REFERENTIEL

V4.6

JANVIER 2018

Contenu

Editorial

Déclinaison opérationnelle du Livre blanc sur la Défense et la Sécurité nationale qui érige la cyberdéfense et la cybersécurité en priorités nationales, le Pacte défense cyber a instauré la mise en place d'un Pôle d'excellence cyber au profit du ministère des Armées et de la communauté nationale autour de ce domaine. Il est aussi une composante du Pacte d'avenir pour la Bretagne. Ce pôle d'excellence doit répondre à trois enjeux principaux.

Le premier concerne la formation, où le pôle doit contribuer à ce qu'une offre de formation adaptée aux besoins des entreprises et institutions soit développée et permette de disposer d'un volume suffisant de personnels qualifiés pour assurer le développement de la filière.

Le second est de voir l'ensemble des partenaires académiques de la recherche travailler de concert à l'écoute des besoins du ministère des Armées et des industriels, dont les OIV.

Le troisième concerne l'accompagnement des industriels afin de combler les manques dans l'offre de service et de produit de confiance.

Ces enjeux mobilisent l'ensemble des partenaires du Pôle d'Excellence Cyber, instituts de recherche, de formation, PME, grands groupes industriels, ministère des Armées et région Bretagne. C'est la synergie entre ces différentes entités qui permet la mise en place de projets concrets par l'émergence d'opportunités croisées.

Ce document de structuration est un résultat concret des premières actions mises en place dans le cadre du GT référentiel du PEC, qui est en charge de sa tenue à jour. Face à un domaine en pleine mutation, il est en effet important de préciser entre les différents partenaires du Pôle d'excellence cyber le périmètre technique sur lequel nous menons nos réflexions et travaux. Élaboré par un panel d'experts privés et étatiques, du monde de la recherche, de la formation ou de l'industrie, ce document a vocation à contribuer à décrire, 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 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 et d'identifier les enjeux et les opportunités de développement associés. Outil de dialogue et de concertation tout-à-fait dans l'esprit du Pôle d'excellence cyber, 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.

Philippe Verdier

Président du Pôle d'excellence cyber

A. Préambule

A.1 Introduction

Le pacte défense cyber présenté par le ministre de la défense le 7 février 2014 à Rennes, a vocation à favoriser le développement de l'activité de recherche, de l'offre de formation ainsi qu'à dynamiser le tissu industriel afin de répondre à l'accroissement des besoins dans ce domaine. Le pôle d'excellence en cyber, qui est aussi intégré dans le pacte d'avenir pour le Bretagne est une concrétisation de cette volonté.

Une étape essentielle pour l'organisation du pôle est de déterminer ce que recouvrent la Cybersécurité et la Cyberdéfense. En effet, derrière ces terminologies en vogue, se cache une réalité technologique, scientifique et économique complexe qu'il est important de cerner afin de déterminer le périmètre d'intervention du pôle d'excellence cyber. L'objectif du présent document est de proposer ce périmètre.

Bien entendu, ce document a vocation à être partagé largement, et il évoluera en fonction de retours de l'ensemble des acteurs.

Pour atteindre ces objectifs, ce document s'inscrit dans la méthodologie suivante en couvrant les trois premiers points :

1. Décliner les besoins en produits/services/méthodes liés à la Cybersécurité : analyse des technologies et services
2. Identifier les besoins domaines fonctionnels liés à la Cybersécurité.
3. Esquisser une identification des cas d'usage
4. Amorcer une identification des Produits & Services Cyber français et étranger
5. Mettre en cohérence 1, 2, 3 et 4 pour alimenter la feuille de route des actions de développement de la filière dans le cadre du pôle d'excellence Cyber

La première partie du document permet d'identifier le périmètre du domaine et d'identifier les enjeux techniques 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 Telecommunication 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 (Cyber Security Coordination Group : CSCG). Lors d'une réunion récente, ce groupe a émis la recommandation suivante :

The EC 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.

On voit donc que la préoccupation de clarifier le périmètre de la cybersécurité est assez généralement partagée par les acteurs concernés et correspond à des actions en cours. Au niveau national, on peut cependant retenir les définitions suivantes :

ANSSI	**Cybersécurité** état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace 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 cybercriminalité 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.
Ministère des Armées	Les grands constitutifs de la cybersécurité : 1. **Volet cyberprotection** Ensemble des mesures techniques, physiques et organisationnelles mise en place pour bâtir des architectures les plus robustes possibles face aux menaces portant sur la disponibilité, la confidentialité et l'intégrité des informations ou des services. 2. **Volet cyberdéfense** Ensemble des mesures techniques ou organisationnelles permettant la surveillance, l'appréciation de la sécurité et la réaction face à des attaques. 3. **Volet cyberrésilience** Capacité des systèmes à continuer à fonctionner éventuellement en mode dégradé lorsqu'ils sont soumis à des agressions.

Le terme cybersécurité est englobant et sera utilisé dans le reste du document.

B. Technologies et services

On peut trouver de multiples catégorisations pour structurer ce domaine. Celui qui est proposé ci-dessous s'articule autour d'une déclinaison en trois thématiques : produits & technologies, services, méthodes & outils métiers.

Les trois 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, sans rechercher l'exhaustivité, explicite l'importance stratégique de certaines de ces thématiques.

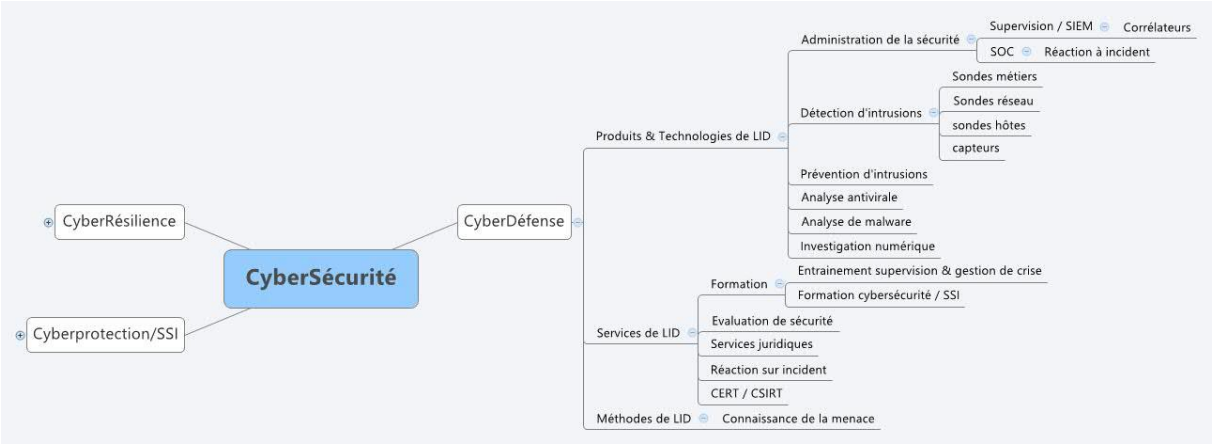

Figure 1 : Besoins en produits/services/méthodes de Cyberdéfense

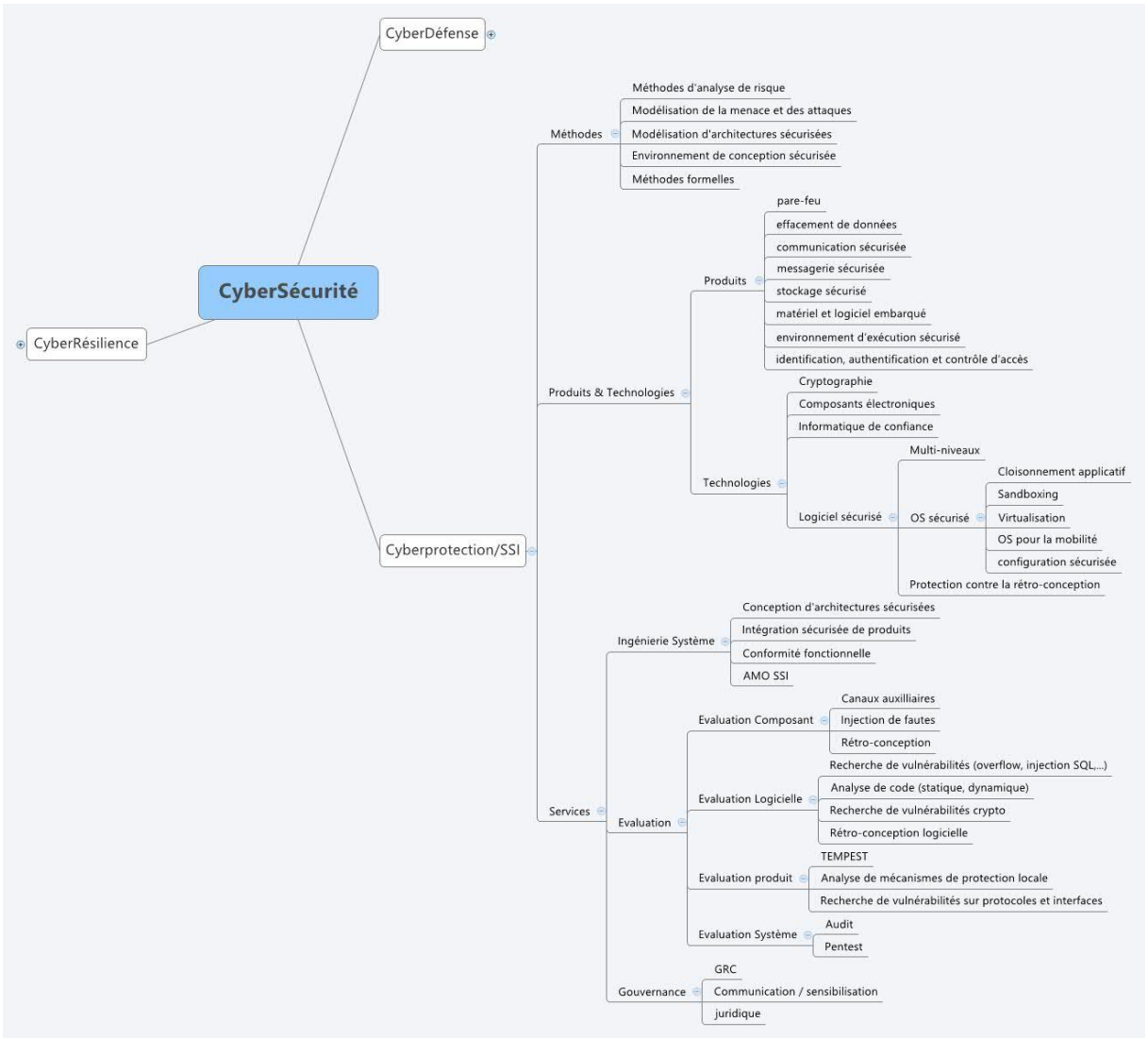

Figure 2 : Besoins en produits/services/méthodes de Cyberprotection

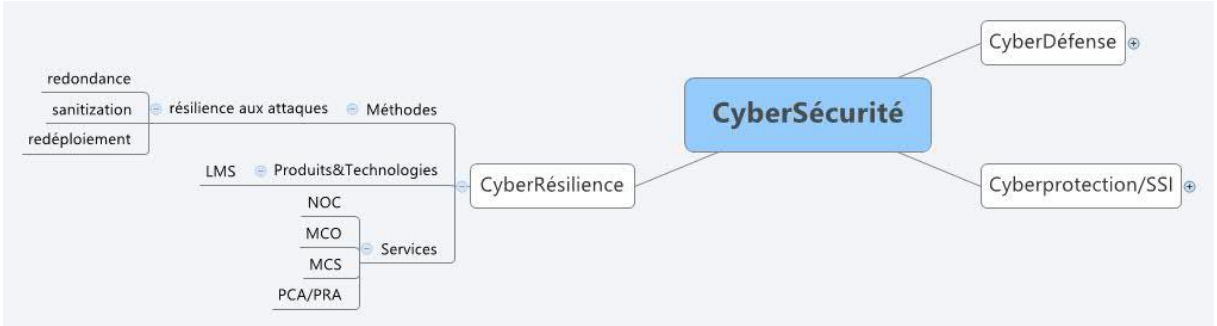

Figure 3 : Besoins en produits/services/méthodes en CyberRésilience

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

Les sections suivantes exposent un certain nombre de thématiques critiques en termes de positionnement de la filière.

B.1 Cyberdéfense

B.1.1 Services

B.1.1.1 Formation

B.1.1.1.1 Formation cybersécurité / SSI

L'ANSSI propose sur son site (http://www.ssi.gouv.fr/entreprise/formations/profils-metiers/) une liste de 16 profils. Cette liste sert de base pour les travaux du PEC, et deux profils ont été ajoutés. Elle est détaillée au chapitre E. Des formations initiales ou continues doivent être proposées pour pouvoir disposer de ressources humaines à la fois en quantité et en qualité pour remplir les postes nécessaires que ce soit dans la sphère privée ou étatique. Ce besoin en formation initiale ou continue 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 (techniciens, ingénieurs), civils ou militaires et dans ce dernier cas pour des systèmes en métropole ou sur théâtre d'opérations extérieures.

B.1.1.1.2 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 inclure aussi la dimension juridique liée à la cyberdéfense (quels sont les droits en cas d'attaque, quelles limites à la réaction, …), des aspects éthiques, et prendre en compte des aspects psychologiques comme la gestion du stress. Les aspects contractuels, afin de mieux spécifier les contrats de service ou de développement de produits doivent aussi être abordés.

B.1.1.2 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.2.3.1).

B.1.1.3 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.1.1.4 Réaction aux incidents

Dans le cas où une attaque a été couronnée de succès, 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.1.1.4 CERT[1] / CSIRT

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

B.1.2 Méthodes de Lutte Informatique Défensive (LID).

B.1.2.1 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 (darkweb). L'exploration du deepweb 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 sources ouvertes et 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, …

B.1.3 Produits et technologies de LID

On peut notamment citer les thèmes d'intérêt suivants :

B.1.3.1 Administration de la sécurité

B.1.3.1.1 SIEM (Security Incident end Event Manager)

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.1.3.1.2 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 on peut citer les techniques d'aide à la décision suivantes :

- 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 replis en fonction de conditions pré-établies.

[1] Le terme CERT est une marque deposée de l'université Carnegie Mellon et ne peut être utilisé sans leur accord

- La réaction automatique par système expert.

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

B.1.3.2 Produits de détection d'intrusion

On retrouve ici les sondes qui vont capter l'information qui va alimenter le reste de la chaîne de LID. On peut identifier :

- 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 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 des différents modes de détection notamment la détection comportementale (déviance par rapport à un usage normal).

B.1.3.3 Prévention d'intrusion

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 comme l'indique leur nom de détecter et de bloquer les attaques.

B.1.3.4 Analyse anti-virale

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.

B.1.3.5 Analyse de malware

Pour comprendre le fonctionnement des malwares et pouvoir les éradiquer il est nécessaire de disposer d'outils spécifiques. En effet, pour des raisons évidentes on ne peut analyser ces logiciels que dans un environnement très maîtrisé pour éviter leur propagation. Par ailleurs, les malwares

étant de plus en plus sophistiqués il faut leur présenter un environnement réaliste sinon 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.

B.1.3.6 Investigation numérique

Les outils d'investigation numérique vont être utilisés pour rechercher les traces laissées par une agression informatique et reconstruire la chronologie des événements. Elle peut être utilisée aussi 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 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 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.

B.2 Cyberprotection

B.2.1 Méthodes

B.2.1.1 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 on souhaite se protéger. Ensuite un processus d'analyse de risques doit être intégré à toutes les décisions d'évolution d'un système.

L'ISO/IEC 27005 « Gestion des risques en sécurité de l'information » décrit les grands principes de cette analyse de risque. On peut citer la méthode EBIOS proposée par l'ANSSI qui fixe des grandes étapes permettant de réaliser ces analyses de risques. L'outillage existant peut par contre être amélioré pour mieux prendre en compte l'analyse par arbre d'attaques, la recherche automatique de scénarios, le lien avec la modélisation système …

B.2.1.2 Modélisation de la menace et des attaques

La modélisation de la menace peut être vue comme une brique des méthodes d'analyse de risques. On peut aussi songer à la réalisation de bibliothèques de menaces et d'attaques qui pourraient être utilisées au sein de plate-forme 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.2.1.3 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 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, … toutes choses indisponibles dans les outils standards.

B.2.1.4 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. 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.

B.2.1.5 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 utilisées par exemple 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 apportant un maximum d'automatisation.

B.2.2 Produits et technologies de sécurité

B.2.2.1 Produits

Le thème des produits de sécurité est très vaste. On y trouve bien entendu les produits de chiffrement (réseau, téléphonie, messagerie, poste de travail, …), les produits de contrôle d'accès et d'authentification, les produits de filtrage (firewall, 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.2.2.2 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 des objets communiquant qui n'en est qu'à ses balbutiements renforcera ce besoin de bases matérielles et logicielles de confiance.

L'importance des 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.2.2.2 Technologies

B.2.2.2.1 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 verrous restent à lever nombreux sujets restent à développer comme par exemple :

- La cryptographie à très haut débit.
- La cryptographie à bas coût 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,
- Les technologies de type blockchain,
- …

B.2.2.2.2 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.2.2.2.3 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 assurer 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, …) 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.2.2.2.4 Logiciel sécurisé

B.2.2.2.4.1 Multi-niveaux

Le multi niveau est un besoin prégnant dans le domaine de la défense ou coexistent des niveaux de classification ou de sensibilité très divers. Il existe aussi au sein des entreprises où on peut trouver des informations ouvertes, des informations confidentielles liées aux personnels, des informations financières, stratégiques, relevant du secret industriel, … On peut vouloir aussi 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 multiniveaux peut s'exprimer suivant plusieurs modalités :

- Interconnecter des réseaux et systèmes de niveaux différents en permettant des échanges selon une politique de sécurité définie (exemple : connecter un réseau contenant des informations sensibles et des informations ouvertes à 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 leurs droits d'accès.
- 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 théorisés 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 et par l'incapacité d'arriver à concilier un niveau de sécurité satisfaisant avec un niveau fonctionnel acceptable par les utilisateurs. Il existe donc dans ce domaine un vaste champ de recherche et de réalisation 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.2.2.2.4.2 OS sécurisé

Tous les systèmes informatiques utilisent 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 que l'on doit pouvoir maîtriser. Toutes les techniques de cloisonnement, de sand boxing, d'hyperviseurs, etc sont donc d'un intérêt certain.

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 un minimum de 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 la réalisation d'outils de vérification ou de configuration automatique.

B.2.2.2.4.3 Protection contre la rétro-conception

La protection contre la rétro-conception est une étape indispensable pour la protection de droits (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 permettre leur utilisation par les industriels mettant des produits à protéger sur le marché. Ils doivent pouvoir s'adapter aux différents langages de programmation, s'insérer dans les processus de développement et aux différents environnements d'exécution. 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 les mettant en œuvre.

B.2.3 Services

B.2.3.1 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. A 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, on citera notamment :

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

B.2.3.1.1 Evaluation composant

L'évaluation de composants a pour objectif de déterminer le niveau de sécurité apporté par un composant matériel. On va trouver 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 l'analyse de canaux auxiliaires. La recherche dans le domaine peut déboucher sur des produits destinés aux CESTI mais aussi aux concepteurs de composants pour leur permettre d'améliorer le niveau de sécurité de leurs produits.

B.2.3.1.2 Evaluation logicielle

La recherche de vulnérabilités dans le logiciel est une activité complexe et extrêmement couteuse. Même si 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 dans tous les cas ne permettent pas à moyen terme de pouvoir garantir l'absence de vulnérabilités. Les méthodes et outils d'évaluation logicielle sont donc indispensables pour les entreprises spécialisées dans

l'évaluation sécurité (CESTI) mais aussi pour tous les développeurs afin de vérifier au plus tôt dans les cycles de conception le niveau de qualité et de sécurité des logiciels 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 mais 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 fuzzing, injection de code, …
- Les outils de rétro conception logicielle.

Ces différents outils peuvent être utilisés quelque 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.2.3.1.3 Evaluation produit

Même si la plupart des produits embarque une forte proportion de logiciel, certaines fonctions de sécurité peuvent être rendues par le matériel. On peut citer par exemple les mécanismes de protection locale anti-intrusion sur les boitiers. Par ailleurs, en complément d'une évaluation logicielle, ou bien 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 fuzzing appliquées aux interface et protocoles, les outils de tests d'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 l'existence de moyens d'analyse numériques performants et accessibles ouvre un large champ de vulnérabilités qu'il est utile d'adresser. Les travaux d'évaluation de protocoles radio, d'évaluation TEMPEST ou plus généralement les travaux classifiés nécessitent l'utilisation de cages de Faraday.

B.2.3.1.4 Evaluation système

B.2.3.1.4.1 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 ces audits. La certification d'entreprises peut être recherchée pour faciliter le choix de prestataires compétents par les clients.

On peut ranger dans cette catégorie les prestations de type « pentest », qui sont plus ciblées et purement techniques.

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

B.2.3.2 Ingénierie système

B.2.3.2.1 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.2.3.2.2 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.2.3.2.3 Intégration sécurisées 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.2.3.2.4 Conformité fonctionnelle

La conformité fonctionnelle vise à s'assurer qu'un produit répond 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.2.3.1 sont indispensable pour fournir un service pertinent.

B.2.3.3 Gouvernance

B.2.3.3.1 GRC (Gouvernance Risk Compliance)

Il existe un besoin de services autour de la GRC (Gouvernance 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.2.3.3.2 Communication et sensibilisation des utilisateurs

Les services liés à la communication et à la sensibilisation des utilisateurs qui sont essentiels sachant que la vulnérabilité se situe « entre la chaise et l'ordinateur ». Ce sont les hommes et les femmes qui sont à la fois la plus grande vulnérabilité et la solution au problème de cybersécurité.

B.2.3.3.3 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 en cas de défaillance ou de non-respect des contrats.

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

B.3 Cyber-résilience

B.3.1 Méthodes

Une partie des fonctions de cyber résilience est apportée par les architectures de systèmes. Les méthodes identifiées au B.2.3.2 seront donc utilisées pour bâtir des architectures incluant des redondances au niveau réseau ou au niveau des 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 bien entendu avoir effectué les copies nécessaires aux actions de forensic), puis réinstaller à partir d'archives saines l'ensemble du système. Les outils de d'administration offrent les fonctions de base pour ce type d'action mais il est nécessaire de définir des méthodes appropriées pour tenir compte du contexte d'agression.

B.3.2 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 plus ou moins 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.3.3 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. On peut ensuite identifier les services de maintien en condition opérationnelle (MCO) et de maintien en condition de sécurité (MCS). En effet nombre d'attaques informatiques peuvent se diffuser à cause de la mauvaise configuration des systèmes : versions obsolètes, bases anti-virales non mises à jour, … Le MCS de systèmes enfouis ou de systèmes industriels ou 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 pannes uniques.

C. 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).

A titre d'exemple, dans le domaine des TICs, 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 de la 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 de la Cyber. Cette liste pourra évoluer en fonction de l'évolution de ces marchés de la Cyber.

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.

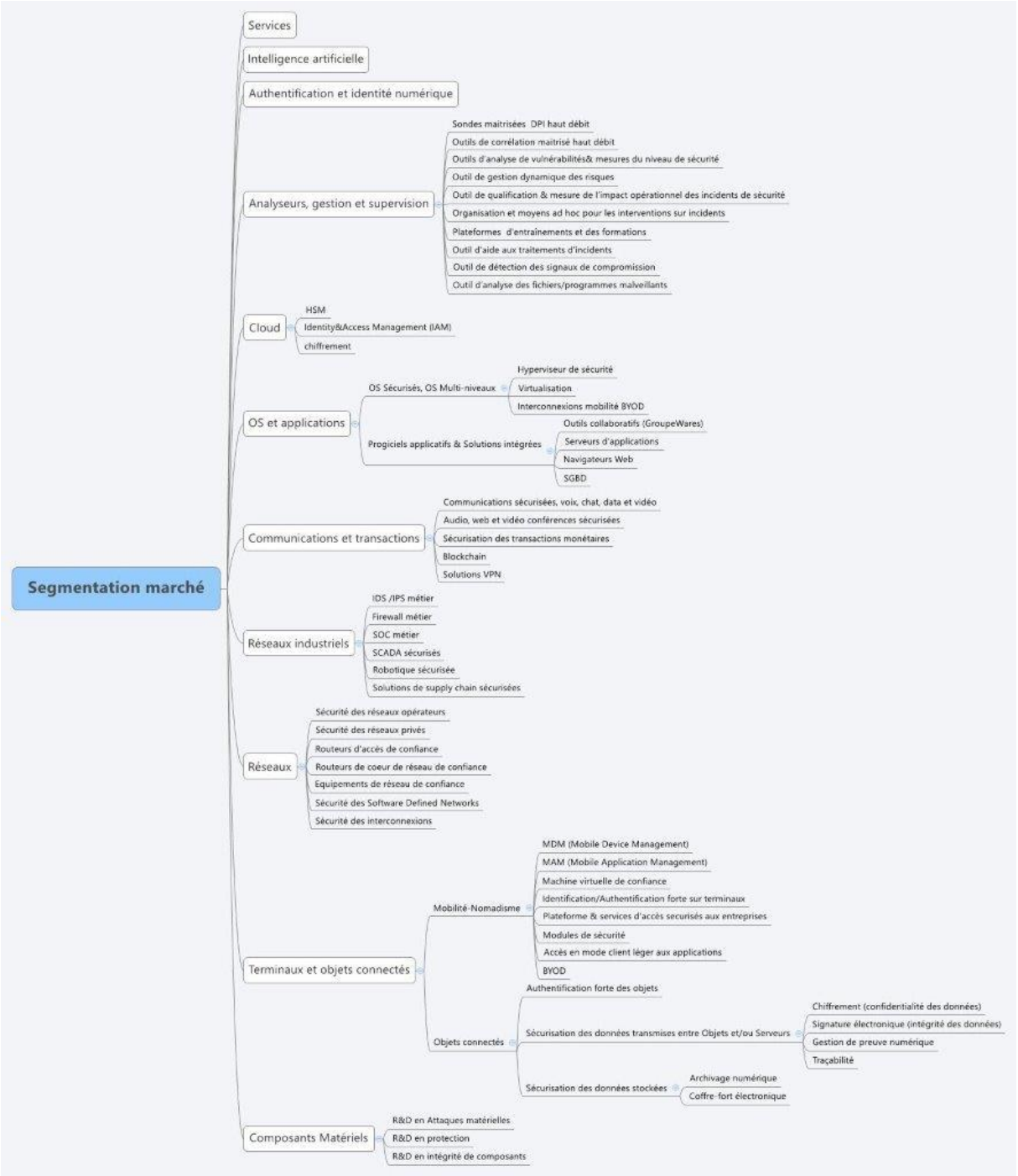

Figure 4 : Segmentation marché

C.1 Services

Les différents services du domaine cyber sont décrits au chapitre B (B.1.1 pour les services liés à la cyberdéfense, B.2.3 pour la cyber-protection et B.3.3 pour la cyber-résilience).

C.2 Intelligence Artificielle

Les applications de l'IA (Intelligence Artificielle) dépassent bien entendu largement le cadre de la cybersécurité. Il s'agit néanmoins d'un domaine où les applications potentielles sont nombreuses,

que ce soit pour les activités de protection (recherche automatique de vulnérabilités, …) que dans celui de la défense (détection d'attaques, propositions de plans d'action, …). Les publications ou les démonstrations sur le sujet sont en forte croissance. Il ne fait aucun doute que ce domaine va prendre une importance majeure dans les années à venir.

C.3 Authentification et identité numérique

Chacun utilise une ou plusieurs identités numériques pour accéder aux différents services offerts sur Internet. La gestion de ces identités pose des problèmes techniques autour par exemple 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 très complexes.

C.4 Analyseurs, gestion et supervision

On va retrouver dans ce domaine l'ensemble des produits, technologies et services décrits au § B.1 ci-dessus. Leurs besoins et leurs enjeux découlent donc directement de ceux-ci.

C.5 Cloud

Le Cloud 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). A la croisée d'autres domaines, on retrouve aussi la gestion des identités pour garantir un accès sécurisé quel que soit le lieu ou le moyen d'accès aux données.

C.6 OS et applications

C.6.1 OS Sécurisés, OS Multi-niveaux

Comme les composants matériels, les systèmes d'exploitation sont une brique de base de tous les systèmes numériques. Il semble aujourd'hui assez illusoire de penser réaliser un système d'exploitation à partir d'une feuille blanche. Il est donc nécessaire de trouver des solutions pour utiliser de la manière la plus sûre possible les OS existants. Un premier moyen est de les configurer pour améliorer leur niveau de sécurité. Les systèmes de virtualisation et de cloisonnement permettent d'aller plus loin en limitant les impacts d'une défaillance ou de l'exploitation d'une vulnérabilité (« sandboxing »). Plusieurs techniques sont utilisables et il est notamment possible de se reposer sur un noyau, beaucoup plus petit qu'un OS et qui peut être maîtrisable. Ces techniques sont notamment mises en œuvre pour bâtir des architectures multi-niveaux, chaque niveau de sécurité fonctionnant dans une « cage » étanche, sauf pour des échanges maîtrisés passant par le noyau.

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 audios, vidéo, de chat ou de data. De même le développement de visio ou de la vidéo conférence souvent pour du travail collaboratif à haute valeur ajoutée nécessite la mise en place de solutions adaptées. On peut noter aussi dans cette catégorie les solutions VPN (Virtual Private Network) utilisées notamment pour l'accès à distance à des réseaux d'entreprises par des postes nomades.

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 qui viennent. Elles viennent compléter les solutions plus historiques mais qui restent indispensable 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, se retrouvent dans une infinité de domaines que ce soit pour le pilotage de process industriels que dans la gestion technique de bâtiments, et bien sûr dans de nombreux systèmes d'armes. Leur positionnement à l'interface entre un domaine informatique (applications métiers) et un système physique via des ensembles de capteurs et actionneurs, en font des systèmes particulièrement sensibles en termes de sécurité. Comme l'on 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 (black out 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, …). 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)
- Protocoles parfois spécifiques
- …

Ce domaine inclut également la sécurisation des solutions de robotique et des solutions de « supply chain ».

Les solutions sur étagères du domaine informatiques ne sont donc pas entièrement capables de répondre à tous les besoins. Il s'agit par ailleurs d'un domaine très vaste et encore peu exploré même si la profusion d'articles scientifiques sur le sujet et les annonces des grands fournisseurs de solutions montrent que la situation évolue rapidement.

C.9 Réseaux

Ce chapitre concerne l'ensemble des équipements et solutions qui constituent les réseaux de transmissions et de communications, du niveau 1 au niveau 3. On y regroupe les équipements de transmission électriques ou optiques, les commutateurs 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 un domaine bien connu, se pose la question de la maîtrise des équipements, des protocoles et des services constituant les cœurs de réseaux des opérateurs. Il est en effet clair qu'aujourd'hui le fonctionnement global de notre société repose sur la disponibilité de services de communication. Les conséquences d'un arrêt général des services de communication aurait un impact considérable tant sur le fonctionnement de l'Etat que celui des entreprises. L'évolution vers des technologies dites SDN (Software Defined Networking) va engendrer des problèmes de sécurité et de confiance d'un genre nouveau du fait de la virtualisation et donc potentiellement de la « délocalisation » de fonctions intelligentes des réseaux (sans parler des impacts sur des fonctions régaliennes de type interceptions légales).

Dans un autre registre, l'interconnexion de réseaux de sensibilités différentes est un sujet très largement partagé. On pense bien sûr à la connexion entre un Intranet et Internet avec tous les problèmes imaginables : fuite de données sensibles de l'entreprise, pollution par des malwares, déni de service, … Mais il peut aussi exister d'autres applications concernant la connexion entre un réseau industriel et un réseau bureautique, le cloisonnement entre Extranet / Intranet, … Le sujet est bien entendu au cœur des préoccupations de la défense avec de nombreux niveaux de sécurité et des enjeux très importants.

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 ou 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 une perte du terminal ou des données qu'il contient, ou bien sûr l'intrusion 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 concernés que ce soit dans les domaines industriels, dans celui du commerce et de la distribution,

dans le domaine médical ou dans une utilisation personnelle. Jusqu'à aujourd'hui, la sécurité a rarement été prise en compte, tant au niveau des connexions qui sont en général réalisées via des connexions sans fils, qu'au niveau des applicatifs 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 domicile, …). On peut aussi craindre leur prise de contrôle à distance qui pourrait provoquer des accidents graves (dispositifs médicaux implantés). 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 veut adresser 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. Mais selon un autre point de vue, ils peuvent aussi renforcer considérablement la sécurité d'un objet en rendant inopérantes les modifications du logiciel en vue de mener une attaque.

Pour prendre un exemple, il est beaucoup plus facile de protéger un logiciel contre la copie si on peut s'appuyer sur un élément matériel plutôt que de se baser uniquement sur une solution logicielle.

D. 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 types de solutions ou de produits à mettre en place.

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'expérience 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 (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 à des capacités techniques financières des différents types de clients
- …

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 cette réalité.

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. A titre d'exemple, une première liste de cas d'activités qui nous semblent mériter une analyse est la suivante :

- Transports :
  - Automobile et infrastructure routière connectée.
  - Aéronautique
  - Navires et navigation maritimes
  - Infrastructures ferroviaires

- Production et distribution d'énergie (y compris smart grids)
- Gestion de l'eau (distribution et retraitement)
- Santé
- Systèmes de communication
- Domotique / gestion technique de bâtiments.
- Banques / assurances.
- Usine du futur
    - Industries agro-alimentaires
    - Cobotique et robotique industrielle
    - industries culturelles et créatives
- Drones et robots
- Protection de la vie privée
- Smart cities

D.1.1 Transports

Le domaine des transports se caractérise mais 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 on peut identifier un risque commun pour tous les acteurs qui est le risque de pertes humaines et de dysfonctionnement majeur de la société en cas d'accident qui serait provoqué par une attaque cyber.

D.1.1.1 Automobile connectée.

L'automobile devient de plus un objet connecté, que ce soit dans le cadre d'une utilisation personnelle ou professionnelle (gestion de flotte, suivi de trajets, ...). De nombreux articles ont montré la vulnérabilité potentielle des architectures actuelles [2]et des travaux sont 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, …) avec des bus utilisés pour des fonctions de confort ou de divertissement. L'arrivée de ports de type USB permettant la connexion de supports amovibles et la généralisation de l'intégration de fonctions de téléphonie mobile offrent à la fois des portes d'entrées pour l'introduction de logiciels malveillants, et un lien pour les activer ou les piloter à distance. On peut ainsi imaginer des attaques ciblées ou aléatoires pouvant causer des dommages matériels et 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. On peut penser que le niveau de sécurité exigé va se rapprocher 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 au niveau des aéronefs avec des règles de certification très poussées. La prise en compte de menaces

[2] : par exemple : Experimental Security Analysis of a Modern Automobile, 2010 IEEE Symposium on Security and Privacy, Karl Koscher et al

cyber s'effectue progressivement, à mesure que l'évolution des techniques et des usages augmente les risques potentiels. On peut par exemple citer les réseaux de divertissement à bord permettant 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 attaques.

En termes d'infrastructures aéroportuaires, on trouve bien évidemment de nombreux systèmes informatiques pour assurer la logistique des aéroports et le contrôle aérien. Pour le premier point, le risque principal qu'on peut 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. On peut noter à cet effet les travaux de Thales Raytheon systems qui a lancé depuis 2013 un dispositif nommé Cybair Radbox qui protège les radars de surveillance aérienne contre les risques de cyber attaques (par exemple ajout ou suppression de pistes radars).

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 font au mieux du blocage 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, on se trouve dans une situation 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 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 au systèmes portuaires peuvent réaliser des vols de grande envergure.

D.1.1.4 Infrastructures ferroviaires

Les infrastructures ferroviaires sont sensibles aux risques en disponibilité pouvant conduire à de graves perturbations de trafic. Leur intégrité est aussi à protéger 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. Au niveau production, l'intégrité des systèmes d'information et la disponibilité des systèmes industriels doit donc être garantie et protégée contre les risques de cyber attaques. L'absence de connexion directe entre les réseaux critiques et les réseaux ouverts ne doit pas être considérée comme une barrière absolue comme a pu le montrer la diffusion de l'attaque Stuxnet.

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

Les smarts grids viennent ajouter d'autres dimensions en multipliant les points d'accès au système d'information et 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 commerciale (masquage de consommation, …) peuvent aussi apparaitre avec des impacts financiers mais aussi d'image.

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

L'eau potable est une ressource importante pour de nombreux secteurs et bien entendu 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 ou des impacts pour certains secteurs d'activités. Au niveau des systèmes de retraitement, une prise de contrôle de stations d'épuration pourrait impliquer des pollutions de milieux naturels. On peut cependant noter que la gestion de l'eau est essentiellement locale et que les impacts seront dans tous les cas limités à une zone géographique limitée, 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 avec les dispositifs médicaux assistés. On retrouve là des problématiques habituelles de risques et disponibilité ou en intégrité pouvant conduire notamment à des fraudes avec des impacts financiers ou pénaux directs, ou d'acceptabilité (perte de confiance).

La multiplication des dispositifs implantés ou d'auto diagnostic fait apparaitre d'autres risques pouvant avoir des impacts plus directs sur la santé voire 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 que du secret des affaires ou de propriété intellectuelle.

D.1.6 Domotique / gestion technique de bâtiments.

Après un démarrage poussif, la domotique est pleine croissance grâce à la généralisation d'internet qui permet des accès à distance simples et avec des débits maintenant compatible de la vidéo et d'autres services, à la miniaturisation et à la baisse de coût des capteurs et aux protocoles sans fils de type wifi qui facilitent leurs connexions. Si on se place du point de vue des particuliers ou des entreprises qui peuvent aussi les utiliser, il est important que ces systèmes qui assurent notamment la protection contre le vol ne puissent pas être neutralisés ou détournés de leur usage (capture de flux vidéo de caméras de surveillance par exemple).

D.1.7 Banques / assurances.

Dans le domaine des banques et assurances on retrouve bien entendu les préoccupations sur la disponibilité des services mais surtout des craintes sur l'intégrité des échanges ou des données qui pourraient avoir de graves conséquences. On peut citer 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 (krach boursiers, manipulation de cours, …).

Des incidents, même de moindre importance mais largement médiatisés peuvent aussi avoir des conséquences fortes sur les entreprises concernées en termes de perte d'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 de ces différents 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, … Les conséquences en termes d'image ou de santé publique peuvent être très lourdes pour les entreprises 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 (comme par exemple arrêt d'activité suite à une cyber attaque) soit insidieux comme une modification malveillante du process industriel conduisant à un sabotage.

D.1.8.3 Industries culturelles et créatives

Pour des industries culturelles et créatives la récente attaque contre TV5 monde montre qu'en vulnérabilité sur le réseau interne informatique de l'entreprise peut conduire à un impact 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 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 récents médiatisés de survol de sites sensibles par des drones montrent les risques potentiels de ces objets. Les risques peuvent être liés à une prise de contrôle à distance d'un drone en vol et l'utilisation de drone comme projectile, mais aussi l'utilisation d'un drone 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 rester dans un cercle maîtrisé. Il est nécessaire de trouver un équilibre entre cette protection de la vie privée et la nécessaire imputabilité des actions pour éviter que ces outils ne soient utilisés à des fins délictueuses ou criminelles.

D1.11 Smart cities

Le concept de smart city est assez large et certains termes abordés plus haut pourraient en faire partie. La caractéristique de la smart city est la surface d'attaque due à l'élongation géographique de la ville et la multiplicité des capteurs et actionneurs qui permettent de rendre les services. Les dysfonctionnements possibles en cas de cyber attaque sont potentiellement conséquents et peuvent surtout être utilisés pour renforcer l'effet d'attaques physiques concomitantes (par exemple : désorganisation du trafic provoquant un engorgement de la circulation avant un attentat pour bloquer l'arrivée des secours).

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

On pourra considérer trois grands groupes :

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

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

Les produits ou les services pour le groupe 1 doivent être simples d'utilisation, quasi autonomes ou administrés par tiers car les entités concernées n'ont pas les capacités techniques, humaines ou financières pour mettre en œuvre des systèmes complexes. A contrario, les OIV ou les grandes administrations pourront vouloir être autonomes et 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 et un OIV ou une entité gouvernementale. Les PME ou ETI, selon leur activité, pourront se rattacher à l'un ou l'autre groupe. On voit rapidement qu'il doit exister des gammes de produits et services adaptés ou 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

L'ANSSI, avec un groupe de travail composé de représentants de l'enseignement supérieur et du monde industriel, a défini 16 profils pour les métiers de la cybersécurité (http://www.ssi.gouv.fr/entreprise/formations/profils-metiers/). Ces profils ont été intégralement repris au sein du PEC. Ils sont listés ci-dessous, classés par catégorie et complétés de deux profils :

- Un profil « évaluateur », distinct du profil auditeur/contrôle. Les compétences et méthodes à mettre en œuvre sont en effet sensiblement différentes entre ces deux profils. L'évaluateur va essentiellement travailler en laboratoire, et effectuer des recherches de vulnérabilités en suivant une méthodologie de type critères communs. Les auditeurs / contrôleurs vont essentiellement travailler sur site et vont largement prendre en compte les aspects humains et organisationnels.
- Un profil « expert R&D cyber », pour matérialiser l'importance de la recherche dans ce domaine en pleine expansion.

Quatre catégories ont été identifiées pour classer ces différents profils :

1. Métiers liés au développement de produits ou systèmes : on y trouve tous les métiers de conception, d'évaluation, d'intégration et d'expertise permettant de réaliser des produits ou des systèmes de cybersécurité ou prenant en compte la cybersécurité.
2. Métiers opérationnels : on y trouve tous les métiers liés à l'exploitation au sens de la cybersécurité de systèmes.
3. Métiers du contrôle : on y trouve tous les métiers qui permettent d'évaluer le niveau de sécurité d'un système par rapport à un référentiel normatif ou à l'état de l'art.
4. Développement de capacités : on y trouve les chercheurs publics ou privés qui vont permettre l'émergence de nouveaux concepts, de nouvelles technologies, produits ou services.

E.1 Métiers liés au développement de produits ou de systèmes

a. **Architecte [système, logiciel, matériel] sécurité :** de niveau BAC +5, l'architecte sécurité structure les choix techniques, technologiques et méthodologiques d'un ensemble [système, logiciel, matériel] répondant à des exigences de sécurité, en cohérence avec les activités équivalentes réalisées au niveau de la solution qui l'intègre. Il s'assure de la déclinaison optimale des exigences techniques d'entrée (fonctionnalités à offrir, contraintes de performance, d'interopérabilité, d'interchangeabilité, de robustesse, d'intégration de solutions sur étagère, d'exportabilité), selon des critères de coût, d'efficacité, de stabilité, de maîtrise, de niveau de risque, de respect des standards, d'aptitude à la production, au déploiement et à la maintenance MCO (maintien en conditions opérationnelles) et MCS (maintien en conditions de sécurité). Il identifie et valide la cartographie du système d'information et notamment s'assure que les hypothèses de sécurité relatives à l'environnement de son architecture sont clairement énoncées et prises en compte dans sa conception. Il veille à ce que les exigences de sécurisation applicables aux différents constituants de son architecture ou aux outils permettant de la produire soient effectivement déclinées. Il fournit la connaissance de l'état de l'art des architectures prenant en compte les développements futurs et il prépare les dossiers de conception et de justification.

b. **Développeur [produit, logiciel, matériel] de sécurité :** de niveau BAC +5, le développeur de sécurité assure le sous-ensemble des activités d'ingénierie nécessaires à la réalisation d'éléments, de produits, de logiciels répondant à des exigences de sécurité, en cohérence avec les objectifs qui leur sont alloués et une définition d'architecture d'ensemble. Le spectre de ces éléments, produits et logiciels comprend : design, interfaces, spécification, conception, codage, production de binaire, assemblage, test, préparation à l'intégration de niveau solution, gestion de sources, gestion de configuration, gestion des faits techniques, archivage, documentation. Il développe de façon méthodique, en appliquant des règles de conception / codage / tests (qu'il définit au besoin ou qu'il contribue à définir) et s'assure que les composants qu'il produit sont testables en termes de conformité fonctionnelle, de robustesse (tests aux limites et hors limites), de sécurité (résistance aux attaques identifiées en entrée de la conception), et de performances. Il s'assure de l'applicabilité des licences des solutions qu'il utilise, et au besoin de l'innocuité de leurs composants.

c. **Evaluateur [produit, logiciel, matériel] de sécurité :** de niveau BAC +2 à BAC +5, l'évaluateur recherche des vulnérabilités dans un [produit, logiciel, matériel] en suivant une méthodologie publique (comme les Critères Communs) ou adaptée

d. **Intégrateur :** de niveau BAC +5, l'intégrateur de sécurité système analyse et prend en charge les volets sécurité en liaison avec l'architecte des projets informatiques et programmes dans l'infrastructure. Il définit et met en œuvre des plates-formes nécessaires à l'intégration des solutions (services ou produits de sécurité) dans les nouvelles applications. Il planifie, coordonne, en relation avec les autres secteurs concernés (réseaux, système de gestion base de données, etc.), les besoins d'intégration exprimés. Il installe des composants matériels, des composants logiciels ou des sous-systèmes supplémentaires dans un système existant ou en cours de développement, respecte les processus et procédures établis (i.e. gestion de configuration) en tenant compte de la spécification, de la capacité et de la compatibilité des modules existants et des nouveaux modules afin de garantir intégrité et interopérabilité. Il contribue à la qualification technique et à l'intégration dans l'environnement de production. Il documente les processus de mise en œuvre, de mise à jour et d'exploitation des composants de sécurité et organise les conditions de mise en œuvre du maintien en condition de sécurité.

e. **Expert :** de niveau BAC +5, l'expert en SSI / cyberdéfense est en capacité de traiter des dossiers complexes (périmètre d'envergure ou spécificité technique poussée). Ses connaissances approfondies des référentiels de sécurité, réglementations, produits et systèmes lui permettent d'instruire des dossiers de sécurité et de les soutenir auprès des acteurs du domaine (administration, instances de régulation, CESTI). Ses capacités pédagogiques et rédactionnelles lui permettent d'élaborer des argumentaires techniques détaillés, voire de proposer de nouveaux développements pour constituer ses dossiers. Sa connaissance des solutions techniques lui permet d'argumenter sur les spécifications de sécurité avec des développeurs et des intégrateurs, en charge de définir et d'implémenter les architectures. Une expertise sécurité ciblée peut couvrir l'ensemble des fonctionnalités d'un produit ou de logiciels complexes d'éditeurs ou encore des domaines spécifiques comme les noyaux ou protocoles autour des métiers de l'embarqué, la téléphonie sur IP, les multiples technologies associées au cloud computing voire aux systèmes nouveaux (systèmes d'armes, systèmes de contrôle industriels…).

f. **Consultant :** de niveau BAC +5, le consultant sécurité anticipe et fait mûrir la prise en compte des enjeux de sécurité dans les organisations. Il alimente les nouveaux

projets par une analyse des dispositifs existants et une sensibilisation aux problématiques de cybersécurité (menaces, vulnérabilités, analyse du marché) liées aux technologies en rapport avec une analyse prospective des processus métiers. Il assiste la direction ou la maîtrise d'ouvrage dans la définition des besoins, de la politique et des solutions de sécurité à mettre en œuvre, en veillant à améliorer l'intégration de la sécurité dans le système d'information d'entreprise. Ses actions consistent en :

i. prescrire recommander des pistes pour le développement et la mise en œuvre de la sécurité d'une organisation, d'un projet ou d'une solution ;

ii. participer à la définition des processus, des spécifications générales des projets ;

iii. vérifier la cohérence de l'architecture applicative et fonctionnelle et de son évolution ;

iv. participer si besoin à l'évaluation et au choix d'une solution de sécurité ;

v. assister les métiers ou la maîtrise d'ouvrage pour le développement de la sécurité du projet ;

vi. effectuer des préconisations de management garantes de la cyber résilience dans le cadre de l'accompagnement d'un projet.

E.2 Métiers opérationnels

g. **Technicien support (technique ou administratif) :** de niveau BAC +2/+3, le technicien support est responsable de diverses activités de support, de gestion ou d'administration de la sécurité aux plans techniques ou administratifs : conception, production, conditionnement et gestion des réseaux de chiffrement et des éléments secrets. Selon le profil d'emploi et la formation reçue, il est en mesure de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements serveurs et des terminaux traitants. Il est en capacité d'effectuer des tâches de contrôles administratifs de conformité dans le domaine des habilitations du personnel, du suivi comptable et des inventaires réglementaires, de l'application des procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle. Il contribue aux séances de sensibilisation pour l'usage des ressources par les utilisateurs finaux. Dans le domaine de la cybersécurité, le technicien veilleur analyse et interprète les alertes, les événements corrélés et recherche les vulnérabilités..

h. **Expert connexe :** de niveau BAC +5, nouveau profil d'expert, né de la nécessité de coordination des techniques de cyberdéfense et de résilience (continuité d'activité métier) face aux attaques, il dispose d'une double compétence et expérience dans les deux domaines. Indifféremment issu de la SSI ou de l'un des secteurs concernés (énergie, télécom, finances, etc.), il a pour rôle essentiel d'analyser, de concevoir, d'intégrer ou de mettre en œuvre, selon son périmètre d'action, les technologies de sécurisation dans le cadre de son domaine métier et des enjeux afférents. Maîtrisant les référentiels respectifs, il est en mesure de :

i. faire converger les objectifs de sécurité et de sûreté de fonctionnement,

ii. conduire des analyses de risques en rapport

iii. proposer les solutions de résilience optimales, afin de minimiser sans concession les impacts métiers, face à l'installation définitive de la menace cyber dans les entreprises et l'Administration.

iv. Conseiller des directions métiers, il contribue à l'expression de besoin globale et technique de sécurité en conception, en intégration et en gestion de la sécurité.

i. **Formateur / Instructeur :** de niveau BAC +3 à BAC +5, il participe à (formateur) ou est responsable de (instructeur) la formation ou la sensibilisation du personnel sur les volets réglementaires, techniques ou opératifs de la SSI et de la cybersécurité. En mesure de mettre en place des travaux pratiques sur les produits et réseaux, il pourra animer des équipes attaque/défense sur des plates-formes d'entraînement représentatives des domaines de l'informatique classique ou des automates industriels, simulant en temps contraint la réponse à des attaques ou incidents de sécurité. Cette tâche est confiée aux formateurs et instructeurs les plus expérimentés. Disposant d'une expérience technique ou opérationnelle dans les domaines enseignés (administrateur, opérateur, réglementation, technique), il se tient informé de l'état de l'art dans son domaine et assure une veille active permettant d'actualiser ses cours en fonction de l'évolution du contexte (technique, menaces, régulation). Titulaire de références pédagogiques, il veille à illustrer ses cours de travaux pratiques, démonstrations ou exercices participatifs.

j. **Gestion de crise :** de niveau BAC +5, le spécialiste en gestion de crise cyber conseille l'organisme pour lui permettre de disposer d'une capacité de gestion de crise majeure dédiée aux systèmes d'information, ou avec un volet cyber prépondérant. Il organise la gestion de crise pour :

   i. agir et résoudre la crise ;

   ii. communiquer l'état de la crise aux personnes et aux organismes concernés ;

   iii. coordonner l'action des différentes parties en présence.

   Il limite les volets organisationnels, l'entraînement et la simulation aux acteurs susceptibles d'intervenir en cas de crise majeure liée aux systèmes d'informations et à leurs interlocuteurs métiers ou support concernés à contacter (gestionnaire de crise, RSSI, responsables de l'ingénierie, administrateurs systèmes / données). À un autre niveau plus technique et sous la pression d'une attaque en cours, le profil de gestionnaire de crise technique peut être également identifié.

k. **Opérateur :** de niveau BAC +3 à BAC +5, l'opérateur met en œuvre la politique de sécurité de l'information, contrôle et prend des mesures contre les intrusions, les fraudes, les agressions ou les fuites concernant la sécurité. Il garantit l'analyse et la gestion des évènements concernant la sécurité des données et des systèmes d'informations de l'organisme, il passe en revue les incidents de sécurité et formule des recommandations pour une amélioration continue de la sécurité.

l. **Analyste :** de niveau BAC +5, l'analyste cyber peut contribuer à plusieurs domaines d'activités de la cyberdéfense, dans les domaines de :

   i. l'anticipation technologique avec de la veille technique ;

   ii. l'anticipation dans le domaine du renseignement sur les menaces, avec de l'analyse d'impact des codes d'exploitation (activités CERT et intégrateur de solutions) ;

   iii. l'anticipation en conduite pour évaluer les dommages subis par un système compromis, participer à la conception de la solution technique visant à restituer le service et apporter ses compétences de spécialiste en matière de mise en œuvre des principes de sécurisation SSI et dans le domaine technique de la cyber sécurité.

Il peut contribuer au schéma directeur et à l'urbanisation sécurisée des systèmes.

m. **Juriste spécialisé :** de niveau BAC +5/+6, le juriste spécialisé en cybersécurité est un expert du droit des technologies de l'information et de la communication spécialiste des thèmes et des corpus concernés par la cybersécurité, la cybercriminalité et la protection des données à caractère personnel. Il peut opportunément présenter une expérience d'avocat à même d'éclairer la direction sur les conséquences pénales ou civiles d'une cyberattaque, dès lors qu'une décision voire la gestion d'une crise avec une composante cyber requiert son expertise. Conseil de la direction en matière de responsabilités civile et pénale, il se tient informé des évolutions de la réglementation internationale, européenne et nationale. Il effectue une veille juridique depuis le simple projet jusqu'à la publication et l'entrée en vigueur des textes régissant les conflits armés, le droit des affaires (notamment le secret des affaires), ainsi que la jurisprudence, en différenciant selon que la décision soit un cas d'espèce ou au contraire amène des réflexions plus générales sur la pratique du droit.

n. **Responsable de la Sécurité des SI (RSSI) :** de niveau BAC +3 à BAC +5, le RSSI se charge de proposer à l'autorité compétente la politique de sécurité du SI et de veiller à son application. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir en matière de SSI sur tout ou partie des systèmes informatiques et télécoms de son entité, tant au niveau technique qu'organisationnel. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose les évolutions qu'il juge nécessaires pour garantir la sécurité du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projets, mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI.

E.3 Métiers du contrôle

o. **Post-auditeur :** de niveau BAC +5/+6, le post-auditeur, architecte de sécurité expérimenté et certifié « système » ou « réseau », établit la cartographie et oriente les investigations des équipes d'analyse dans un contexte difficile. Il intervient sur sollicitation à la suite d'un audit, d'un incident ou d'une intrusion, prend la mesure de la situation et propose un plan de remédiation. Conjointement à l'élaboration du profil de l'agresseur et à son éviction du système, il aide à produire les informations qui seront nécessaires pour les activités aval de remédiation avec les potentiels impacts métiers, pilotant les équipes et rendant compte. Ses compétences et son expertise des solutions lui permettent de dialoguer efficacement avec les interlocuteurs et experts techniques dans le(s) domaine(s) touché(s), qu'il mobilise en tenant compte de la culture de l'entreprise. Il propose les mesures techniques et processus palliatifs prioritaires à court terme..

p. **Audit & contrôle :** de niveau BAC +5, Le spécialiste de l'audit ou du contrôle recherche :

   i. la conformité, si requise, au plan réglementaire (contrôle des règles d'installation pour l'homologation ou la ré-homologation) ;

   ii. les vulnérabilités susceptibles de contourner les mécanismes de sécurité en conception ou en mode déployé afin d'éviter les compromissions de données ou d'éléments de protection.

q. **Intruder (hacker éthique) :** de niveau BAC +2 à BAC +5, « l'intruder » est en mesure de pénétrer le système d'information et d'identifier les divers chemins d'intrusions,

les techniques classiques ou atypiques utilisées, traçant ainsi le profil (profiling) des attaquants, leurs habitudes et méthode de travail (accès, dépôt, exfiltration, habitudes, périodicité…). Il connaît les principes de protection des produits de sécurité, leurs limites voire leurs méthodes de contournement. Se tenant informé grâce aux forums ad hoc et revues spécialisées, il est en mesure de développer des scénarios d'intrusion à l'état de l'art et peut se spécialiser sur certaines cibles techniques (systèmes d'exploitation, téléphonie sur IP, protocoles réseau, etc).

E.4 Développement des capacités

r. **Expert R&D cyber :** niveau bac+5 ou docteur, l'expert R&D identifie les technologies d'avenir et les technologies de rupture et contribue à développer la recherche académique dans le domaine cyber.

F. Les domaines de recherche académique

Les domaines académiques de recherche en cyberscurité 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		cyberprotection	Produits & technologies	technologies	cryptographie
	Public key (asymmetric) techniques	Digital signatures	cyberprotection	produits & technologies	technologies	cryptographie
		Public key encryption	cyberprotection	produits & technologies	technologies	cryptographie
	Symmetric cryptography and hash functions	Block and stream ciphers	cyberprotection	produits & technologies	technologies	cryptographie
		Hash functions and message authentication codes	cyberprotection	produits & technologies	technologies	cryptographie
	Cryptanalysis and other attacks		cyberprotection	produits & technologies	technologies	cryptographie
	Information-theoretic techniques		cyberprotection	produits & technologies	technologies	cryptographie
	Mathematical foundations of cryptography		cyberprotection	produits & technologies	technologies	cryptographie
Formal methods and theory of	Trust frameworks		cyberprotection	méthodes	environnement de conception	

Taxonomie de l' « Association for Computing Machinerie »			Référentiel PEC			
security					sécurisé	
	Security requirements		cyberprotection	services	ingénierie système	
	Formal security models		cyberprotection	méthodes	méthodes formelles	
	Logic and verification		cyberprotection	méthodes	méthodes formelles	
Security services	Authentication	Biometrics	cyberprotection	produits & technologies		
		Graphical / visual passwords	cyberprotection	produits & technologies		
		Multi-factor authentication	cyberprotection	produits & technologies		
	Access control		cyberprotection	produits & technologies		
	Pseudonymity, anonymity and untraceability		cyberprotection	produits & technologies		
	Privacy-preserving protocols		cyberprotection	produits & technologies		
	Digital rights management		cyberprotection	produits & technologies	technologies	informatique de confiance
	Authorization		cyberprotection	produits & technologies		
Intrusion/anomaly detection and malware mitigation	Malware and its mitigation		Cyberdefense	produits &technologies de LID	analyse de malware	
	Intrusion detection systems		Cyberdefense	produits &technologies de LID	détection d'intrusion	
	Social engineering attacks	Spoofing attacks	méthodes de LID	connaissance de la menace		
		Phishing	méthodes de LID	connaissance de la menace		
Security in hardware	Tamper-proof and tamper-resistant designs		cyberprotection	produits & technologies	technologies	composants électroniques
	Embedded systems security		cyberprotection	produits & technologies	produits	matériel et logiciel embarqué

Taxonomie de l' « Association for Computing Machinerie »			**Référentiel PEC**			
	Hardware security implementation	Hardware-based security protocols	cyberprotection	produits & technologies	technologies	composants électroniques
	Hardware attacks and countermeasures	Malicious design modifications	domaines fonctionnels	composants matériels		
		Side-channel analysis and countermeasures	cyberprotection	services	évaluation	évaluation composant
	Hardware reverse engineering		cyberprotection	services	évaluation	évaluation composant
Systems security	Operating systems security		cyberprotection	produits & technologies	technologies	logiciel sécurisé
	Mobile platform security	Trusted computing	cyberprotection	produits & technologies	technologies	logiciel sécurisé
		Virtualization and security	cyberprotection	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		cyberprotection	produits & technologies	produits	
	Denial-of-service attacks		cyberrésilience	méthodes	résistance aux attaques	
	Firewalls		cyberprotection	produits & technologies	produits	
	Vulnerability management	Penetration testing	cyberprotection	services	évaluation	évaluation système
		Vulnerability scanners	Cyberdefense	produits &technologies de LID		
	File system security		cyberprotection	produits & technologies	produits	
Network security	Security protocols		cyberprotection	produits & technologies	produits	
	Web protocol		cyberprotection	produits &	produits	

Taxonomie de l' « Association for Computing Machinerie »			Référentiel PEC			
	security			technologies		
	Mobile and wireless security		domaines fonctionnels	mobilité-nomadisme		
	Denial-of-service attacks		cyberrésilience	méthodes	résistance aux attaques	
	Firewalls		cyberprotection	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		cyberprotection	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		cyberprotection	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		

Taxonomie de l' « Association for Computing Machinerie »			**Référentiel PEC**			
	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		

G. Les plates-formes

L'ensemble des éléments présentés dans les précédents chapitres de ce document peut nécessiter à un moment ou 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, etc.). 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 PEC (pour plus de détails, se reporter au document : « Typologie de plateformes, Version 1.1 – Août 2016, Réf. PEC GTPF Ac D ») :

- 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 limitatif, 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 du savoir-faire sur la base de leurs connaissances. On distingue ainsi deux aspects de l'entraînement :

- 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 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).

H. Annexe

H.1 Versions du document

V1.0	10/04/2014	Première version diffusée suite au GT du 25 mars
V2.0	28/11/2014	Refonte complète document. 1. Identification des besoins sectoriels et opérationnels liés à la Cybersécurité pour la défense et le secteur civil. 2. identification préliminaire des Produits & Services Cyber français et étranger 3. Synthèse des axes de développement & d'applications de la filière Cybersécurité
V3.5	8/12/2014	Réorganisation et remise en forme du document Complément sur la partie technique
V4	3/6/2015	Ajout d'un éditorial Complément du chapitre C « domaines fonctionnels » Reprise du chapitre D Suppression des chapitres E et F
V4.1	1/7/2015	Evolutions mineures suite à relecture et réunion du GT
4.1.1	13/08/2015	Prises en compte des remarques d'un OIV
4.2	12/9/2016	Ajout d'un paragraphe sur les plates-formes Déplacement et refonte du chapitre sur les métiers Ajout d'un domaine fonctionnel identité numérique Corrections mineures
4.3	20/03/2017	Mise à jour de l'éditorial Remontée de la partie ACM dans le corps du document
4.4	9/05/2017	Restructuration du chapitre domaine fonctionnel
4.6	19/01/2018	Correction de coquilles, version finale avant publication