IoT – Internet of Things (Internet des Objets)
ITU – International Telecommunication Union
LID – Lutte informatique défensive
MCO – Maintien en condition opérationnelle
MCS – Maintien en condition de sécurité
OIV – Opérateur d'importance vitale
OSI – Modèle Open System Interconnection
OSINT – Open Source INTelligence
PCA/PRA – Plans de continuité d'activité / plans de reprises d'activité
PEC – Pôle d'excellence cyber
PME – Petite et moyenne entreprise
RGPD – Règlement Général sur la Protection des Données
RSSI – Responsable de la sécurité des systèmes d'information
RTE – Rapport technique d'évaluation
SCI – Systèmes de contrôle industriel
SDN – Software Defined Networking
SI – Système d'information
SIEM – Security Information and Event Management
SOC – Security Operation Center
SOCMINT – SOCial Media INTelligence
SSI – Sécurité des systèmes d'information
SVM – Support Vector Machine
TCG – Trusted Computer Group
TIC – Technologie de l'information et de la communication
TPE – Très petite entreprise
TTP – Tactiques, Techniques et Procédures
VPN – Virtual Private Network

I.2 Table des liens et bibliographie

- **Site de l'ANSSI :**
  - https://www.ssi.gouv.fr/entreprise/reglementation/
  - http://www.ssi.gouv.fr/entreprise/formations/profils-metiers/
  - https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/
  - https://www.ssi.gouv.fr/entreprise/reglementation/cybersecurity-act-2/le-cadre-de-certification-europeen/

- **Site de la défense :**
  Informations sur le renseignement et le cyber-engagement militaire :
- https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf
- https://www.defense.gouv.fr/content/download/551530/9394277/Politique%20MINARM%20de%20lutte%20informatique%20DEFENSIVE.pdf

- **Sites gouvernementaux :**
  - https://www.gouvernement.fr/risques/espionnage
  - https://franceconnect.gouv.fr/
  - https://www.cnil.fr/fr/reglement-europeen-protection-donnees
  - https://www.pole-excellence-cyber.org/wp-content/uploads/2018/02/Typologie-de-plateformes-V1.4.pdf
  - https://sisse.entreprises.gouv.fr/fr/outils/la-securite-economique-au-quotidien-26-fiches-thematiques
  - https://inhesj.fr/kit-de-sensibilisation-des-atteintes-la-securite-economique
  - http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

- **Site de l'Alliance pour la Confiance Numérique**
  - https://www.confiance-numerique.fr/

- **Ouvrage sur l'intelligence artificielle :**
  Russel, S., Norvig, P., 2003.
  Artificial Intelligence: a modern approach.
  2nd Edition.
  Prentice Hall, Pearson Education Inc.

PÔLE D'EXCELLENCE CYBER

RÉFÉRENTIEL CYBER V5.0

NOVEMBRE 2019

PÔLE D'EXCELLENCE
CYBER

12 B rue du Patis Tatelin
35700 RENNES
France

www.pole-excellence-cyber.org

Conception et impression : Temps-Présent - tpcommunication.com