

Quelles sont les évolutions possibles de la gestion du personnel de défense pour lutter efficacement dans le cyberspace ?

CEIS

Systeme de réseaux

CYBERESPACE

Cyberconflit

Données

Lutte informatique

Infoguerre

Cyber warfare

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTRE DE LA DEFENSE



La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la Compagnie Européenne d'Intelligence Stratégique cette étude sur le thème " Quelles sont les évolutions possibles de la gestion du personnel de défense pour lutter efficacement dans le cyberspace ?", sous le numéro de marché 2013 105 009 4016.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique
75700 PARIS SP 07

1. Table des matières

2.	Introduction	6
2.1.	Constats	6
2.2.	Trois défis.....	6
2.3.	Objectifs	8
2.4.	Méthodologie de l'étude.....	8
2.5.	Périmètre	9
3.	Fondamentaux de l'emploi cyber	10
3.1.	Photographie de la population active « cyber ».....	10
3.1.1.	Quelques chiffres.....	10
3.1.2.	Des profils variés.....	12
3.2.	Un marché de l'emploi tendu	20
3.2.1.	Une demande en progression.....	20
3.2.2.	Une offre encore insuffisante	20
3.2.3.	Quelles perspectives ?	22
4.	Bonnes pratiques	23
4.1.	Gouvernance globale	26
	B1 : instituer une structure de gouvernance unifiée	26
	B2 : mettre en place un « guichet unique » en matière de carrières et de formation.....	27
4.2.	Alimentation du <i>pipeline</i>	31
	B3 : former les enseignants	31
	B4 : labéliser et certifier des formations.....	33
	B5 : revaloriser des filières scientifiques et techniques auprès des scolaires	36
	B6 : créer des «serious game » sur la cybersécurité.....	38
	B7 : animer une campagne de promotion des métiers cyber	40
	B8 : organiser des challenges pour les scolaires.....	45
	B9 : organiser des bootcamps.....	46
4.3.	Recrutement.....	48
	B10 : concevoir une méthode d'évaluation et de planification des besoins	48
	B11 : développer un modèle de maturité.....	49
	B12 : organiser une campagne de communication.....	53
	B13 : développer l'apprentissage	55
	B14 : développer les stages	57
	B15 : financer des bourses d'étude.....	59
	B16 : cibler des profils atypiques	62
	B17 : organiser des compétitions informatiques	63

B18 : développer une stratégie de relations privilégiées avec les écoles spécialisées.....	68
B19 : participer à des évènements spécialisés.....	69
B20 : adopter des procédures de recrutement flexibles.....	71
B21 : adopter un système de cooptation.....	72
4.4. Gestion des carrières	73
B22 : créer un référentiel des métiers et des compétences.....	73
B23 : mettre en place un processus normalisé de gestion des compétences	87
B24 : se doter d'outils d'évaluation des compétences.....	89
B25 : organiser la mobilité des profils	94
B26 : valoriser par le salaire.....	101
B27 : créer une communauté.....	105
4.5. Formation et entraînement.....	109
B28 : favoriser les <i>labs</i> et l'auto-formation afin de stimuler l'innovation	109
B29 : promouvoir le tutorat interne.....	109
B30 : faire de la formation continue une récompense et un moteur de mobilité interne.....	110
B31 : animer un centre de formation et d'entraînement mutualisé	111
B32 : former et sensibiliser les élites.....	116
B33 : mettre en place un centre de formation pour les personnels internes et externes	119
5. Analyse forces / faiblesses de la Défense par rapport à l'emploi « cyber ».....	122
5.1. Aperçu global	122
5.2. Analyse détaillée	124
5.2.1. Recrutement aujourd'hui : forces et faiblesses.....	124
5.2.2. Recrutement demain : menaces et opportunités	126
5.2.3. Formation aujourd'hui : forces et faiblesses.....	127
5.2.4. Formation demain : menaces et opportunités.....	129
5.2.5. Gestion des carrières et compétences aujourd'hui : forces et faiblesses	130
5.2.6. Gestion des carrières et compétences demain : menaces et opportunités.....	131
6. Recommandations	133
R1 : réaliser une évaluation de la situation existante	137
R2 : créer un observatoire des métiers et compétences cyber interministériel	138
R3 : organiser un challenge national public-privé	141
R4 : construire un centre d'entraînement intégré et mutualisé.....	142
R5 : créer un référentiel des emplois et compétence partagé	144
Les métiers	145
Les compétences et « talents » ou « appétences ».....	150
Le croisement des métiers et des compétences	151

R6 : favoriser le recrutement de hauts potentiels dans le domaine	154
R7 : proposer une offre de formation variée et cohérente.....	155
R8 : concevoir des parcours et communiquer des carrières, pas uniquement sur des emplois	156
R9 : faciliter la mobilité interne	157
L'inventaire des facteurs de mobilité pour mieux les adresser	157
Proposer des parcours-type.....	159
Laisser une liberté dans la mobilité grâce aux « aires de mobilité »	162
Créer le statut de « leader technique »	164
Créer une communauté.....	165
R10 : systématiser les échanges public-privé.....	166
R11 : former les DRH aux enjeux et spécificités du marché de l'emploi cybersécurité.....	167
R12 : faciliter l'accès aux ressources en créant une « cyber map » interactive	169
R13 : prévoir des possibilités d'admissibilité directe vers certains corps.....	172
7. Conclusion.....	173
8. Liste des entretiens	174
9. Bibliographie indicative	175
10. Table des illustrations.....	177
11. Annexes.....	180
11.1. Annexe 1 – Proposition d'un référentiel des métiers.....	180
11.2. Annexe 2 – Synthèse des bonnes pratiques	1
11.3. Annexe 3 – Synthèse des recommandations.....	6

2. Introduction

2.1. Constats

« Dans la mesure où le cyberspace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace ». C'est en ces termes que le Livre Blanc de 2008 avait fait de la lutte informatique défensive et offensive et de la cyberdéfense une priorité pour la France. Cinq ans après, de nombreuses actions ont été réalisées tant au niveau interministériel qu'au sein du Ministère de la Défense : mise en place de l'ANSSI (juillet 2009), publication d'une stratégie nationale de défense et de sécurité des systèmes d'information (2011) par cette même agence, création d'un poste d'officier général à la cyberdéfense au sein de l'Etat-major des Armées (2011), rédaction d'une doctrine interarmées de cyberdéfense (DIA 6-3) en 2011 etc.

Malgré un contexte budgétaire très contraint, cette montée en puissance s'accompagne d'une volonté de renforcement des compétences en matière de cyberdéfense, et ce dans les différentes composantes du dispositif défense (EMA Cyber, CALID, DGA, DPSD...). La réalisation des objectifs fixés au Ministère de la Défense dans le domaine dépend en effet largement de sa capacité à recruter, former et gérer des personnels spécialisés, et ce dans un marché de l'emploi « cybersécurité » où la demande est largement supérieure à l'offre.

2.2. Trois défis

Dans ce contexte, la Défense doit aujourd'hui affronter simultanément plusieurs défis :

- Un défi de recrutement. Au plan quantitatif, l'offre reste largement insuffisante par rapport à la demande. La 6^{ème} étude GIWS (Global Information Security Workforce study) publiée par Frost & Sullivan et (ISC)¹ sur les professionnels de la sécurité montrait en 2012 que le nombre de postes allait progresser de 10 à 15 % par an de 2010 à 2015. En 2013, à lui tout seul, le Pentagone planifierait le recrutement de 4 000 personnels civils et militaires. Au plan qualitatif, l'offre de formation initiale se révèle également peu en adéquation avec les besoins. De nombreux postes restent ainsi non pourvus, tant chez les « offreurs » que les « clients ». Au-delà des tensions du marché, la question de l'attractivité de la défense par rapport aux autres employeurs potentiels se pose également.
- Un défi lié à la gestion des carrières des personnels affectés à des missions de cyberdéfense et, plus globalement, à l'ensemble des opérations dans le cyberspace. Une fois ces personnels recrutés, il faut encore les fidéliser en leur proposant des carrières attractives et diversifiées, tant en termes de compétences que de niveaux. Cela suppose notamment une vision globale

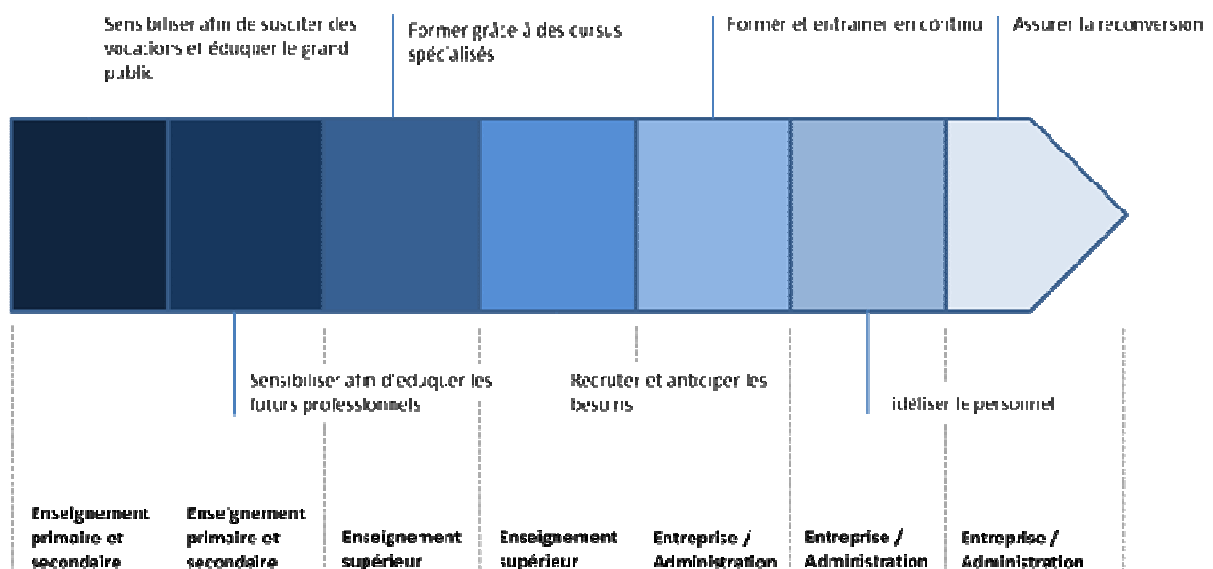
¹ http://www.computerworld.com/s/article/9236289/Pentagon_to_add_thousands_of_new_cybersecurity_jobs

de la cybersécurité, la définition d'un référentiel des emplois-type et d'une véritable stratégie RH dans le domaine.

- Un défi lié à la formation et à l'entraînement. L'innovation permanente et extrêmement rapide qui sous-tend le développement du cyberspace constitue un facteur d'attractivité non négligeable pour les personnes intéressées mais implique également l'animation d'un dispositif de formation continue et d'entraînement adapté pour maintenir les compétences en conditions opérationnelles. L'employabilité des seniors, désirant souvent évoluer vers des activités d'encadrement plus que vers des activités d'expertise soulève également des difficultés.

Au-delà des problématiques de recrutement, de gestion des carrières, de formation ou d'entraînement, c'est en fait tout simplement de la constitution et de l'animation d'un véritable « pipeline cybersécurité » qu'il s'agit.

Figure 1 : le pipeline cybersécurité



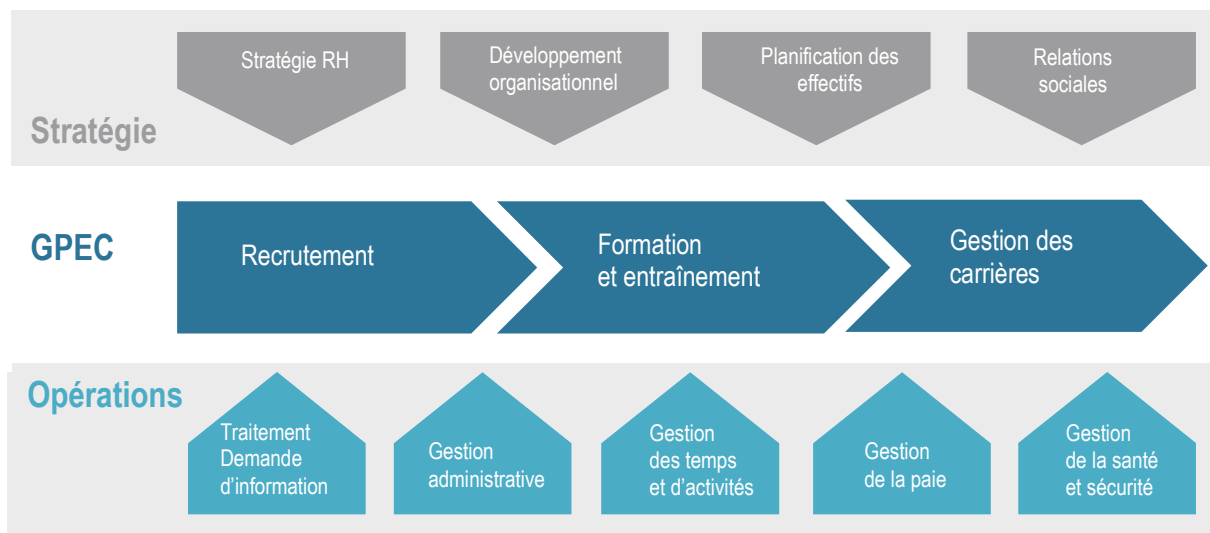
Ces défis ne sont d'ailleurs pas propres au monde de la Défense, ni même à la France. Même s'ils ont une acuité particulière dans ce domaine compte tenu de la spécificité des missions, on les retrouve, à des degrés divers, au sein des organisations privées, en France ou à l'étranger.

2.3. Objectifs

La mission a pour objectif de proposer au Ministère de la Défense des axes d'amélioration en matière de gestion prévisionnelle des emplois, effectifs et des compétences (GPEEC²) pour le personnel intervenant dans le domaine de la cyberdéfense.

Ces axes d'amélioration couvriront l'ensemble des leviers de la GPEEC présentés dans le schéma ci-dessous : recrutement (mobilité interne, recrutement externe, etc.), formation et entraînement (formation initiale, formation continue...), gestion des carrières (pilotage, rémunération, gestion de la performance, fidélisation, etc.).

Figure 2 : les composantes de la GPEC



2.4. Méthodologie de l'étude

La réalisation de l'étude a été structurée autour de 4 phases :

- Collecte de retours d'expérience menée grâce à des recherches documentaires et à la conduite d'entretiens. Cette phase a débouché sur la transmission d'une note de veille mensuelle tout au long du projet ;
- Identification des « bonnes pratiques » en matière de GPEC. Chaque « bonne pratique » fait l'objet d'une analyse permettant de mettre en exergue les résultats escomptés ainsi que les contraintes associées ;
- Identification des forces et faiblesses spécifiques de la Défense ;
- Proposition de recommandations.

² La GPEEC est une démarche d'ingénierie des ressources humaines qui consiste à concevoir, à mettre en œuvre et à contrôler des politiques et des pratiques visant à réduire, de façon anticipée, les écarts entre les besoins et les ressources disponibles, tant sur le plan quantitatif (effectifs) que qualitatif (compétences).

Figure 3 : les phases de l'étude



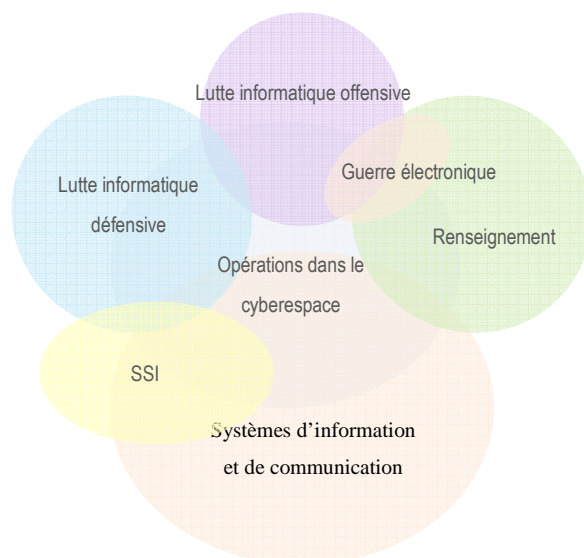
2.5. Périmètre

Le terme « cyber », régulièrement utilisé dans la suite de l'étude, recouvrira, sauf précision complémentaire, l'ensemble des opérations menées par le Ministère de la Défense dans le cyberspace, qui recouvrent les spécialités suivantes :

- La sécurité des systèmes d'information (SSI)
- La Lutte Informatique Défensive (LID) ;
- La Lutte Informatique Offensive (LIO) ;
- Le Renseignement d'Origine Cyber (ROC) et le Renseignement d'Intérêt Cyber (RIC) ;
- La guerre électronique.

Si ces différentes spécialités requièrent des compétences parfois très spécifiques, elles portent sur un même environnement, et partagent donc certaines caractéristiques, technologies ou capacités.

Figure 4 : les opérations dans le cyberspace



La sensibilité du sujet fait qu'une large partie de l'analyse portera d'abord sur la sécurité des systèmes d'information et la lutte informatique défensive. Les retours du secteur privé porteront d'ailleurs très logiquement sur ces deux aspects uniquement.

3. Fondamentaux de l'emploi cyber

L'objectif de ce premier chapitre est de dresser un panorama rapide de la population active dans le domaine à partir des quelques données existantes sur le sujet et d'identifier quelques fondamentaux du marché de l'emploi « cyber ».

3.1. Photographie de la population active « cyber »

3.1.1. Quelques chiffres

- **Données globales**

Au plan international, une étude menée par Frost & Sullivan pour le compte de l'organisation (ISC)³ évaluait en 2010 le nombre de professionnels de la sécurité de l'information à 2,28 millions dans le monde avec une croissance annuelle comprise entre 12 et 14 % selon les régions.

Figure 5 : Prévisions de croissance annuelle des emplois SSI

	2010	2011	2012	2013	2014	2015	2010-2015 CAGR
Americas	920,845	1,058,972	1,214,641	1,393,193	1,570,128	1,785,236	14,2%
EMEA	617,271	703,689	769,576	897,741	1,014,448	1,148,355	13,2%
APAC	748,348	830,666	924,531	1,038,248	1,168,029	1,310,529	11,9%
Total	2,286,464	2,593,327	2,935,748	3,329,183	3,752,605	4,244,120	13,2%

Ces chiffres sont évidemment à prendre avec beaucoup de précautions compte tenu des périmètres très différents que recouvrent les notions de sécurité des systèmes d'information et de cybersécurité selon les pays. Bien souvent sont en effet intégrés dans les professionnels de la sécurité des administrateurs systèmes ou réseaux qui disposent certes de compétences en matière de sécurité mais dont l'activité principale n'est pas la sécurité.

Au-delà du chiffre lui-même, c'est surtout la forte croissance de l'emploi « cyber » qui frappe, même si cette tendance varie légèrement d'un pays à l'autre. La société Wanted Analytics constate ainsi aux Etats-Unis 19 % d'offres d'emplois de plus en septembre 2012 par rapport à septembre 2011⁴.

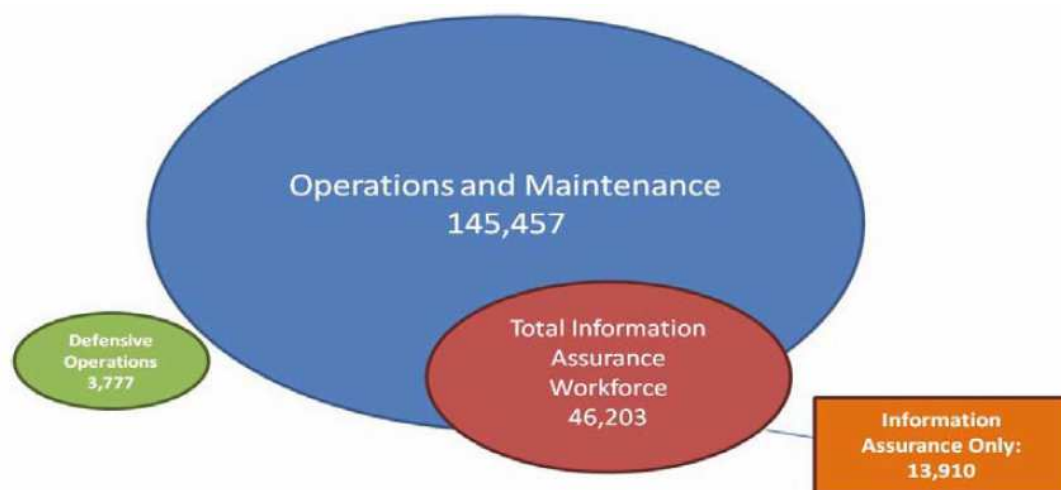
³ <https://www.isc2.org/GISWSRSA2013/>

⁴ <http://criminaljusticeschoolinfo.com/legal-justice-news/2013/02/cyber-security-career-paths-6213/>

- **Etats-Unis**

Cette définition extensive de la population active en cybersécurité est notamment en usage aux Etats-Unis. Il suffit pour s'en rendre compte d'analyser les données concernant la population active en cybersécurité de l'administration fédérale. La Cyber Operations workforce du DoD comptait ainsi 163 000 militaires et civils en 2009, dont 145 000 dévolus à l'exploitation et à la maintenance, 3 777 aux opérations défensives et 13 910 à la sécurité de l'information (« information assurance »). Le terme « cyber » recouvre donc ici l'ensemble des activités ayant trait aux systèmes d'information, non simplement la seule cybersécurité.

Figure 6 : Répartition de la « cyber operations workforce » fédérale américaine (2009)



- **France**

A titre de comparaison, la population active en matière de cybersécurité (c'est-à-dire dont la cybersécurité est l'activité principale) peut être évaluée, selon les personnes interrogées, à entre 15 et 20 000 personnes en France. Ce chiffre est inférieur à celui donné par l'Alliance pour la Confiance Numérique et la société PAC qui fait lui état de 40 000 personnes environ pour un chiffre d'affaires de 13 milliards, dont 4,5 en France⁵. L'écart vient là aussi d'une différence de périmètre, ce chiffre portant sur l'ensemble des activités de confiance numérique, lesquelles incluent environ 30 000 personnes employées par des acteurs industriels (fabricants, équipementiers, constructeurs, etc.) ou par des sociétés de services (archivage à valeur probante, fourniture de certificats, gestion d'identités, etc.) dont les produits et prestations concourent fortement à la sécurité mais dont la réalisation suppose des compétences nettement plus larges que la sécurité des systèmes d'information. Il serait donc intéressant de se référer systématiquement à une définition commune pour faciliter les comparaisons.

⁵ http://www.confiance-numerique.fr/wp-content/uploads/2014/05/brochure_observatoire_confiance_numerique_2013.pdf

3.1.2. Des profils variés

- **Quels diplômes ?**

Une majorité de la population active en cybersécurité est diplômée de l'enseignement supérieur, de premier ou second cycle. Sur 23 000 personnes appartenant à la cybersecurity workforce de l'administration fédérale américaine, près de 18 000 personnes indiquent posséder un diplôme universitaire⁶. Il convient donc de relativiser la problématique du hacker de génie autodidacte. S'il existe effectivement un certain nombre de profils atypiques, parfois non diplômés, cette population est limitée et constitue une minorité de la population active dans le domaine. Dans son étude "HACKER5 WANTED, an examination of the cybersecurity labor market" publiée en 2014⁷, la RAND Corporation confirme cette réalité et évalue les besoins à quelques pourcents. Cette minorité joue cependant un rôle important, notamment en matière de tests d'intrusion et de *reverse engineering*.

Ces profils atypiques posent par ailleurs d'épineux problèmes, tant pour le recrutement que pour la gestion des carrières. Difficile par exemple de proposer à ces profils des emplois en dehors des filières techniques. « *Le sujet nécessite de fait une certaine maturité, estime Sébastien Bombal, responsable de la majeure systèmes, réseaux, sécurité (SRS) au sein de l'Epita Paris. Il ne s'agit pas seulement de maîtriser des techniques, mais surtout d'avoir une approche globale de l'organisation de l'information au sein de l'entreprise.* »⁸ Ce qui manque alors, ce ne sont pas les compétences et capacités techniques, mais bien les « soft skills » en termes de management, de marketing, etc.

- **Quelles formations et certifications ?**

La formation initiale la plus répandue est sans surprise l'IT. Des spécialisations techniques sécurité se développent néanmoins, notamment sous la forme de masters spécialisés suivis à l'issue d'un cursus d'ingénieur généraliste. Apparaissent également quelques formations de premier cycle comme par exemple la licence CDAISI (collaborateur pour la défense et l'anti-intrusion des systèmes informatiques) lancée par l'IUT de Maubeuge.

La formation continue joue également un rôle clé dans le domaine. Pour deux raisons essentielles : d'une part, l'obsolescence rapide des compétences techniques, d'autre part la faiblesse des formations initiales (dédiées ou non) en matière de cybersécurité. Ces deux éléments poussent les recruteurs à investir de façon considérable dans la formation des jeunes recrutés en cybersécurité. Une entreprise de la défense américaine de plus de 100 000 employés⁹ explique ainsi qu'elle recrute principalement en interne au sein d'une population principalement constituée de scientifiques et d'ingénieurs. Elle a pour ce faire développé son propre cursus de formation interne structuré autour d'un tronc commun de

⁶ https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf

⁷ http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

⁸ <http://etudiant.aujourd'hui.fr/etudiant/info/fiche-metier-expert-de-la-cybersecurite-une-filiere-encore-rare.html>

⁹ http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

deux semaines de formation et d'une formation spécialisée de 6 à 8 mois pour les plus talentueux. Outre l'intérêt au plan opérationnel, la formation continue est également un moyen de fidéliser la main d'œuvre.

Les certifications jouent enfin un rôle capital dans le cursus des spécialistes de la sécurité pour les mêmes raisons. Le recruteur a par ailleurs besoin de disposer de points de repères et d'un certain nombre de garanties quant aux compétences du futur recruté dans un domaine nouveau. De façon globale, c'est la certification CISSP qui arrive au palmarès des certifications les plus répandues dans le domaine. 54 % des professionnels britanniques en cybersécurité (hors profils commerciaux) détiennent ainsi une certification CISSP¹⁰. Même constat aux Etats-Unis.

Figure 7 : Certifications sécurité les plus répandues en Grande-Bretagne

Qualification	All	NC	Com
MSc Infosec	5%	9%	0%
MBA	4%	4%	5%
CISSP	34%	54%	5%
CISA	9%	15%	1%
COSM	9%	15%	0%
QSA	4%	6%	1%
CLAS	4%	6%	1%
GIAC	3%	5%	0%
CEH	9%	14%	1%
CREST	1%	2%	1%
CHECK	1%	2%	0%
TIGER	0%	1%	0%
LPT	0%	1%	0%
CCNA	21%	31%	6%
ISO 27001 LA	4%	7%	0%
CompTIA Security+	3%	4%	1%

¹⁰ "Career analysis into cyber security : new & evolving occupations". Etude publiée en 2013 par la société Alderbridge pour le compte du programme « Cyber Security Learning Pathways Programme » de e-Skills UK.

- **Quelles expériences professionnelles ?**

Trois parcours-type peuvent être identifiés si l'on examine les emplois précédents des spécialistes sécurité :

- **Expérience(s) IT.** Une large partie des professionnels de la sécurité ont un début de carrière dans le domaine IT « généraliste. D'après l'étude britannique déjà citée, 28 % des personnes sondées en 2012 occupaient ainsi un poste précédent dans l'IT, ce pourcentage montant à 39 % si l'on considère le second emploi précédent, à 49 % pour le troisième emploi précédent. Seuls 4 % ont occupé précédemment dans un autre domaine que l'IT, 8 % si l'on remonte à l'emploi d'avant, 9 % si l'on remonte au troisième emploi précédent. 68 % avaient déjà un poste dans le domaine de la sécurité. Respectivement 68 %, 53 % et 45% occupaient enfin déjà un poste dans le domaine de la sécurité.
- **Expérience(s) sécurité.** Ce type de parcours, encore peu fréquent aujourd'hui, va naturellement se développer compte tenu de l'arrivée sur le marché de jeunes diplômés intégrant directement des emplois « sécurité ». Au plan quantitatif, il devrait cependant rester minoritaire par rapport au parcours IT.
- **Expérience(s) « métiers ».** Ce type de parcours est relativement rare. Plusieurs observateurs notent cependant l'apparition dans « la profession » de profils issus des métiers de l'organisation considérée, par exemple à des postes de responsable sécurité des systèmes d'information, principalement côté maîtrise d'œuvre.

Le *turnover* apparaît globalement assez faible dans le domaine. Une étude menée par Frost & Sullivan en partenariat avec Booz Allen Hamilton en 2013¹¹ souligne la stabilité des professionnels de la cybersécurité, seuls 3 % des personnes ayant déclaré un changement d'activité l'année précédant l'enquête.

- **Quelles compétences ?**

Un grand nombre des personnes déclarant avoir des activités en matière de cybersécurité partagent en réalité leur temps entre plusieurs activités et possèdent donc d'autres compétences IT. Si l'on examine par exemple les catégories de spécialités déclarées par les salariés civils du DoD américain intervenant en matière de sécurité, on observe ainsi que la catégorie de spécialités la plus représentée est à 73 % le support technique et le service client. Viennent ensuite la formation et la sensibilisation, l'expression de besoin et la planification. En queue de peloton : l'analyse forensique, l'analyse des menaces, le « all source intelligence » et les « cyber operations » qui sont des compétences peu répandues. Loin de se résumer au seul poste de RSSI comme on le pense souvent, la filière cybersécurité est ainsi composée d'emplois et de compétences diversifiées.

¹¹

https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=5&ved=0CD8QFjAE&url=https%3A%2F%2Fwww.isc2.org%2FGISWSRSA2013%2F&ei=kuPYU4aKH8HJ0QWjioGICA&usg=AFOjCNEF5GJscvZ11lqHcRzTdZb5_gNhsQ

Ces résultats démontrent également, s'il en était besoin, que la frontière entre les activités de cybersécurité et les activités IT « traditionnelles » sont difficiles à établir. Les compétences liées à la cybersécurité sont indissociables des compétences IT « génériques ». S'il est indispensable pour des raisons de gestion RH de distinguer les emplois à dominante « cybersécurité » des autres emplois IT, il est tout aussi indispensable d'établir des passerelles entre les différentes spécialités de cybersécurité et les autres emplois IT. La transformation numérique touchant l'ensemble des secteurs d'activité et des processus, il est en outre indispensable de développer des ponts vers les « métiers », la sécurité devant de plus en plus s'enraciner dans les activités de l'organisation.

Même constat dans un contexte militaire. L'Air Force américaine a ainsi défini deux types de postes¹² : ceux nécessitant des compétences se rapprochant de spécialités traditionnelles (renseignement, développement, guerre électronique, TIC, etc.) et ceux nécessitant un renforcement des spécialités traditionnelles combinées avec des capacités « cyber ». Des postes appelés « cyber hybrides ». Au total l'Air Force estimait en 2010 à 2 600 les emplois « cyber- hybrid » en son sein.

Les postes « cyber » sont donc, en large partie hybrides, à mi-chemin entre la sécurité, l'IT, mais aussi les métiers.

- **Quel âge ?**

Les informations disponibles montrent que la population active en cybersécurité est globalement assez âgée. 52 % des professionnels britanniques ont ainsi entre 30 et 49 ans, la tranche des 20-29 ans ne représentant que 7 % de la population active¹³. Même constat aux Etats-Unis : une étude du CIO Council et du DHS publiée en avril 2013¹⁴ indiquent que 78 % de la population active en cybersécurité au sein de l'administration fédérales (23 000 civils issus des 52 départements et agences fédérales ont répondu à cette enquête) est âgée de plus de 40 ans, les moins de 30 ans ne représentant que 5,15 % de la population totale. 20 % de cette population devrait même partir à la retraite dans les 3 ans, d'où les vives inquiétudes des autorités américaines devant le vieillissement de cette population et le besoin de voir arriver rapidement de jeunes diplômés.

Si la tendance au vieillissement de la population active en cybersécurité devrait s'inverser compte tenu de l'arrivée sur le marché de profils junior -une entreprise de services numériques française interrogée indique ainsi que 60 % de ses embauches dans le domaine concerne des profils juniors (0 à 2 ans d'expérience-, un trou subsistera néanmoins dans la pyramide des âges, ce qui pose notamment des problèmes de transmission de savoir-faire et d'encadrement dans certaines organisations.

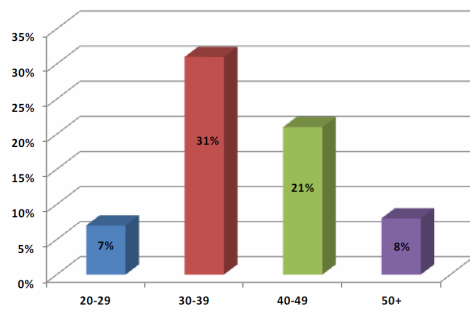
Figure 8 : répartition de la population active "cyber" par âge

¹² http://www.rand.org/content/dam/rand/pubs/documented_briefings/2010/RAND_DB579.pdf

¹³ "Career analysis into cyber security : new & evolving occupations". Etude publiée en 2013 par la société Alderbridge pour le compte du programme « Cyber Security Learning Pathways Programme » de e-Skills UK.

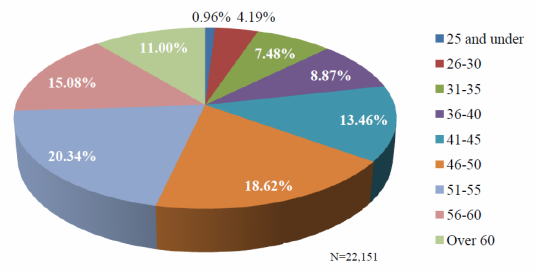
¹⁴ https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf

Situation en Grande-



Bretagne

Situation aux Etats-Unis



- **Quelle rémunération ?**

Les rémunérations varient fortement en fonction des postes et du niveau d'expérience. La grille ci-dessous a été établie avec l'aide de trois chasseurs de tête spécialisés dans l'IT et concernant spécifiquement la France.

Figure 9 : Niveaux de rémunération constatés en France

Domaine	Emploi	Age moyen en entrée de poste / Expérience professionnelle moyenne	Grille salariale (valeur du profil en entrée en en sortie) en K€ bruts annuels
Gouvernance de la sécurité des systèmes d'information	RSSI	15-18 ans minimum	75-130
	Chef de projet sécurité (MoA)	5-10 ans	48-60
	Responsable continuité d'activité	Si PCA profil du type 10 ans d'expérience, multiples cursus d'entrée possible (infra, infogérance, exploitation). Ne sont pas forcément spécialisés « sécurité » au départ.	60-75
Audit de sécurité	Auditeur sécurité technique (pen-testeurs, red team, etc.)	0 et plus (pas de filière de chasse identifiée en particulier).	35-60
	Auditeur sécurité organisationnel	3-8 ans	à partir de 45 (en fonction de ses certifications)
	Auditeur conformité	A partir de 3 années (si filière sécurité durant ses 3 premières années) Le plus souvent en banque, autour de 2-5 années d'expérience	40-52

Conception et déploiement de système d'information	Architecte système, architecte réseau, architecte application	10 ans + ou -	60-80 (plus le profil est technique plus il sera cher)
	Architecte sécurité/Référent sécurité projet	A partir de 10 années d'expérience	65-100 (idem poste précédent, plus il sera technique plus il sera cher)
	Chef de projet (MoE/MoI)	5-10 ans	45-60
Analyse de la menace et investigation numérique	Analyste/chercheur en vulnérabilités	Rien de pertinent à vous proposer nous avons peu de recul sur ces postes.	Inconnu
	Analyste malware		
	Analyste forensics et investigations		
Exploitation	Administrateur système, administrateur réseau	0-8/10 ans	35-55
	Administrateur sécurité	3-8 ans	44-50/55
	Technicien sécurité	0-6 ans	35-45
Développement logiciel et matériel	Architecte/concepteur logiciel	5-10	45/50 - 80
	Architecte/concepteur hardware	5-10	45/50 - 80
	Ingénieur de développement	0-5 années	37-50
	Cryptologue (cryptanalyste/cryptographe)	Rien de significatif pour vous donner une information fiable	Inconnu

Les comparaisons de salaires sont toujours délicates car elles supposent d’analyser également le coût de la vie dans chacun des pays et de tenir compte, en plus des rémunérations brutes annuelles, des charges sociales, de diverses primes et avantages généralement non comptabilisés dans les enquêtes. On se bornera donc ici à donner quelques indications concernant les salaires en vigueur aux Etats-Unis ou en Australie.

- Le salaire médian constaté aux Etats-Unis par la société Wanted Analytics¹⁵ pour les offres d’emploi estampillées cybersécurité en juillet 2014 s’établissait à 57 000 \$, soit 43 177 €.
- La grille des rémunérations¹⁶ 2012 des profils cybersécurité du DoD américain ci-dessous indique que pour le recrutement d’un profil junior de niveau « General Schedule » 8/9 (niveau master ou équivalent), la rémunération proposée va de 34 à 50 000 € annuels. Une offre d’emploi pour un « Information technology specialist (INFOSEC) » au *Navy Cyber Defense Operations Command* publiée en août 2014¹⁷ propose ainsi une rémunération de 54 à 77 000 \$, soit de 40 à 58 K€ annuels pour un profil GS 9 (master) avec 1 an d’expérience. On note par ailleurs que certaines agences du DoD comme la NSA ou le Cyber Command ont adopté pour certains profils spécifiques des régimes dérogatoires au droit commun pour proposer des rémunérations compétitives à certains spécialistes (voir bonne pratique B20 : adopter des procédures de recrutement flexibles).

Figure 10 : Grille des salaires « cybersécurité » du DoD (2012)

Civilian Grade	Percentage of Occupation	Annual Pay Band
GS-15	2	123,758 - 155,500
GS-14	12	105,211 – 136,771
GS-13	19	89,033 – 115,742
GS-12	28	74,872 – 97,333
GS-10/11	18	56,587 – 81,204
GS-8/9	17	46,745 – 67,114
GS-6/7	2	37,983 – 54,875
GS-5	2	34,075 – 44,293

¹⁵ <https://www.wantedanalytics.com/>

¹⁶ http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

¹⁷ <https://www.usajobs.gov/GetJob/ViewDetails/379307700>

- Le Defense Signals Directorate australien (données 2011)¹⁸ propose lui des « entry positions » avec des rémunérations de 66 000 à 91 000 \$ AUD (46 677 € à 64 000 €) et pour les « executive positions » des rémunérations de 101 à 141 000 AUD (71 à 100 000 €).

3.2. Un marché de l'emploi tendu

La forte augmentation des besoins en compétences et la rareté des compétences disponibles sur le marché de l'emploi génèrent une situation très tendue sur le marché de l'emploi « cyber », laquelle a notamment pour conséquence l'augmentation des rémunérations dans le domaine ces dernières années.

3.2.1. Une demande en progression

Selon le rapport du sénateur Jean-Marie Bockel sur la cyberdéfense (juillet 2012), les besoins pour la France étaient de 1 000 par an (200 pour les administrations et 800 pour le secteur privé). Côté américain, la DARPA indique que le seul DoD doit former 4 000 experts sécurité d'ici 2017¹⁹ quand le FBI souhaiterait lui embaucher 1 000 agents et 1 000 analystes en 2015²⁰. D'autres pays affichent également des objectifs de recrutement ambitieux. Le gouvernement indien a ainsi décidé de recruter 4 446 experts (contre 556 aujourd'hui)²¹. La demande devrait donc globalement progresser de 13,2 % par an jusqu'en 2017 estime la société de conseil Frost & Sullivan²².

Cette augmentation des besoins peut notamment s'évaluer grâce à l'analyse des offres d'emplois « cyber » publiées sur Internet. La société Wanted Analytics constatait ainsi dans son tableau de bord mensuel de juillet 2014 que 14 145 emplois « cyber » étaient alors proposés aux Etats-Unis avec une durée moyenne de publication de 46 jours, en forte augmentation par rapport à l'année précédente, le nombre d'offres aux Etats-Unis ayant progressé de 20 % entre avril 2012 et avril 2013²³.

3.2.2. Une offre encore insuffisante

L'ensemble des observateurs, tant en France qu'aux Etats-Unis s'accordent pour constater que l'offre de compétences est insuffisante sur le marché, tant d'un point de vue quantitatif que qualitatif.

Au plan quantitatif, Laurent Trébulle, directeur des relations entreprises à l'école d'ingénieurs Epita, constate : « on peut s'attendre à près de 1 000 à 1 200 recrutements en 2014, alors que le nombre de jeunes diplômés se situerait plutôt entre 200 et 300 par an »²⁴ « Nous avons 30 postes que nous ne parvenons pas à pourvoir », explique de son côté Sébastien Héon d'Airbus Defense & Security²⁵.

Mêmes échos outre-Atlantique où Diane Miller, directeur du programme CyberPatriot pour Northrop

¹⁸ http://www.asd.gov.au/publications/Cyber_Ops_Careers_Brochure_for_Industry.pdf

¹⁹ <http://www.defense.gov/news/newsarticle.aspx?id=121670>

²⁰ <http://www.businessweek.com/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete>

²¹ <http://www.iissm.com/newsletter/pdf/NewsletterJune1824.pdf>

²² The 2013 (ISC)2 Global Information Security Workforce Study

²³ <https://www.wantedanalytics.com/analysis/posts/network-security-concerns-drive-hiring-for-cyber-security-professionals-up-by-20>

²⁴ <http://www.metronews.fr/info/la-cybersecurite-un-eldoradopour-l-emploi/mnbb16OdEwn5RvpeM/>

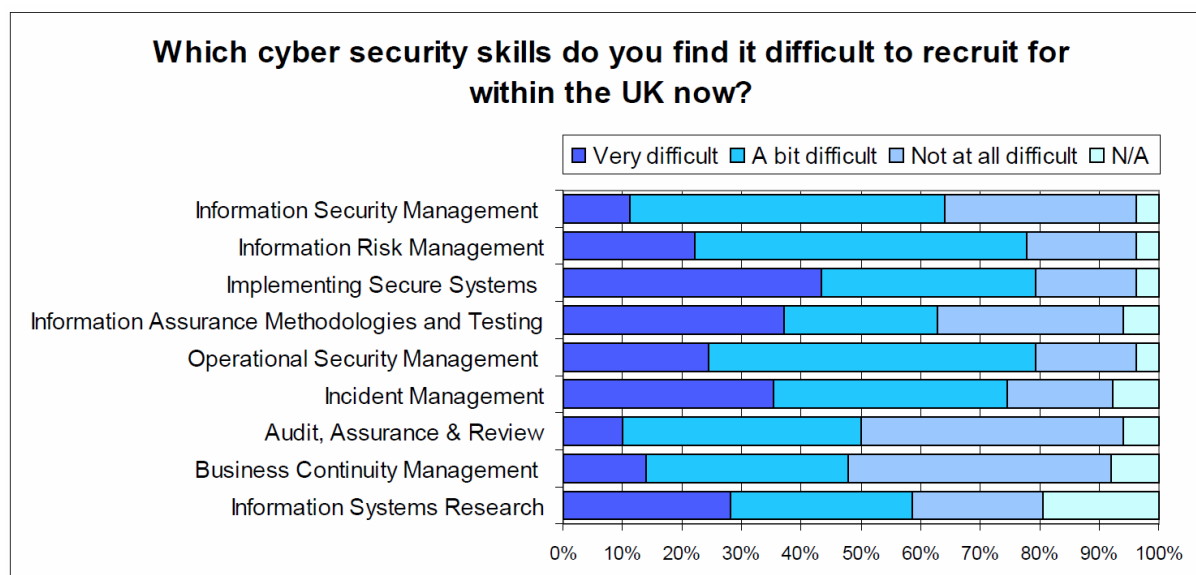
²⁵ <http://www.usinenouvelle.com/article/penurie-de-talents-en-cybersecurite-a-qui-la-faute.N190563>

Grumman se plaignait de ne pas réussir à trouver des personnes qualifiées pour les 700 postes cyber qui étaient ouverts dans l'entreprise en mai 2013²⁶.

Au plan qualitatif, les candidats sont loin d'avoir systématiquement les compétences et l'expérience requises par les recruteurs. Aux Etats-Unis, un tiers des CIO (Chief Information Officer) et CISO (Chief Information Security Officer) s'estiment satisfaits par la qualité des candidats²⁷. Le manque serait particulièrement criant pour les 5 % de postes les plus qualifiés, constate la RAND Corporation²⁸. Au plan fédéral, 83 % des recruteurs estiment ainsi difficile ou très difficile de recruter des candidats qualifiés.

En Grande-Bretagne, une étude publiée en mars 2014 sur les compétences sécurité manquantes montre que ce sont les compétences en matière de déploiement de systèmes sécurisés, de gestion d'incident et de méthodologies de protection des systèmes d'information qui sont les plus manquantes²⁹.

Figure 11 : quelles sont les capacités cyber difficiles à trouver sur le marché ?



Face à la difficulté de trouver les compétences idoines sur le marché, l'externalisation, qui contribue à la mutualisation des savoir-faire sécurité, est une solution intéressante, mais en aucun cas une solution miracle. Certaines tâches ne doivent pas être externalisées : tout dépend de la « densité métier » de celles-ci. Plus les tâches toucheront au cœur des activités de l'organisation considérée, moins celles-ci pourront être externalisées. Le recours massif à la sous-traitance en matière de cybersécurité, et plus globalement de technologies de l'information, est d'ailleurs l'une des faiblesses importantes des agences fédérales américaines.

²⁶ <http://www.bloomberg.com/news/2013-05-16/cybersecurity-starts-in-high-school-with-tomorrow-s-hires.html>

²⁷ https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf

²⁸ http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

²⁹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf

3.2.3. Quelles perspectives ?

L'écart existant entre l'offre et la demande devrait encore être la règle pendant quelques années, même s'il se réduira, principalement en raison du développement des formations spécialisées.

- **La demande ne devrait pas baisser à moyen terme**

La demande en compétences « cyber » ne devrait pas baisser à moyen terme en dépit des phénomènes de mutualisation de la sécurité, de « security by design » ou de standardisation des architectures. La transformation numérique gagne en effet l'ensemble des secteurs d'activité, des process et des organisations. Et la sécurité joue un rôle clé dans cette transformation. Par ailleurs, l'expansion des services managés dans la sécurité contribue à faire croître la demande, au moins dans un premier temps. Idem pour le développement du Cloud Computing qui génère de nouveaux besoins de sécurité. De nouveaux emplois, qui requièrent des compétences sécurité avec une densité plus ou moins forte, tels les métiers centrés sur les données (« data scientist », « chief data officer », correspondant informatique et libertés, etc.). Il est à cet égard intéressant d'observer que certains analystes américains estiment que le Joint Information Environment (JIE) du DoD, la nouvelle architecture Cloud de tout le réseau .mil, basé sur une infrastructure partagée et une architecture sécurité unique, qui consolide et standardise les fonctions et les datacenters du DoD, permettrait de diminuer le personnel affecté à la cybersécurité en homogénéisant les formations et les besoins à travers les services, et en supprimant ou limitant les problèmes de mobilité.

- **L'offre restera insuffisante**

Malgré le développement de cursus spécialisés et l'intégration de modules de cybersécurité dans des cursus IT généralistes, l'offre devrait rester à moyen terme insuffisante pour répondre à une demande en progression. L'élargissement de la base du « pipeline cybersécurité » ne portera en effet ses fruits que dans quelques années. A noter que ce constat dépasse largement la cybersécurité et concerne plus globalement l'ensemble du secteur des technologies de l'information, notamment en France. On note par ailleurs une certaine désaffection des jeunes pour les filières scientifiques et techniques et pour des carrières « techniques ». Ce constat est particulièrement marqué aux Etats-Unis où de nombreuses actions ont été lancées pour attirer des jeunes vers les filières STEM (scientifiques, techniques, engineering, mathématiques). La revalorisation des filières d'expertise technique est en effet un élément clé : tous les ingénieurs IT ne peuvent, ni ne doivent, opter pour des parcours managériaux ou « gestion de projet ».

La gestion du « pipeline » suppose cependant une évaluation permanente des besoins pour adapter l'offre de formation. Le risque serait en effet de créer une « bulle » avec des jeunes diplômés ou des professionnels qui ne trouveraient plus les débouchés suffisants. Pour Lazaro Pejsachowicz, président du CLUSIF, « *il faut rester prudent et ne pas demander au système public de former trop de gens. Le*

résultat se verra dans 5 ou 6 ans. Or personne ne sait comment sera le marché de l'emploi à ce moment-là. Il faut éviter de reproduire les erreurs commises par le passé dans d'autres secteurs³⁰ ».

4. Bonnes pratiques

L'utilisation de l'expression « bonnes pratiques » est sans doute un peu présomptueuse dans un domaine aussi nouveau et changeant que le cyberspace. Difficile en effet d'identifier ce qui sera à coup sûr efficace dans 6 mois compte tenu de la vitesse des évolutions technologiques ou d'usage qui sous-tendent le cyberspace. Difficile également d'identifier des « bonnes pratiques » universelles : ce qui est efficace au sein d'une organisation donnée ne l'est pas forcément pour une autre.

Plus que des « bonnes pratiques », les actions décrites et analysées dans ce chapitre sont donc d'abord des pratiques « innovantes », dont l'examen est susceptible de conduire à des améliorations dans la gestion des emplois « cyber ». Elles ont été structurées, en fonction de leurs principaux effets, autour des trois dimensions principales de la GPEC que sont le recrutement, la gestion des carrières, l'entraînement et la formation. Deux axes « gouvernance globale » et « alimentation du pipeline cybersécurité » ont été ajoutés pour catégoriser les actions intervenant en amont du recrutement, de la gestion des carrières ou de la formation continue et ayant un impact global sur la filière.

Avertissement : ces bonnes pratiques ont été identifiées grâce à des recherches documentaires et à quelques entretiens. Dans la très large majorité des cas, les actions décrites concernent les Etats-Unis ou la Grande-Bretagne. La collecte d'information s'est par ailleurs révélée relativement difficile auprès des entreprises qui sont souvent réticentes à évoquer le sujet, soit en raison du contexte tendu qui règne sur le marché de l'emploi « cyber », soit en raison de l'absence de dispositions RH spécifiques concernant la population « cyber ».

³⁰ <http://www.usinenouvelle.com/article/penurie-de-talents-en-cybersecurite-a-qui-la-faute.N190563>

Gouvernance globale

B1 - Mise en place d'une structure de gouvernance unifiée

B2 - Mise en place d'un « guichet unique » en matière de carrières et de formation

Alimentation du pipeline

B3 - Diffusion de kits de formation pour enseignants

B4 - Labéliser et certifier des formations

B5 - Revalorisation des filières scientifiques et techniques auprès des scolaires

B6 - Lancement de « serious game » sur la cybersécurité

B7 – Animer une campagne de promotion des métiers cyber

B8 - Organiser des challenges pour les scolaires

B9 - Organiser des bootcamps

Recrutement

B10 - Utilisation d'une méthode d'évaluation et de planification des besoins

B11 - Développement d'un modèle de maturité

B12 - Communiquer sur les emplois « cyber » grâce à une campagne de communication offensive

B13 - Développer l'apprentissage

B14 - Développer les stages

B15 - Financer des bourses d'étude

B16 - Cibler des profils atypiques

B17- Organiser des compétitions informatiques

B18 - Développer une stratégie de relations privilégiées avec les écoles spécialisées

B19 - Participer à des événements spécialisés

B20 - Adopter des procédures de recrutement flexibles

B21 - Adopter un système de cooptation

Gestion des carrières

B22 - Créer un référentiel des métiers et des compétences

B23 - Mise en place d'un processus normalisé de gestion des compétences

B24 - Se doter d'outils d'évaluation des compétences

B25 – Organiser la mobilité des profils

B26 – Valoriser par le salaire

B27 - Créer une communauté

Formation et entraînement

B28 - Favoriser les labs et l'auto-formation afin de stimuler l'innovation

B29 - Le tutorat entre collègues

B30 - Faire de la formation continue une récompense et un moteur de mobilité interne

B31 - Création d'un centre de formation et d'entraînement mutualisé

B32 - Formation et sensibilisation des élites

B33 - Mettre en place un centre de formation continue destinés aux personnels internes et externe

4.1. Gouvernance globale

B1 : instituer une structure de gouvernance unifiée

En 2009, le rapport Cyber In-security³¹ faisait quatre constats sans appel sur la gestion de la population active « cyber » de l'administration fédérale :

- Le « pipeline » de nouveaux talents n'est pas suffisant ;
- Une gouvernance fragmentée et un leadership non coordonné entravent la capacité de l'administration fédérale à répondre aux besoins en matière de main d'œuvre spécialisée en cybersécurité ;
- Des règles et processus compliqués gênent le recrutement et rendent difficile la fidélisation de la main d'œuvre ;
- Il y a une déconnexion entre les opérationnels qui recrutent et les équipes RH.

Lancée en 2010 à la suite de la Comprehensive National Cybersecurity Initiative (CNCI), la National Initiative for Cybersecurity Education (NICE)³², animée par le NIST (National Institute of Standards and Technology)³³, a pour objectif de répondre à ces défis en introduisant l'idée d'une gouvernance unifiée de la filière.

Le dispositif compte trois volets :

- Un volet « sensibilisation du grand public », dès l'école primaire pour sensibiliser les enfants aux dangers d'internet jusqu'à la promotion des carrières de la cybersécurité auprès des étudiants. La gouvernance de ce pilier a été confiée au DHS ;
- Un volet « développement du « pipeline » cybersécurité », dont la gestion est assurée par la National Science Foundation et le département de l'éducation. Ce pilier est axé principalement sur l'enseignement supérieur ;
- Un volet « développement de pratiques opérationnelles », dont la gouvernance est assurée par le DoD, le DHS et l'ODNI (Office of the Director of National Intelligence), à travers l'entraînement et la formation de la « cyber security workforce », la mise en place de stratégies de recrutement, la gestion de la filière etc. Dans ce cadre, une méthodologie de planification des besoins intéressante et un modèle de maturité ont été mis en place (voir point 4).

Même s'il est difficile d'en mesurer à l'heure actuelle les résultats, ce programme a le mérite d'avoir généré de nombreuses initiatives en matière de formations et contribué à alimenter le « pipeline » cybersécurité. Il a par ailleurs débouché sur la constitution d'un « Cybersecurity Workforce Framework » et d'un référentiel des emplois et compétences type en cybersécurité permettant à l'ensemble des acteurs de parler le même langage.

--	--

³¹ http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf

³² <http://csrc.nist.gov/nice/aboutUs.htm>

³³ <http://www.nist.gov/>

Descriptif	Le NICE comprend plusieurs volets : sensibilisation, développement du « pipeline », développement des pratiques opérationnelles.
Résultats	Difficiles à évaluer pour le moment. La coordination de l'ensemble des acteurs, tant publics que privés, est très lourde.
Contraintes associées	Il faut une structure d'animation permanente.
Intérêt	Le NICE contribue à développer le « pipeline » cybersécurité grâce à des actions portant sur l'ensemble de la chaîne, depuis la sensibilisation, la formation, jusqu'au recrutement. Il permet par ailleurs à l'ensemble des acteurs de discuter.

B2 : mettre en place un « guichet unique » en matière de carrières et de formation

Le NICCS (National Initiative for Cybersecurity Careers and Studies)³⁴ est présenté comme le guichet unique de la cybersécurité américaine en matière de carrières et de formation. Animé par le DHS, ce portail est la ressource principale pour le gouvernement, le secteur de l'industrie, le monde universitaire et le grand public de manière générale, pour la sensibilisation, la formation, le développement des effectifs et les évolutions de carrière dans la cybersécurité.

Le site est organisé autour de 4 rubriques principales : sensibilisation (il s'agit principalement de conseils en matière d'hygiène numérique³⁵), formation, entraînement et carrières. La navigation est facilitée par le fait que le visiteur peut facilement rechercher une information en fonction de son profil (grand public, étudiants, employés gouvernementaux ou professionnels de la cybersécurité par exemple) ou de ses objectifs (travailler dans la cybersécurité, évoluer dans sa carrière,



³⁴ <http://niccs.us-cert.gov>

³⁵ Le site relaie enfin une campagne de sensibilisation nationale baptisée Stop Think Connect (<http://www.stophinkconnect.org/>)

découvrir le référentiel des emplois ou se renseigner sur l'éducation de ses enfants).


Particularités du site :

- La découverte interactive des carrières en cybersécurité. L'utilisateur peut découvrir le référentiel NICE en navigant par domaine d'activité, spécialité, mission ou par compétences. Chacune des sept catégories précédemment évoquée est présentée ainsi que chaque spécialité qui y est rattachée. Les spécialités décrites dans le schéma précédent sont détaillées sous la forme suivante : une brève description de la spécialité, des métiers type relatifs à cette spécialité, les missions qui y sont attachées et les prérequis nécessaires (KSA : Knowledge, Skills and Ability). Le visiteur a en outre la possibilité de rechercher directement depuis chaque fiche les offres de formation correspondantes. Chaque fiche présente également les autres spécialités qui nécessitent les mêmes compétences. Il eut été intéressant de décrire de manière plus précise chacune des tâches avec par exemple une interview vidéo d'un professionnel ayant à les réaliser au quotidien. De même une interview d'un professionnel pour présenter le métier ainsi que la possibilité de rechercher directement des offres d'emploi associées, comme pour les formations, auraient conféré un caractère plus concret à chaque fiche.
- Entraînement et formation. Le portail propose un véritable catalogue des formations, des entraînements et des challenges. Le candidat peut effectuer une recherche selon plusieurs critères : la spécialité recherchée, son niveau, la localisation géographique de la formation ainsi que l'organisme de formation.
- Animation de la communauté. Le site propose des liens vers plusieurs « communautés de pratique » (CoP) centrées sur la cybersécurité pour permettre aux professionnels d'échanger entre eux.

A noter que cette initiative peut être rapprochée de la « cyber academy » créée en Grande-Bretagne en août 2013 et rassemblant employeurs, universités et écoles, administrations. Cette académie joue un rôle de « hub » et est soutenue et armée par le dispositif e-Skills. L'académie cyber constitue une partie de la National Academy for IT³⁶.

³⁶ <http://www.e-skills.com/professional-development/cyber-security/>

Figure 12 : exemple de fiche « emploi type » NICCS



Competencies

KSAs for the Specialty Area roll-up into the following

- Computer Forensics
- Computer Network Defense
- Incident Management
- Information Assurance
- Information Systems/Network Security
- Infrastructure Design
- Vulnerabilities Assessment

Incident Response

Related Job Titles | Tasks | KSAs [Show Courses](#)

Description

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Related Job Titles

Persons working in this Specialty area may have job titles similar to:

- Computer Crime Investigator
- Incident Handler
- Incident Responder
- Incident Response Analyst
- Incident Response Coordinator
- Intrusion Analyst

Tasks

Professional involved in this Specialty perform the following tasks:

- Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
- Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
- Employ approved Defense in Depth principles and practices (i.e., Defense in Multiple Places, Layered defenses, Security robustness, etc.)
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise

KSAs

Experts in the Specialty Area have the following Knowledge, Skills, and Ability:

- Knowledge of basic system administration, network, and operating system hardening techniques
- Knowledge of Computer Network Defense policies, procedures, and regulations
- Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools
- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution, etc.)
- Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])
- Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)

Descriptif	Le NICCS (National Initiative for Cybersecurity Careers and Studies) est un site-guichet unique pour la sensibilisation, la formation, l'entraînement et la découverte des carrières en cybersécurité.
Résultats	Le site se révèle très complet et relativement ergonomique.
Contraintes associées	Une animation permanente du site est nécessaire.
Intérêt	Intéressant notamment pour la découverte des carrières en cybersécurité via le référentiel NICE.

4.2. Alimentation du pipeline

B3 : former les enseignants

Le programme *Behind the screen* regroupe des projets et des ressources dédiées aux écoles britanniques³⁷. Géré par e-skills UK, le site propose 8 projets en cours (Social media, Coding in HTML5 and CSS, Understanding data and how it is used and stored by organisations, Cyber security, Website design, Game design, App design and development, Software architecture) et 4 autres en preparation (Coding in JavaScript, entrepreneurial use of technology, monitoring energy use with a Raspberry Pi, data analytics and benchmarking) développés avec des partenaires industriels (parmi lesquels Cisco, Dell, Delloite, HP, IBM, Steria, Atos, Capgemini, BT, Intel ou encore Oracle). Les projets consistent à la présentation d'un problème et la résolution de celui-ci de manière guidée grâce à des ressources et des supports fournis. Chaque projet dure entre 6 et 15 heures. Certains projets peuvent conduire à l'obtention d'un diplôme, le GCSE (General Certificate of Secondary Education). Le projet numéro 5 porte sur la cybersécurité. Il propose une sensibilisation aux notions de cybersécurité et de vie privée. Les écoles ont la possibilité de découvrir les règles de base pour assurer un niveau suffisant de sécurité au sein de l'entreprise.

L'utilisateur incarne un « cyber Ninja » qui doit se former aux principes de base de la cybersécurité. Pour avancer dans le jeu, l'utilisateur doit parcourir la ville Cybercity et remporter les défis à dispositions. Le *gameplay* n'est pas punitif et le joueur peut avancer comme bon lui semble dans les différents thèmes, en prenant connaissance des documents mis à sa disposition et en participant à des questionnaires et à des mini-jeux. A chaque défi accompli, le joueur obtient une récompense, un grade sous forme de « ceinture », confirmant ses connaissances en cybersécurité et l'encourageant à débloquent tous les autres défis. Ce jeu est à destination de ceux qui veulent parfaire leurs connaissances en matière de sécurité en ligne et aux néophytes qui veulent découvrir ce domaine de manière ludique et bien encadré. Le projet se conclut par la découverte des métiers de la cybersécurité et des opportunités qui s'offrent à eux dans leur orientation scolaire.

³⁷ <http://www.behindthescreen.org.uk/>

Descriptif	Le programme <i>Behind the screen</i> fournit des ressources de formation et de sensibilisation aux enseignants britanniques. L'un des projets concerne spécifiquement la cybersécurité.
Résultats	Contenus de qualité. Approche ludique intéressante.
Contraintes associées	Suppose la mise en ligne de nombreux contenus.
Intérêt	Action très en amont qui permet à la fois de sensibiliser les scolaires mais aussi de susciter des vocations

Figure 13 : saisie d'écran programme "Behind the screens"



B4 : labéliser et certifier des formations

Le CESG (Communications-Electronics Security Group), le bras armé du GCHQ en matière de sécurité de l'information, a lancé en partenariat avec l'EPSRC (Engineering and Physical Sciences Research Council) un label intitulé « ACE-CSR »³⁸ (pour Academic Centres of Excellence in Cyber Security Research). Objectif : adapter les recherches universitaires aux besoins du gouvernement, et plus largement du secteur public, et des entreprises³⁹. Actuellement, onze universités britanniques ont obtenu ce label.

Afin d'être labellisée, une université doit démontrer ses capacités en matière de cybersécurité au cours d'un appel à projet annuel⁴⁰. Principaux critères :

- Un environnement de recherche dédié à la cybersécurité, qui évolue dans un cadre et avec une stratégie bien établie
- Des chercheurs actifs, publiant régulièrement et reconnus par leurs pairs dans le domaine de la cybersécurité et dont les productions aboutissent à des utilisations concrètes
- Une production dont la qualité est reconnue dans la communauté de la cybersécurité au sens large, à savoir le secteur public et les entreprises
- Un programme pour les doctorants dont le niveau est soutenu
- Des projets financés par des acteurs extérieurs dont les résultats sont exploités par ces derniers

Le GCHQ a également démarré un programme de certification des formations proposées dans l'enseignement supérieur⁴¹. Jusqu'à présent, six formations spécialisées en cybersécurité (MSc – Master of Science, l'équivalent d'un Master 1) ont été certifiées dans le cadre du programme ACE-CSE (Academic Centres of Excellence in Cyber Security Education).

Cette certification fait partie intégrante de la stratégie britannique de cybersécurité. Les objectifs sont de faciliter le choix des étudiants et de s'assurer de l'adéquation des formations avec les besoins des employeurs. « *Chez BT, nous sommes parfaitement conscients de notre déficit en compétences et recruter les bonnes personnes avec les bonnes connaissances et capacités est un véritable défi pour nous. Le fait que le GCHQ reconnaisse ces cursus comme étant de haut niveau nous donne chez BT l'assurance que les personnes ayant ces diplômes ont les compétences que nous recherchons* », explique le président de BT Security, Mark Hughes⁴².

³⁸ <https://www.cesg.gov.uk/awaresstraining/academia/Pages/Academic-Centres.aspx>

³⁹ <http://www.epsrc.ac.uk/research/centres/acecybersecurity/>

⁴⁰ <http://www.epsrc.ac.uk/files/funding/calls/2014/scheme-to-recognise-academic-centres-of-excellence-for-cyber-security-research/>

⁴¹ http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-certifies-Masters-Degrees-in-Cyber-Security.aspx

⁴² <http://www.digitaltrends.com/computing/uk-spy-agency-approves-new-cyber-degrees/#!bMLRSz>

Afin de bénéficier de cette certification, les universités doivent répondre à plusieurs critères :

- Proposer aux futurs jeunes diplômés et aux employeurs des formations dont le contenu et la qualité sont en adéquation avec leurs attentes ;
- Accompagner les étudiants dans leur orientation professionnelle ainsi que les employeurs dans l'adaptation de leur processus de recrutement ;
- Mettre à disposition des moyens conséquents, afin d'attirer les meilleurs étudiants du Royaume ainsi que des étudiants étrangers.

Descriptif	Le GCHQ britannique a engagé un programme de labélisation et de certification de formations supérieures en cybersécurité.
Résultats	Les premières certifications venant d'être délivrées, il est trop tôt pour mesurer l'impact de ces programmes.
Contraintes associées	Il faut établir un référentiel très précis en amont.
Intérêt	Permet de s'assurer de la qualité des formations et de garantir leur adéquation avec les besoins des entreprises et organisations publiques.

Figure 14 : les critères de certification d'une formation cybersécurité par le GCHQ

Security Discipline	Skills Group	Indicative Topic Coverage
F. Incident Management <i>Principle: Capable of managing or investigating an information security incident at all levels.</i> CESG Knowledge Requirements include: <ul style="list-style-type: none"> Secure Information Management (stakeholder management within organisational context) Incident detection techniques Incident response management (internal and external) Audit log management Forensics (e.g. Evidential standards, Tools, Impact assessment) 	xi. Incident Management (F1)	<ul style="list-style-type: none"> Intrusion detection methods Intrusion response Intrusion management Incident handling Intrusion analysis, monitoring and logging
	xii. Forensics (F3)	<ul style="list-style-type: none"> Collecting, processing and preserving digital evidence Device forensics Memory forensics Network forensics Anti-forensic techniques Forensic report writing and expert testimony
Security Discipline	Skills Group	Indicative Topic Coverage
A. Information Security Management <i>Principle: Capable of determining, establishing and maintaining appropriate governance of (including processes, roles, awareness strategies, legal environment and responsibilities), delivery of (including policies, standards and guidelines), and cost-effective solutions (including impact of third parties) for information security within a given organisation.</i> CESG Knowledge Requirements include: <ul style="list-style-type: none"> Management frameworks such as ISO 27000 series Legislation such as Data Protection Act Common management Frameworks such as ISO 9000 	i. Policy, Strategy, Awareness and Audit (A1, A2, A3, A5, G1)	<ul style="list-style-type: none"> The role and function of security policy Types of security policy Security standards (e.g. ISO/IEC 27000) Security concepts and fundamentals <ul style="list-style-type: none"> Security roles and responsibilities Security professionalism Governance and compliance requirements in law Third party management Security culture Awareness raising methods Acceptable use policies Security certifications Understanding auditability The internal audit process
	ii. Legal & Regulatory Environment (A6)	<ul style="list-style-type: none"> Computer Misuse legislation Data Protection law Intellectual property and copyright Employment issues Regulation of security technologies
Security Discipline	Skills Group	Indicative Topic Coverage
E. Operational Security Management <i>Principle: Capable of managing all aspects of a security programme, including reacting to new threats and vulnerabilities, secure operational and service delivery consistent with security policies, standards and procedures, and handling security incidents of all types according to common principles and practices, consistent with legal constraints and obligations.</i> CESG Knowledge Requirements include: <ul style="list-style-type: none"> Governance and Management responsibilities IT Service Management processes (e.g. ITIL) Existing and Emerging Vulnerabilities Use of penetration testing and vulnerability testing Risk Assessment and Monitoring Operating Procedures and accountability Continuous improvement 	ix. Secure Operations Management and Service Delivery (E1, E2)	<ul style="list-style-type: none"> Internet threats: common attacks (human and technical), malicious code, situational awareness, threat trends, threat landscape, CERTs, adversarial thinking Cryptography: AES and RSA, key management, digital signatures Network security: networking fundamentals, firewalls and traffic filtering, intrusion detection and prevention systems, intrusion analysis, network monitoring, mobile and wireless network security System security: authentication (secrets, tokens, biometrics), access control (MAC, DAC, RBAC) and privilege management, mobile device security and BYOD, anti-virus technologies Application security: email, Web, social networks, DRM, database security, big data security, identity management Physical security: physical and environmental controls, physical protection of IT assets
	x. Vulnerability Assessment (E3)	<ul style="list-style-type: none"> Malware analysis: static and dynamic analysis, detection techniques, host-based intrusion detection, kernel rootkits System and network-level vulnerabilities and their exploitation Vulnerability analysis and management Penetration testing Social Engineering Dependable/resilient/survivable systems

B5 : revaloriser des filières scientifiques et techniques auprès des scolaires

Le manque de personnel dans la cybersécurité réside en partie dans le manque d'attractivité des carrières scientifiques et techniques, aujourd'hui largement sous-valorisées. Afin de revaloriser ces filières, le Gouvernement britannique a lancé le programme STEMNET⁴³ (Science, Technology, Engineering and Mathematics NETwork). Ce programme, soutenu par le DfE (Department for Education) et le BIS (Department for Business, Innovation and Skills), a pour objectif de communiquer massivement sur les filières techniques et scientifiques auprès des étudiants du primaire. Ce programme repose sur trois axes :

- STEM Ambassadors : le programme a constitué un réseau de représentants, dont le nombre avoisine les 27000, dont la majorité sont relativement jeunes (moins de 3 ans). Issus de plusieurs professions (ingénieurs, biologistes, pharmaciens ou architectes par exemple), leur fonction est de promouvoir les filières techniques et scientifiques auprès des écoliers. La gestion des ambassadeurs est décentralisée : chaque région gère son propre réseau. Le processus pour devenir ambassadeur est assez aisé puisqu'il suffit de s'inscrire sur le site. Une campagne de communication nationale a été lancée en mars 2014.
- STEM Clubs Programme : le programme STEM met gratuitement à disposition des écoles des conseils et des supports pédagogiques en vue de constituer des clubs pour les enfants. Un site tiers⁴⁴ est totalement dédié aux clubs. Si le site propose des conseils pratiques, comme la construction d'un plan d'action pour le club, les contenus sont pour le moment très peu nombreux. A la demande d'une école, STEMNET peut envoyer un ambassadeur pour aider à la mise en place du club.
- Schools STEM Advisory Network : le programme propose enfin des supports et la mise à disposition de personnels afin d'aider les étudiants à construire leur projet professionnel et à les orienter. Cette structure est la plus aboutie des trois : les coordonnées de chaque responsable par zone sont disponibles sur le site et les employeurs peuvent contribuer à cette initiative en orientant la prochaine génération d'actifs britanniques par leurs retours d'expérience et l'expression de leurs besoins.

Ce programme semble à priori être un succès puisque 71% des enfants ayant rencontré un ambassadeur STEM déclare aimer la science (contre 55% initialement). Il en est de même pour les enfants appartenant aux clubs STEM, le chiffre atteignant même 80%. Ce programme est complété par des événements ponctuels autour des filières techniques et scientifiques. Le programme gagnerait toutefois à afficher des sponsors, notamment au niveau de son réseau d'entreprise afin d'accroître ses vecteurs de communication.

--	--

⁴³ <http://www.stemnet.org.uk/>

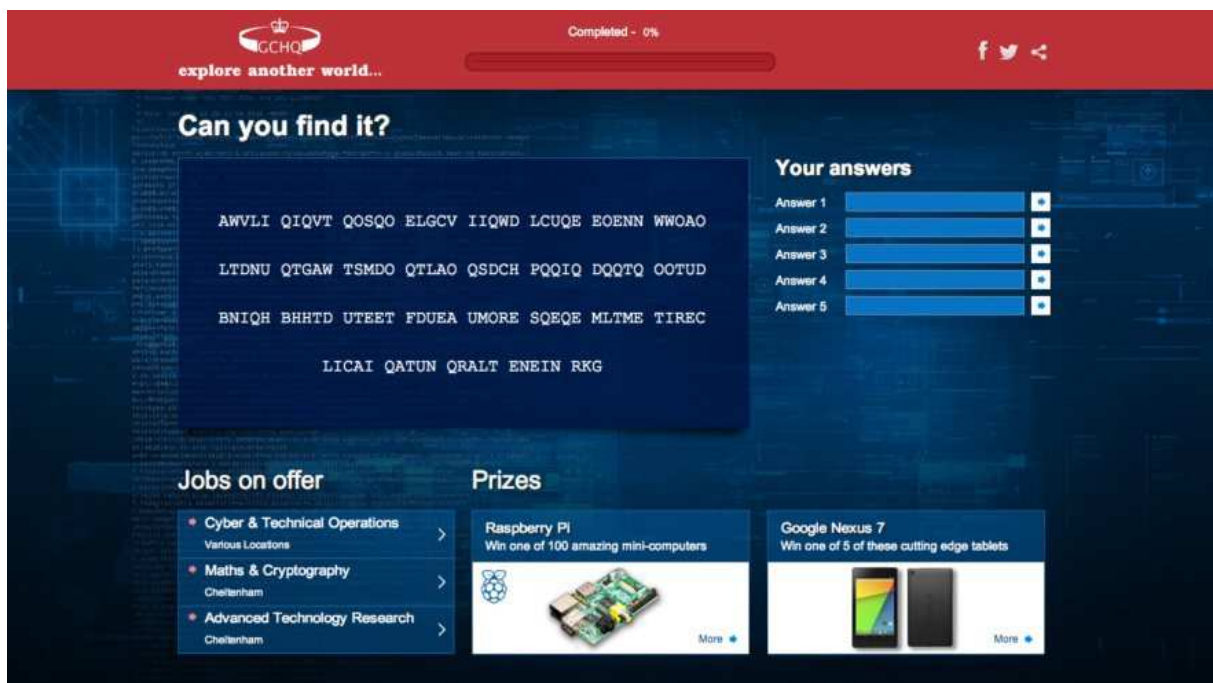
⁴⁴ <http://www.stemclubs.net/>

Descriptif	Le programme a pour objectif de communiquer massivement sur les filières techniques et scientifiques auprès des étudiants du primaire pour revaloriser ces parcours.
Résultats	Les statistiques semblent montrer l'efficacité du programme.
Contraintes associées	Structure d'animation
Intérêt	La valorisation des cursus scientifiques et techniques est un vrai enjeu.

B6 : créer des «serious game » sur la cybersécurité

Le GCHQ a lancé une campagne en ligne, « Can you find it? »⁴⁵, proposant des défis avec des codes complexes à trouver en ligne et à résoudre. L'objectif est de tester les capacités des potentiels futurs employés. Cette campagne fait suite à une initiative de l'année dernière intitulée « Can you crack it? »⁴⁶: 5 000 personnes ont participé, dont 170 ont été reçues en entretien par l'organisme, les postes proposés offrant des salaires variant entre 26 000 £ et 60 000 £. Le site dispose curieusement d'une version française, seule langue représentée, ce qui tendrait à prouver que le GCHQ est prêt à recruter des français ou tout au moins des francophones.

Figure 15 : saisie d'écran de la campagne du GCHQ "Can you find it ?"



A noter que la Marine nationale française avait engagé une opération similaire en 2009 dans le cadre de sa campagne de recrutement *Etre Marin*. Plusieurs *serious games*⁴⁷ présentaient les différents corps de métier de la Marine afin de susciter des vocations. Jouables sur Internet, ces huit jeux illustraient les différents métiers. A titre d'exemple, le jeu « exfiltration d'otages » proposait une mission de protection d'otage, sur un principe proche du « Tower Defense » en plaçant des unités en couverture sur la plage, l'otage essayant ensuite de rejoindre le bateau, poursuivi par des assaillants.

⁴⁵ <http://www.thecodex.com/en/gchq-can-you-find-it-solution>

⁴⁶ http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-code-cracking-challenge-reveals-UK-talent.aspx

⁴⁷ <http://www.jeux-serieux.fr/2009/04/14/des-serious-games-pour-devenir-marin/>

Descriptif	Le GCHQ a lancé une campagne en ligne, « Can you find it? » ⁴⁸ , proposant des défis avec des codes complexes à trouver en ligne et à résoudre.
Résultats	Bons résultats
Contraintes associées	Conception et développement informatique
Intérêt	Action de communication efficace sur une cible 10-15 ans

⁴⁸ <http://www.acumin.co.uk/main/news/view/gchq-launches-new-campaign-to-fill-cyber-security-roles/3824>

B7 : animer une campagne de promotion des métiers cyber

B7-1 : animer une campagne permanente

Big Ambition⁴⁹, une branche de e-Skills UK, est un programme qui a pour vocation de pousser les jeunes âgés de 14 à 19 ans à s'orienter vers des carrières dans le domaine de l'IT. Ce programme, financé par plusieurs entreprises (Accenture, IBM UK, Hewlett Packard, Microsoft, Oracle, Vodafone and T-Mobile, British Airways, Ford Motor Company, EDF Energy, BT, etc.), mène plusieurs campagnes pour faire découvrir les métiers et les entreprises du secteur.

Le site propose plusieurs supports interactifs et très visuels pour communiquer auprès du public ciblé : vidéo, fiches de poste, jeux, quizz, etc. L'entrée en matière fait appel au patriotisme du visiteur puisque la vidéo de présentation du portail s'achève sur le message « *Your country needs you* ». Le programme semble avoir du succès puisque depuis son lancement en 2013, près de 1000 étudiants ont dit avoir été « inspirés » par les ressources proposées.

Le site propose une présentation plus ludique de quelques métiers bien spécifiques à la cybersécurité (pen tester, analyste de code malveillant, RSSI, risk manager ou analyste forensic)⁵⁰. Chaque métier fait l'objet d'une fiche qui présente les compétences nécessaires à la réalisation de ce métier sous la forme de pourcentages : sang-froid nécessaire, niveau technique requis et la réputation. De même, l'expérience nécessaire, le niveau de salaire et la position stratégique au sein de l'entreprise sont exprimés en pourcentages, ce qui est certainement plus parlant pour le public visé.

Figure 16 : fiche de poste de RSSI sur le site Big Ambition



⁴⁹ <https://www.bigambition.co.uk/>

⁵⁰ <https://www.bigambition.co.uk/BigAmbition/cyber-careers/index.html#/meet>

Une fois les 5 métiers découverts, le visiteur poursuit sa visite à travers un mini-jeu dans lequel il est appelé à s'immerger dans 5 situations différentes : une fraude à l'encontre d'une plateforme de musique en ligne, une banque victime de cyberattaques, le défacement du site de la mairie, l'intrusion dans le système de contrôle du métro et la volonté du maire de lutter contre tous ces fléaux. Des indices permettent au joueur de mieux comprendre les caractéristiques de chaque incident et de faire appel au métier le plus adapté pour le résoudre.

Secure Future⁵¹ propose au joueur d'intégrer l'agence nationale de cybersécurité du pays pour lutter contre la cybercriminalité au sein d'une ville à travers plusieurs petits jeux. Le premier, *Rescue the Rocket Programme*⁵², représente à l'écran une ville dans laquelle les attaques apparaissent en rouge. Le but est alors de cliquer sur l'élément pour découvrir l'origine du problème et de le résoudre grâce aux réponses proposées. Un score apparaît en fonction des réponses apportées et les missions sont au fur et à mesure complétées (« Disaster recovery » et « Risk management » en l'espèce). A la fin du jeu, outre le score, un message demandant au joueur s'il est intéressé par la cybersécurité apparaît.

Figure 17 : saisie d'écran du jeu "rescue the rockets"



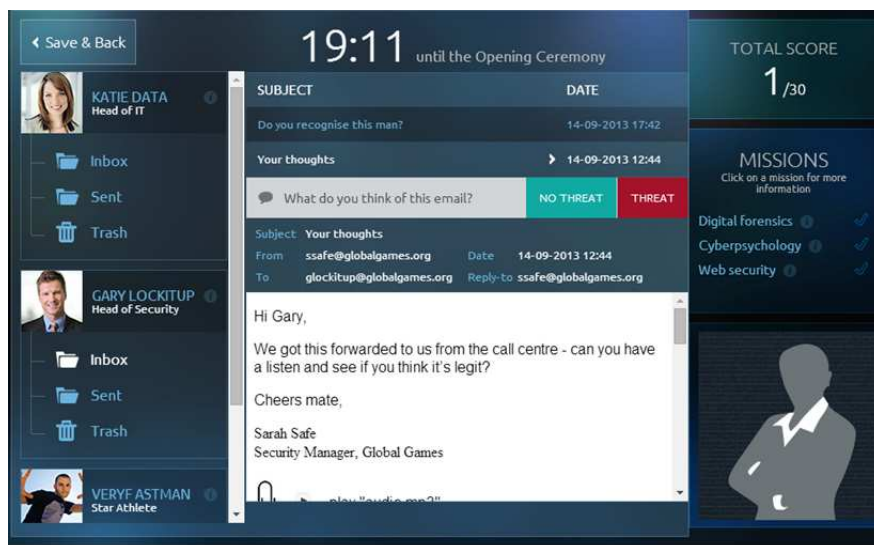
Autre jeu proposé : *Save the Global Games*⁵³ à travers lequel le joueur doit gérer l'équipe de sécurité d'un évènement à venir : les jeux olympiques qui se déroulent cette année à Cardiff. A travers les boites mails de plusieurs personnages (Katie Data, la directrice de l'IT, Gary Lockitup, le directeur de la sécurité et Veryf Astman, un athlète reconnu), le joueur doit déterminer si les sujets évoqués dans les mails représentent ou non une menace. Ce jeu est nettement plus difficile que le précédent : un chronomètre est affiché et toute mauvaise réponse entraînant une perte du temps, les réponses doivent être justifiées et rapportent moins de points. En outre, le nombre de missions a augmenté (Digital Forensics, Cyberpsychology et Web security).

⁵¹ <http://www.bigambition.co.uk/secure-futures/>

⁵² <http://www.bigambition.co.uk/secure-futures/games/rescue-the-rocket-programme/>

⁵³ <http://www.bigambition.co.uk/secure-futures/games/save-the-global-games/>

Figure 18 : saisie d'écran du jeu « save the global games »



La plateforme Big Ambition met enfin à disposition un outil intitulé *Dreamjob*⁵⁴ qui propose au joueur de choisir en quatorze étapes les sujets qui l'intéressent ainsi que de décrire ses traits de caractère. A l'issue de ces étapes, le site propose une suggestion de métiers de la cybersécurité :

Intitulé	Animation d'une campagne de promotion des métiers de la cybersécurité
Descriptif	Le programme britannique « Big Ambition » a lancé plusieurs campagnes pour faire connaître les métiers de l'IT, et notamment les métiers de la cybersécurité.
Résultats	L'idée est intéressante mais les fiches de poste proposées sont assez succinctes, voire incomplètes. Les jeux, quoique simples, sont très bien faits.
Contraintes associées	Développement informatique
Intérêt	Approche ludique ciblant les 10-15 ans.

⁵⁴ <https://www.bigambition.co.uk/Lib/BA/Assets/FlashActivities/Activities/DreamJob1/>

B7-2 : animer une campagne ponctuelle

Dans le cadre du programme NICE, le DHS, en coopération avec le National Cyber Security Alliance et le Multi-State Information Sharing and Analysis Center, a lancé le National Cyber Security Awareness Month (NCSAM)⁵⁵. Objectifs : sensibiliser et éduquer le secteur public et privé aux enjeux de la cybersécurité. Le NCSAM a lieu chaque mois de novembre et l'année 2014 marque la 11^{ème} édition de celui-ci.

L'édition 2014 du NCSAM présente notamment les métiers cyber des forces de l'ordre et met en avant la campagne « Stop. Think. Connect. » qui propose de nombreux supports de communication et pédagogique sur la cybersécurité.

A l'occasion du NCSAM, plusieurs organisations communiquent sur les métiers de la cybersécurité⁵⁶ et profitent de cette occasion pour programmer des événements autour des métiers de la cybersécurité⁵⁷ à l'image de la CyberMaryland Conference (29 et 30 octobre 2014) durant laquelle a lieu le Cyber Career Job Fair⁵⁸.

Intitulé	
Lancement d'une campagne ponctuelle de promotion des métiers cyber	
Descriptif	Le DHS organise chaque année le National Cyber Security Awareness Month (NCSAM). Les événements organisés dans le cadre de ce mois de la cybersécurité ont pour objectifs non seulement de sensibiliser le grand public mais aussi de communiquer sur les carrières et emplois cyber.
Résultats	Excellents. L'édition 2014 est la 11 ^{ème} .
Contraintes associées	Aucune
Intérêt	Permet de fédérer les différents événements existants et de les labéliser

⁵⁵ <http://www.dhs.gov/national-cyber-security-awareness-month-2014>

⁵⁶ <http://www.staysafeonline.org/ncsam/events>

⁵⁷ <http://www.educause.edu/blogs/vvogel/lets-get-ready-ncsam-2014>

⁵⁸ <http://www.cybermaryland.org/>

B8 : organiser des challenges pour les scolaires

Au Royaume-Uni, le Cabinet Office organise depuis quelques années une compétition en cybersécurité⁵⁹. En 2014, près de 700 établissements anglais d'enseignement secondaire y ont participé. L'objectif est de d'identifier les jeunes hackers les plus talentueux du Royaume et de mettre en valeur les opportunités d'emplois du secteur cyber pour les jeunes générations. Par équipe de 4, l'épreuve consistait à casser des codes afin de découvrir un message. Avec le support d'entreprises telles que QinetiQ, Sophos, Cassidian ou Raytheon, les équipes gagnantes étaient récompensées d'un prix de 1 000 £ destiné à l'école.

En 2014, le cabinet Office a décidé de renouveler son programme scolaire permettant l'organisation de challenge de cybersécurité en vue d'évaluer le niveau de compétence des élèves en la matière. Cette année, le Gouvernement britannique a décidé d'investir 100 000 £ afin d'étendre cette initiative au reste du pays⁶⁰. Chloe Smith, du Cabinet Office, a déclaré : « *c'est une fantastique opportunité pour être sûr que les élèves qui possèdent un talent dans le domaine puisse être identifiés et guidés. Le Royaume-Uni a une réputation mondiale en matière d'éducation et d'apprentissage et nous voulons faire la même chose dans le cyber* ».

Les Émirats Arabes Unis ont également mis en place une compétition de cybersécurité pour lycéens⁶¹. Le but de ce concours est de sensibiliser les jeunes émiriens aux opportunités d'emplois dans le secteur cyber. Les écoles participantes ont été intégrées dans un programme de formation cyber de 5 mois afin de préparer les lycéens à la compétition et de repérer les éléments les plus prometteurs. L'événement réunit pour le moment 79 lycéens de 6 écoles du royaume et le gouvernement souhaite aujourd'hui étendre cette initiative au reste des écoles du pays.

Intitulé	
Intitulé	Organiser des challenges pour les scolaires
Descriptif	Le Cabinet Office britannique organise chaque année un challenge inter-écoles auquel participent près de 700 établissements d'enseignement secondaire.
Résultats	Très bons résultats

⁵⁹ <http://www.wired.co.uk/news/archive/2013-06/10/cyber-security-challenge-codebreaking>

⁶⁰ <http://cybersecuritychallenge.org.uk/story/421/cabinet-office-back-expansion-of-cyber-security-challenge-talent-search-in-uk-classrooms.php>

⁶¹ <http://www.thenational.ae/uae/technology/students-take-part-in-uae-cyber-security-contest>

Contraintes associées	Préparation des épreuves et organisation du challenge
Intérêt	Permet de susciter des vocations et d'identifier de jeunes talents

B9 : organiser des bootcamps

Le Council on Cybersecurity⁶², une organisation à but non lucratif regroupant plusieurs acteurs publics et privés américains (SANS Institute, Qualys, Tripwire, DHS, Department of Energy, etc.), a mis en place l'US Cyber Challenge qui organise des stages d'été dédiés à la cybersécurité. Ces camps d'été, ou boot camps, incluent des cours dispensés par des membres de l'institut SANS, des professeurs d'université et des spécialistes de la cybersécurité. Contenus proposés : la détection d'intrusion, le pen testing, le forensic, rencontre avec des employeurs, challenge de type *capture the flag*.

La condition d'accès à ces bootcamps est de s'être qualifié en ligne au tournoi CyberQuests organisé au mois d'avril précédent la formation. Ces formations sont réservées aux citoyens américains, alors même que le tournoi CyberQuests est international, et les places sont distribuées sur invitation, la capacité d'accueil étant limitée.

Cette année, 4 bootcamps sont ouverts :

- Eastern Regional Cyber Camp - Virginia Tech (du 16 au 20 juin 2014)⁶³
- State of Delaware Cyber Camp - University of Delaware (du 21 au 25 juillet)⁶⁴
- State of Illinois Cyber Camp - Moraine Valley Community College, Palos Hills, Illinois (du 4 au 8 août)⁶⁵
- Western Regional Cyber Camp - San Jose State University, San Jose (du 11 au 15 août)⁶⁶

Ces stages d'été ont l'avantage d'être concentrés sur une période relativement courte et de proposer un parcours complet, de l'entraînement au recrutement.

D'autres organismes, tel que Infosec Institute⁶⁷, proposent également des bootcamps mais qui sont cette fois-ci destinés à délivrer des certifications à des personnels déjà qualifiés, y compris du secteur public.

⁶² <http://www.counciloncybersecurity.org/>

⁶³ <http://www.security.vt.edu/uscc.html>

⁶⁴ http://dti.delaware.gov/information/cybersecurity_challenge_boot_camp.shtml

⁶⁵ <http://www.cssia.org/cssia-uscc.cfm>

⁶⁶ <http://www.sjsu.edu/cybersecurity/events/cyberchallenge/>

⁶⁷ <http://www.infosecinstitute.com/>

Intitulé	Organiser des bootcamps
Descriptif	Le Council on Cybersecurity a mis en place l'US Cyber Challenge qui organise des stages d'été dédiés à la cybersécurité.
Résultats	Inconnus pour le moment
Contraintes associées	Logistique et contenus
Intérêt	Permet de susciter des vocations

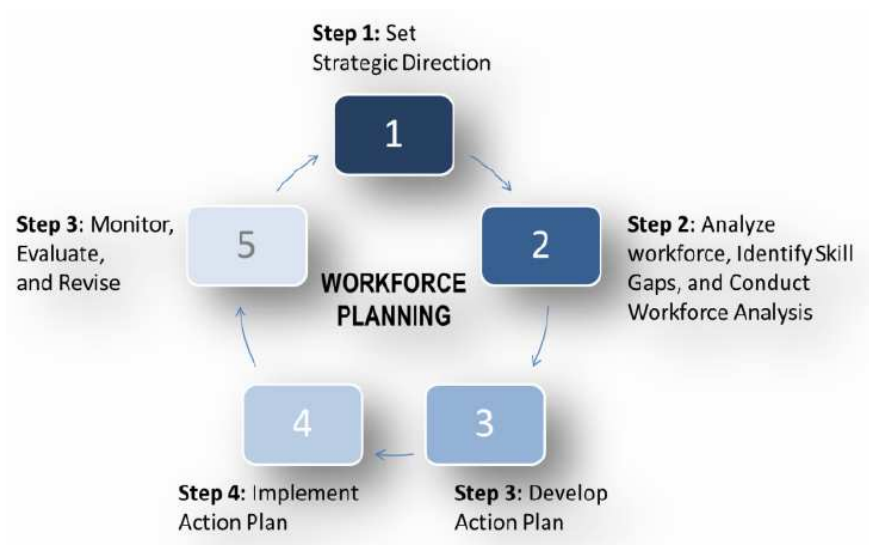
4.3. Recrutement

B10 : concevoir une méthode d'évaluation et de planification des besoins

Le DHS a travaillé, en liaison avec le secteur privé et les autres administrations fédérales, sur la définition de bonnes pratiques en matière d'évaluation et de planification des besoins dans le cadre de la troisième composante du National Initiative for Cybersecurity Education (NICE).

Cette démarche répond à un constat établi en 2011 par le Government Accounting Office (GAO) dans un rapport intitulé *Cybersecurity Human Capital*⁶⁸ : les agences fédérales ont des difficultés à évaluer leurs besoins et à déterminer la taille des équipes nécessaires. La main d'œuvre « cyber » doit par ailleurs être flexible et « agile » pour s'adapter très rapidement aux nouvelles menaces et aux évolutions technologiques, ce qui suppose une forte réactivité.

Figure 19 : les étapes de la planification des effectifs « cyber » proposée par le NICE⁶⁹



⁶⁸ <http://www.gao.gov/new.items/d128.pdf>

⁶⁹ http://niccs.us-cert.gov/sites/default/files/publications/documents/Best%20Practices%20for%20Planning%20a%20Cybersecurity%20Workforce_05312012_v4.1_DRAFT_NICE%20branded.pdf

Intitulé		Utilisation d'une méthode d'évaluation et de planification des besoins
Descriptif	Le NICE a mis en place une méthode d'évaluation et de planification des besoins de main d'œuvre « cyber ».	
Résultats	Le kit ne semble pas finalisé pour le moment. Les documents disponibles se contentent de partager quelques bonnes pratiques et se révèlent assez conceptuels.	
Contraintes associées	Aucune	
Intérêt	Fournir un kit méthodologique complet à des organisations publiques et privés	

B11 : développer un modèle de maturité

Un « Capability Maturity Model » a été développé dans le cadre du NICE pour permettre aux organisations d'évaluer leur maturité en cybersécurité, de se comparer entre elles et de définir leurs besoins en compétences. Trois critères sont utilisés pour l'évaluation : les processus et mécanismes de confrontation entre offre et demande en cybersécurité, la gouvernance, les praticiens et les technologies utilisées. Trois niveaux de maturité ont ensuite été définis : maturité limitée, en progression, optimisé.

Intitulé		Développement d'un modèle de maturité
Descriptif	Le « Capability Maturity Model » développé par le NICE permet aux organisations d'évaluer leur maturité en cybersécurité, de se comparer entre elles et de définir leurs besoins en compétences.	

Résultats	Le kit ne semble pas finalisé pour le moment. Les documents disponibles se contentent de partager quelques bonnes pratiques et se révèlent assez conceptuels.
Contraintes associées	Aucune
Intérêt	Ce kit méthodologique permet de systématiser la démarche.

Figure 20 : le modèle de maturité proposé par le NICE⁷⁰

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Process	<p>An organization has a limited workforce planning capability in the area of Process if they have evidence of the following:</p> <ul style="list-style-type: none"> Workforce planning efforts have only occurred at a sub-organization level Results of these efforts have informed decisions for each sub-organization, which may or may not have been communicated up to the corporate level Performance against these efforts have not been formally assessed 	<p>An organization has a progressing workforce planning capability in the area of Process if they have evidence of the following:</p> <ul style="list-style-type: none"> Workforce planning efforts have been conducted organization-wide for a specific assessment requirement or major change in mission or budget drill Previous, org-wide efforts have been driven at the corporate level through data calls to the lines of business Results of these efforts have informed point-in-time decisions regarding human capital programs or a strategic human capital planning effort Performance against the efforts were not formally assessed 	<p>An organization has an optimized workforce planning capability in the area of Process if they have evidence of the following:</p> <ul style="list-style-type: none"> Established process for conducting organization-wide workforce planning tied to annual budget and business planning processes Process is driven at the corporate level, but fully implemented within each line of business Results of the process are utilized to drive changes in organization-wide human capital programs and investments Performance against the process is assessed on an ongoing basis, and continuous improvements are made
Analytics	<p>An organization has a limited workforce planning capability in the area of Analytics if they have evidence of the following:</p> <ul style="list-style-type: none"> Supply & demand data are only available through ad hoc data calls The data must be manually processed and manipulated for analysis and reporting purposes Few analysis tools, models, and/or templates may exist but are insufficient to support consistent analysis 	<p>An organization has a progressing workforce planning capability in the area of Analytics if they have evidence of the following:</p> <ul style="list-style-type: none"> Supply & demand data are available from various data sources, to include data calls, but may not be complete or up-to-date This data requires compilation, manual processing, and quality reviews for use in analysis and reporting Various analysis tools, models, and/or templates may exist for supply and/or demand data, but are insufficient to support full workforce planning analysis 	<p>An organization has an optimized workforce planning capability in the area of Analytics if they have evidence of the following:</p> <ul style="list-style-type: none"> Complete supply & demand data is available from authoritative data sources This data can be easily accessed and manipulated for analysis and reporting purposes with minimal manual processing Multiple analysis tools, models, and/or templates exist for both supply & demand data, and are sufficient to support full workforce planning analysis

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Integrated Governance	<p>An organization with a limited workforce planning capability has evidence of Integrated Governance:</p> <ul style="list-style-type: none"> No established governance structure at the corporate level Limited or ad hoc corporate level workforce planning guidance that considers workforce planning implications based on changes in budget, mission priorities, and/or policy changes Decentralized decision-making at the sub-organization level 	<p>An organization with a progressing workforce planning capability has evidence of Integrated Governance:</p> <ul style="list-style-type: none"> Established governance structure that exists in either an Human Capital office, CFO Office, or Business Planning office, reaching to other entities as stakeholders in the process Documented workforce planning guidance when major change in mission, program, or policy occurs to communicate workforce planning priorities and/or constraints related to the specific change Workforce planning guidance is utilized to support planning process for a point-in-time corporate decision Results drive short term decision on point-in-time corporate decision 	<p>An organization with an optimized workforce planning capability has evidence of Integrated Governance:</p> <ul style="list-style-type: none"> Established corporate level governance structure comprised of an integrated leadership group from CFO, Human Capital, and Lines of Business Documented workforce planning guidance that incorporates implications of strategic, environmental, and policy issues to formulate workforce planning priorities and/or constraints workforce planning Guidance is utilized to drive a regular (e.g. annual), organization-wide workforce planning process Results drive both short term and long term decision making at a corporate level

⁷⁰http://niccs.us-cert.gov/sites/default/files/documents/files/NICE%20Capability%20Maturity%20Model%20white%20paper_06282013_FINAL_NICE%20branded_0.pdf

Capability Criteria	Level of Maturity		
	Limited	Progressing	Optimized
Skilled Practitioners	<p>An organization has a limited workforce planning capability in the area of Skilled Practitioners if they have evidence of the following:</p> <ul style="list-style-type: none"> • There are few personnel designated to support workforce planning-related efforts as they occur in the organization • This staff exists only at the corporate level, or in some cases, only at the sub-organization level • This staff does not actively share knowledge with others 	<p>An organization has a progressing workforce planning capability in the area of Skilled Practitioners if they have evidence of the following:</p> <ul style="list-style-type: none"> • There are a number of personnel designated to support workforce planning-related efforts as they occur the organization • This staff exists either at the corporate level and/or sub-organization level • This cadre share knowledge on an ad hoc basis as needed to support the efforts as they occur 	<p>An organization has an optimized workforce planning capability in the area of Skilled Practitioners if they have evidence of the following:</p> <ul style="list-style-type: none"> • Established cadre of skilled practitioners trained in the organization's workforce planning process and associated analytics • This cadre exists at both the corporate level and throughout the sub-organizations in sufficient numbers to support all aspects of the workforce planning process • This cadre regularly shares knowledge to promote skill building and continuous process improvement
Enabling Technology	<p>An organization has a limited workforce planning capability in the area of Enabling Technology if they have evidence of the following:</p> <ul style="list-style-type: none"> • Existing data systems and tools must be accessed by a limited pool of authorized users to pull down data and reports needed for workforce planning analysis • There is not centralization of existing tools, models, or templates for the organization's workforce planning community to access • Data that does exist must be integrated manually 	<p>An organization has a progressing workforce planning capability in the area of Enabling Technology if they have evidence of the following:</p> <ul style="list-style-type: none"> • Some data systems, tools, and models can be used by the broader workforce planning community, but several of these systems and tools still require specific technical skill to access and manipulate information • Analysis tools, models, and templates may be accessed on a shared folder or share point site, but data systems must still be accessed separately • Data from various systems and models must be integrated manually without benefit of automation 	<p>An organization has an optimized workforce planning capability in the area of Enabling Technology if they have evidence of the following:</p> <ul style="list-style-type: none"> • Authoritative data systems, analysis tools, and models are built in modern, stable applications that can be used by a wide range of practitioners, regardless of technical skill • A web portal or comparable capability exists to access the full range of data systems, analysis tools, and models used by the workforce planning community • There are automated ways to combine data from various systems to enable analysis and reduce manual processing

B12 : organiser une campagne de communication

Le Defense Signals Directorate (DSD), l'une des agences de renseignement du ministère australien de la défense, a lancé une campagne de communication pour recruter du personnel avec un slogan offensif : « *Do you want to play the game no one else can ?* »⁷¹.

Figure 21 : Publicité du DSD australien : *do you want to play the game no one else can ?*



“Our adversaries are often well resourced, highly skilled and good at concealing themselves.”

Do you want to play the game no one else can?

As the Internet expands as the global hub for business, gathering there too are the forces of cyber crime and foreign espionage.

Our adversaries are often well-resourced, highly skilled and good at concealing themselves. This threat to our cyber and information security is now a top national security priority.

Cyber operations in Defence Signals Directorate (DSD) are dedicated to ensuring our government can operate in cyber space with confidence. In DSD cyber operations, you'll be part of the Australian Government's defence against sophisticated foreign hackers.

This is your chance to be at the forefront of our country's cyber security and make a real difference.

5

Cette campagne de communication fait appel au patriotisme des candidats en jouant sur les menaces : le candidat est appelé à participer à la défense du pays contre des hackers étrangers, mettant ainsi le candidat à l'avant-poste de la défense nationale. L'attrait que peut représenter le côté prospectif et innovant du métier est également mis en avant. La valorisation des candidats est également un élément important, le DSD n'hésitant pas à qualifier ses personnels de pionniers de la cyberdéfense, transformant alors le métier en une véritable aventure, située en dehors des frontières et des règles. L'agence communique également sur les ressources mises à disposition des employés, des capacités matérielles dont ils disposent au salaire qu'ils perçoivent en passant par la qualité de vie dont ils bénéficient.

Le DSD n'hésite pas à communiquer avec des slogans utilisés jusqu'à lors par des publicitaires comme « *La vie est trop courte ! Travailler pour le DSD est un choix de style de vie et non un plan de carrière* ». L'agence n'hésite pas à communiquer sur la flexibilité et le confort dont disposent les employés dans leur travail allant même jusqu'à affirmer que travailler pour le DSD permet de mieux profiter de sa famille et de son temps libre du fait du caractère reposant de l'environnement de travail.

⁷¹ http://www.asd.gov.au/publications/Cyber_Ops_Careers_Brochure_for_Industry.pdf

Dernier aspect de cette communication, le DSD met à disposition des témoignages d'employés, qui parlent de leur métier, ce qui permet de rendre humain le recrutement et à souligner que le recrutement se fait aussi en fonction de la personnalité : « *There is no better job for a modern geek than working for a national intelligence and security agency such as DSD* ».

Figure 22 : interview d'une cyber analyste (DSD australien)

Stacey, 28, works in the fast-paced environment of the Cyber Security Operations Centre as a cyber analyst.

“ I have been working as a cyber analyst for just over a year now, and work right in the middle of the action in the Cyber Security Operations Centre. I help out government users with identifying intrusions and threats to their networks, but this is easier said than done! Given the pace of information technology, providing the right advice when there are so many different systems and users really keeps me on my toes.

My team and I work at the pointy end of information security. Cyber analysts can't be afraid to get in there and get their hands dirty to sort out complex security issues.

It is encouraging to know the work I do ensures government information remains secure. I have a background in Information Technology, and while the work is technical, I have found analytical skills are equally important in this job. ”

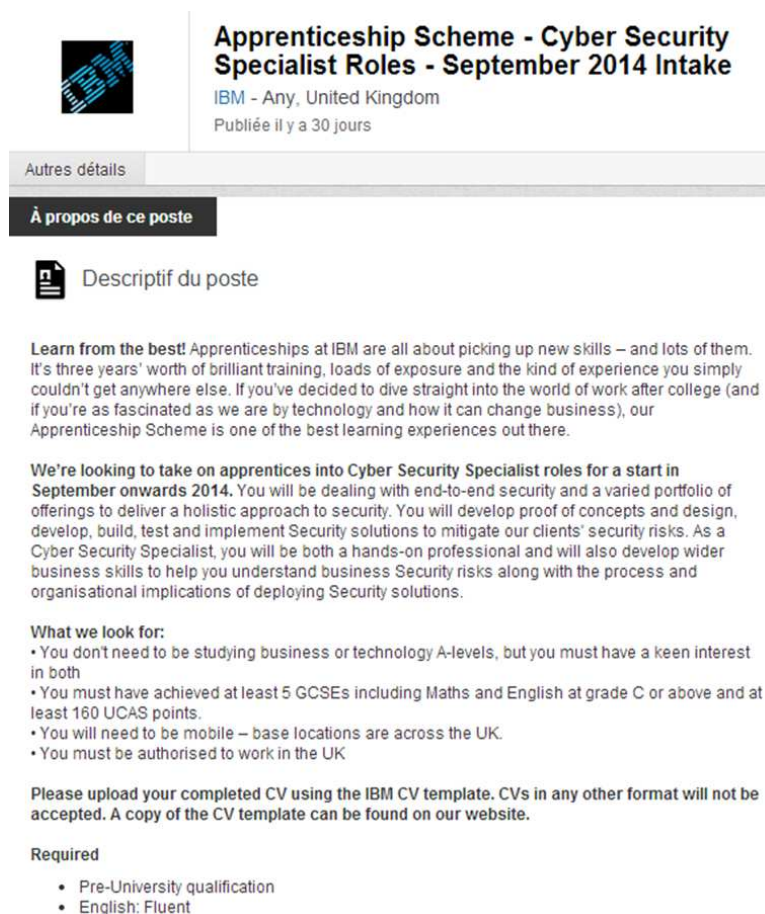
Communiquer sur les emplois « cyber » grâce à une campagne de communication offensive	
Intitulé	
Descriptif	Le Defense Signals Directorate australien a engagé une campagne offensive basée sur le slogan : <i>Do you want to play the game no one else can ?</i>
Résultats	Inconnus
Contraintes associées	Aucune
Intérêt	Campagne résolument offensive où l'on insiste sur le caractère unique de l'engagement au sein d'une agence de renseignement.

B13 : développer l'apprentissage

E-Skills UK, l'entité chargée de promouvoir les métiers de l'IT au Royaume-Uni, a lancé un programme d'apprentissage en cybersécurité en partenariat avec plusieurs acteurs industriels du domaine tels que QinetiQ, BT, IBM, Cassidian, CREST ou encore Atos.

Ce programme a été scindé en 3 parcours qui correspondent chacun à un métier : expert sécurité, pentester et architecte sécurité⁷². Avec un budget global de l'ordre de 5 millions de livres (financé à hauteur de 2 millions par la *UK Commission for Employment and Skills* et par les partenaires privés), l'objectif de cette initiative est d'atteindre entre 280 et 300 apprentis dans la cybersécurité d'ici 2015.

Figure 23 : exemple d'annonce pour un apprentissage (Grande-Bretagne)



Apprenticeship Scheme - Cyber Security Specialist Roles - September 2014 Intake
IBM - Any, United Kingdom
Publiée il y a 30 jours

Autres détails

À propos de ce poste

Descriptif du poste

Learn from the best! Apprenticeships at IBM are all about picking up new skills – and lots of them. It's three years' worth of brilliant training, loads of exposure and the kind of experience you simply couldn't get anywhere else. If you've decided to dive straight into the world of work after college (and if you're as fascinated as we are by technology and how it can change business), our Apprenticeship Scheme is one of the best learning experiences out there.

We're looking to take on apprentices into Cyber Security Specialist roles for a start in September onwards 2014. You will be dealing with end-to-end security and a varied portfolio of offerings to deliver a holistic approach to security. You will develop proof of concepts and design, develop, build, test and implement Security solutions to mitigate our clients' security risks. As a Cyber Security Specialist, you will be both a hands-on professional and will also develop wider business skills to help you understand business Security risks along with the process and organisational implications of deploying Security solutions.

What we look for:

- You don't need to be studying business or technology A-levels, but you must have a keen interest in both
- You must have achieved at least 5 GCSEs including Maths and English at grade C or above and at least 160 UCAS points.
- You will need to be mobile – base locations are across the UK.
- You must be authorised to work in the UK

Please upload your completed CV using the IBM CV template. CVs in any other format will not be accepted. A copy of the CV template can be found on our website.

Required

- Pre-University qualification
- English: Fluent

Ce programme d'apprentissage se déroule sur 2 ans. Les candidats à l'apprentissage peuvent chercher une entreprise grâce au portail *Apprenticeships Vacancies*⁷³. Les apprentissages en cybersécurité sont

⁷² <http://www.zdnet.com/uk/ibm-and-bt-to-launch-new-uk-cybersecurity-apprenticeships-7000015417/>

⁷³ <https://apprenticeshipvacancymatchingservice.lsc.gov.uk/>

classés niveaux 4 (higher level)⁷⁴ et ne sont donc accessibles qu'aux personnes diplômées de l'enseignement supérieur. La rémunération de ces contrats est comprise entre 13 000£ et 16 000£ annuelles (contre une rémunération annuelle de 9 000€ à 13 380€ pour un apprenti français⁷⁵), ce qui confère à ces offres une forte attractivité. On retrouve cette proposition à surpayer des stages ou des apprentis outre-Atlantique où le comté de Montgomery (Maryland - Etats-Unis) a publié, sur son site internet, deux offres de stages dans le secteur de la cybersécurité, rémunérés mensuellement 3 826 \$. E-Skills UK accrédi-te parallèlement des centres de formation pour les apprentis après avoir examiné le contenu des programmes. Tel a été récemment le cas pour le programme de formation proposé par le National Cyber Skills Centre qui a reçu l'accréditation *Tech Industry Gold*⁷⁶.

A noter enfin, que le GCHQ britannique a proposé pour la première fois un apprentissage⁷⁷ : l'agence offrait en effet un apprentissage à compter du mois de septembre 2014 pour une durée de deux ans. Cette offre est présentée comme une opportunité unique de travailler avec le GCHQ, le MI5 et le MI6, « *a world that you won't find on any university course - cyber threats, terrorism, espionage and organised crime* ». L'apprentissage était destiné à un profil technique pour le développement de compétences en matière de programmation, d'ingénierie réseau et télécom, de sécurité de l'information et d'opérations dans le cyberspace. Très bien rémunéré (17 000£ annuel), le candidat devait justifier d'un A Level scientifique (l'équivalent d'un baccalauréat). La première année du stage se déroule dans les locaux du GCHQ à Cheltenham et la seconde dans les locaux du MI5 et du MI6 à Londres. Au-delà du cadre, l'annonce insiste sur les aspects patriotiques du métier, « *tackle threats to national security* », ainsi que sur les moyens dernier cri mis à disposition de l'apprenti.

Intitulé		Développer l'apprentissage
Descriptif	Skills UK, l'entité chargé de promouvoir les métiers de l'IT au Royaume-Uni, a lancé un programme d'apprentissage en cybersécurité en partenariat avec le secteur privé.	
Résultats	Le programme est doté de ressources financières conséquentes et propose des apprentissages bien rémunérés.	
Contraintes	Le développement de l'apprentissage suppose un cadre juridique et financier	

⁷⁴ <http://www.apprenticeships.org.uk/~media/Collateral/BrochuresLeaflets/Apps-Framesworks-2014.ashx>

⁷⁵ <http://www.lapprenti.com/html/apprenti/salaire.asp>

⁷⁶ <http://www.e-skills.com/news-and-events/july-2014/cyber-apprenticeship-gains-tech-industry-gold-accreditation-from-employers/>

⁷⁷ <http://www.notgoingtouni.co.uk/opportunity/technical-apprenticeship-in-it-software-internet-and-telecomms-23716>

associées	incitatif pour les organisations.
Intérêt	L'apprentissage permet d'intégrer des jeunes relativement tôt dans leur cursus et de former progressivement.

B14 : développer les stages

Un programme pilote de stages « cybersécurité » a été monté par l'IAAC (Information Assurance Advisory Council) en 2013 au Royaume-Uni pour développer les stages étudiants du second ou troisième degré. Il a concerné 100 personnes, 50 universités et 50 entreprises durant l'été⁷⁸.

A noter plusieurs programmes similaires aux Etats-Unis :

- Le Student temporary experience program (STEP). Il permet au DoD d'embaucher des stagiaires ;
- Le student career experience program (SCEP). Il permet aux agences fédérales de prendre des stagiaires faisant des études dans le domaine de compétences recherché. Il s'agit souvent d'une antichambre en termes de recrutement. La DISA utilise largement le SCEP pour recruter de nouvelles compétences ;
- Le Federal Career Intern Program (FCIP). Il propose des stages de deux ans.

Ces différents programmes ont été remplacés en 2012 par le « Pathways Internship program ».

Figure 24 : exemple d'offre de stage cybersécurité sur le site e-Skills UK⁷⁹

⁷⁸<http://www.iaac.org.uk/itemfiles/20131028%20IAAC%20report%20on%20its%20cyber%20security%20intern%20pilot%20scheme.pdf>

⁷⁹<http://www.e-skills.com/professional-development/internships/cyber-security-internship-opportunities/cyber-security-internship-with-dtex-systems-uk/>

e-skills uk

News and Events Contact

About e-skills UK | Research | Education | Apprenticeships | Professional Development | Careers | Standards and Qualifications | Using IT

Home » Professional Development » Internships » Internship Opportunities » Cyber Security Internship with Dtex Systems UK

Cyber security skills

IT Professional Standards

IT Professional Profile

Learning Pathways

Wales up-skilling

Internships

STEM Internships

Cyber Security Internships

Internship Opportunities

- Junior C++ developer
- ASP.net C# programmer
- Threat Intelligence Analyst
- Security Researcher
- Graduate Java Middleware Specialist
- Software Engineer Internship with Montvieux Limited
- Software Development with Compliance Control Ltd
- Cyber Security Internship with Dtex Systems UK

Cyber Security Internship with Dtex Systems UK

- Internship duration: 2 months (negotiable)
- Start date: negotiable
- Location: London
- Contact: gu.recruitment@dtexsystems.com

COMPANY PROFILE

Dtex Systems UK is a forward-thinking, high-growth information security company focussing on Enterprise User Monitoring and User Intelligence worldwide. Dtex Systems provide security and auditing related projects for leading global organisations who want to prevent internal threats and maximise efficiency.

Find out more about the company's activities - view the following videos:

- Dtex Systems gives Security Industry view of Sony Hacks on BBC
- Mohan Koo interviewed by CNN regarding the Sega hacking breach
- Mohan Koo gets interviewed by CNN on the IMF cyber attack

INTERNSHIP DESCRIPTION

Dtex Systems are looking for a second or third year student studying towards their degree in IT/Computer Science or a related degree. The successful candidate will be interested in pursuing a career in IT/Cyber security with basic skills in Microsoft SQL, Information Security/Forensics and Networking. Candidates must be able to conduct client facing work and be eager to develop new skills. Other tasks will involve working alongside security analysts to support investigations, including evidence gathering and IT forensics analysis.

DESIRED SKILLS / EXPERIENCE

- ASP .NET/C#, Microsoft SQL Server Reporting Services (SSRS)
- Understanding of best practice security controls for standard desktop technologies (MS Windows, Anti-x and Firewalls etc).
- Basic knowledge of information security principles and encryption technologies

ELIGIBILITY REQUIREMENTS

- Preferably on a degree course in IT/Computer Science or Security related
- Must be eligible to work in the UK without any restrictions

[Back to top](#)

Twitter News Most popular

e-skillsUK @eskillsUK 29 Aug
e-skills UK Weekly News Digest is out!
paper.li/eskillsUK/1328...

Digital Birmingham 22 Aug

Intitulé	Développer les stages
Descriptif	Un programme pilote de stages « cybersécurité » a été monté par l'IAAC (Information Assurance Advisory Council) en 2013 au Royaume-Uni pour développer les stages étudiants.
Résultats	Très bons résultats
Contraintes associées	Cadre juridique adapté
Intérêt	Permet de détecter des profils intéressants très en amont.

B15 : financer des bourses d'étude

L'US Office of Personnel Management, qui a récemment été la cible d'une cyberattaque⁸⁰, a mis en place un programme de bourses, Scholarship For Service (SFS), pour attirer les étudiants vers les métiers de la protection de l'information⁸¹. Ce programme, qui bénéficie d'un budget de 12 millions de dollars par an, s'adresse à tous les étudiants qui sont déjà engagés ou qui veulent s'engager dans un parcours dont la durée d'étude sera au minimum de 4 ans et propose des bourses d'étude attribuées par la NSF (National Science Foundation). Le montant des bourses est tout à fait conséquent :

- 20 000\$ pour les étudiants sans diplôme ;
- 25 000\$ pour les étudiants déjà diplômés d'un master ;
- 30 000\$ pour les étudiants en thèse.

Pour les deux dernières catégories, la bourse a été revalorisée le 11 juillet dernier à 32 000\$ annuels⁸².

⁸⁰ <http://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office/>

⁸¹ <https://www.sfs.opm.gov/StudFAQ.aspx>

⁸² <http://www.nsf.gov/pubs/2014/nsf14586/nsf14586.pdf>

Figure 25 : répartition des étudiants bénéficiant du programme SFS par organisme

Agency	FY 2006	FY 2007	FY 2008	Total Hires
NATIONAL SECURITY AGENCY	53	31	29	113
DEFENSE	34	32	26	92
FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS (FFRDCs)*	27	25	12	64
CENTRAL INTELLIGENCE AGENCY	11	3	3	17
GOVERNMENT ACCOUNTABILITY OFFICE	10	4	3	17
FEDERAL RESERVE SYSTEM	5	5	3	13
JUSTICE	5	3	2	10
HOMELAND SECURITY	0	6	3	9
COMMERCE	3	3	2	8
TREASURY	0	2	4	6
Other Agencies*	16	29	13	58
Total placements as of 01/30/09	164	143	100	407

A cela s'ajoute par année 3 000\$ de subventions si l'étudiant souhaite passer des certifications, ce qui peut être intéressant au regard de l'importance des certifications dans le domaine de la cybersécurité, ainsi qu'un budget de 1 000\$ pour l'achat de livres. Ces bourses sont attribuées pour une durée allant d'un semestre à 5 ans. En contrepartie, l'étudiant devra travailler pour le gouvernement américain durant la même période que celle pendant laquelle il a bénéficié de ce programme. En outre, le premier emploi proposé à l'issue de la période de travail pour le gouvernement ne peut pas être refusé, sous peine de devoir rembourser la bourse versée.

Afin de pouvoir participer à ce programme, les organismes doivent demander à être certifiés. A ce jour, 22 organismes ont obtenus la certification pour participer à ce programme. Depuis sa création en 2000, ce programme a permis à 1 080 étudiants d'être diplômés, dont 80% d'un master. Le programme, qui permet de diplômer 120 étudiants par an en moyenne, devrait atteindre un objectif de 500 à 1 000 étudiants diplômés par an⁸³. Bien que le DoD, à travers la NSA, compte beaucoup d'employés issus de ce programme, beaucoup d'étudiants partent travailler dans le secteur privé en raison du manque de réactivité de l'administration (50% seulement des étudiants sont placés dans des agences gouvernementales à l'issue de leurs formations), ce qui représente une perte sèche pour l'administration en matière d'investissement.

D'autres programmes similaires ont été lancés par le DoD ou le DHS. Le DoD a par exemple lancé le programme IASP⁸⁴ (Information Assurance Scholarship program) qui propose des bourses pour des études spécialisées dans de nombreux domaines de sécurité des systèmes d'information. Ce

⁸³ http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf

⁸⁴ [http://dodcio.defense.gov/TodayinCIO/InformationAssuranceScholarshipProgram\(IASP\)/About.aspx](http://dodcio.defense.gov/TodayinCIO/InformationAssuranceScholarshipProgram(IASP)/About.aspx)

programme est ouvert aux étudiants mais aussi aux personnels actifs du DoD. Le montant des bourses est inférieur à celui proposé par le SFS, les bourses annuelles étant de 17 000\$ pour un étudiant sans diplôme et de 22 000\$ pour les étudiants déjà diplômés⁸⁵. Afin de pouvoir accueillir des étudiants bénéficiant de ce programme, les organismes de formations doivent faire partie de la liste des National Centers of Academic Excellence (CAE) établie par la NSA⁸⁶ :

Les critères de sélection sont différents selon qu'il s'agisse d'étudiants ou des personnels du DoD. Pour les étudiants, ceux-ci doivent avoir au moins 18 ans et avoir été acceptés préalablement par un des centres en question. Pour les membres du DoD, ces derniers doivent être des militaires ou des personnels civils du DoD, posséder la nationalité américaine (ce qui n'est pas une condition pour les étudiants) et doivent avoir été proposé par leur hiérarchie au regard de leurs compétences.

Le DHS a également lancé en 2013 son propre programme de bourses d'études, la Cyber Student Initiative⁸⁷, destiné à engager des étudiants particulièrement brillants dans le domaine. Il consiste à offrir des périodes de formation non rémunérées à des étudiants ou des vétérans de nationalité américaine à travers des stages pouvant aller de 4 à 18 semaines, justifiant deux années d'étude dans le supérieur. En 2013, cette initiative a bénéficié à plus d'une centaine d'étudiants.

Intitulé		Financer des bourses d'étude
Descriptif	Le programme de bourses Scholarship For Service (SFS) bénéficie d'un budget de 12 millions de dollars par an et offre des bourses à tous les étudiants déjà engagés ou qui veulent s'engager dans des études en cybersécurité.	
Résultats	Plus de 1000 étudiants diplômés depuis la création du programme en 2000.	
Contraintes associées	Il faut un cadre juridique adapté. L'administration américaine n'embauche cependant que 50% des boursiers en raison de la complexité des procédures de recrutement.	
Intérêt	Détection très en amont des profils.	

⁸⁵ [http://dodcio.defense.gov/TodayinCIO/InformationAssuranceScholarshipProgram\(IASP\)/ProspectiveScholars.aspx](http://dodcio.defense.gov/TodayinCIO/InformationAssuranceScholarshipProgram(IASP)/ProspectiveScholars.aspx)

⁸⁶ <http://www.nsa.gov/ia/index.shtml>

⁸⁷ http://www.dhs.gov/sites/default/files/publications/SHP_Cyber_Student_Initiative_Bulletin.pdf

B16 : cibler des profils atypiques

Même si ces besoins se limitent à quelques pourcents des effectifs cyber, certaines agences ou entreprises cherchent à recruter des profils dits « atypiques » en dehors des voies classiques de recrutement. Selon un récent sondage réalisé au Royaume-Uni auprès de professionnels de l'IT, près de deux tiers des personnes interrogées considèrent que le meilleur moyen d'assurer un niveau élevé de sécurité est de recruter des ex-hackers⁸⁸. Le site CWjobs.uk, spécialisé dans les métiers de l'IT, propose ainsi des offres, par ailleurs très bien rémunérées, qui font appel directement à des compétences en matière de hacking.

La Joint Cyber Reserve Unit annoncée par le Ministère de la Défense britannique en septembre dernier - qui prévoit un budget de 500 millions de livres dans le recrutement de centaines de réservistes comme experts en informatique – considère que le recrutement de hackers ayant un casier judiciaire est une opportunité⁸⁹, privilégiant le développement de leurs capacités et mettant de côté leurs traits de personnalité. Cette ambition n'est pas forcément accueillie de manière très positive par les principaux intéressés, comme en témoigne la réaction de Mustafa al-Bassam, un des plus jeunes hackers du groupe Luzlec – aujourd'hui dissous et connu notamment pour les piratages du site de la CIA et du SOCA britannique (Serious Organised Crime Agency) en 2011 – qui considère que les révélations d'Edward Snowden sur l'espionnage massif de la NSA sont un obstacle : *« je peux comprendre le besoin d'un gouvernement de se protéger mais le fait de bafouer les libertés des citoyens [...] a pour conséquence de rebuter les personnes talentueuses »*.

Le DoD américain a également lancé une campagne de recrutement à destination des hackers⁹⁰. Lors de conférences telles que la DefCon, durant lesquelles des personnels du DoD, à commencer par le général Keith Alexander⁹¹, rencontrent les participants pour leur proposer de travailler pour le gouvernement.

Mais des obstacles peuvent apparaître dans le recrutement de profils atypiques. Premier obstacle : la rigidité des grilles salariales qui s'adaptent mal à des profils souvent autodidactes. Deuxième obstacle : les habilitations de sécurité et les éventuels antécédents judiciaires. Sur ce point, le directeur du FBI, James Comey, expliquait que la loi américaine de lutte contre la drogue empêchait le bureau de recruter les meilleurs experts en sécurité, car ces derniers seraient souvent des consommateurs de marijuana⁹². La NSA examinerait cependant au cas par cas les candidatures dont les tests de dépistage

⁸⁸ <http://www.recruiter.co.uk/news/2013/09/combat-cyber-security-by-recruiting-ex-hackers/#sthash.NHPWkUmV.dpuf>

⁸⁹ <http://www.bbc.com/news/technology-24613376>

⁹⁰ http://www.huffingtonpost.com/2013/01/28/pentagon-cyber-force_n_2567564.html

⁹¹ <http://news.clearancejobs.com/2012/08/01/cybersecurity-hiring-news-nsa/>

⁹² <http://www.ibtimes.com/fbi-director-says-agencys-pot-policy-needs-reform-attract-cyber-security-professionals-1588245>

de consommation de drogue s'avèrent positifs⁹³ pour ne pas exclure d'emblée des profils potentiellement intéressants.

Intitulé		Cibler des profils atypiques
Descriptif	Agences américaines et britanniques ciblent des profils dits « atypiques » à travers des campagnes de recrutement spécifiques et la participation à des conférences spécialisées.	
Résultats	Agences et entreprises parviennent aujourd'hui à recruter ce type de profils. La question se pose en revanche des conséquences de l'affaire Snowden sur l'attractivité des postes au sein des agences de renseignement.	
Contraintes associées	Le recrutement de profils atypiques demande souvent de déroger aux règles habituellement pratiquées en matière de rémunération et de sécurité.	
Intérêt	Bénéficiaire de compétences techniques très pointues.	

B17 : organiser des compétitions informatiques

B17-1 : organiser des challenges internes

Le Service général du renseignement et de la sécurité de l'armée belge⁹⁴ a organisé en 2014 un challenge pour recruter en interne dix spécialistes en matière de cyberdéfense. L'objectif était d'identifier les candidats potentiels, civils ou militaires déjà en service grâce à un *capture the flag*⁹⁵. Pour y participer, les membres du personnel de la Défense doivent s'inscrire sur un site. Après s'être connectés, ils reçoivent des questions présentées en huit catégories concernant la sécurité de réseaux informatiques. L'objectif est surtout de détecter des potentiels, pas de tester des connaissances. Aux Etats-Unis, le DoD a lancé également pour la première fois cette année un challenge entre les différentes académies militaires de tout le pays, le *Cyber Stakes*⁹⁶. Cet événement, co-organisé par la DARPA, les universités Carnegie Mellon et de New York, a réuni près de 50 aspirants issus des trois

⁹³ <http://www.bbc.com/news/technology-27499595>

⁹⁴ http://www.lavenir.net/article/detail.aspx?articleid=DMF20140205_00428689

⁹⁵ Le CTF est un jeu par équipe, traditionnellement joué en plein air, où l'objectif est de capturer le drapeau (ou un autre objet) de l'équipe adverse, localisé dans leur « base », et de le ramener dans son « camp ».

⁹⁶ <http://www.afcea.org/content/?q=node/12300>

armes (US Army, US Air Force et US Navy)⁹⁷. Plusieurs épreuves ont été organisées pour chacune des équipes :

- Défendre un réseau informatique dont elle avait la charge
- Rechercher et exploiter les vulnérabilités d'un code
- Cracker une liste de 100 mots de passe à l'aide d'outils automatisés

A noter qu'en France, quelques sociétés comme Airbus cybersecurity organisent également des challenges internes.

Intitulé Organiser un challenge interne	
Descriptif	Le Service général du renseignement et de la sécurité de l'armée belge a organisé en 2014 un challenge informatique interne pour détecter des potentiels en matière de cyberdéfense.
Résultats	Inconnus
Contraintes associées	La préparation des épreuves peut demander beaucoup de ressources et de temps.
Intérêt	Le recrutement interne présente de nombreux avantages : fidélisation des effectifs grâce à des parcours diversifiés et de la formation continue, habilitations souvent déjà obtenues etc.

B17-2 : organiser des challenges externes

Steria a organisé en 2014 la deuxième édition de son concours de hacking éthique inter-écoles réservé aux étudiants spécialisés en sécurité informatique⁹⁸. Durant toute une nuit, 170 étudiants réunis en équipes, ont participé à un challenge de type CTF qui comprenait plusieurs épreuves : cryptographie, cracking, forensic, stéganographie et web⁹⁹. Sept écoles d'ingénieurs et d'informatique sont partenaires de cet évènement : Epita, Epitech, EISTI, In'Techinfo, ESIEA, Telecom Sud Paris et EFREI.

⁹⁷ <http://www.defense.gov/news/newsarticle.aspx?id=121670>

⁹⁸ <http://www.steria.com/fr/carrieres/etudiants-et-jeunes-diplomes/steria-hacking-challenge/ledition-2013/>

⁹⁹ <http://www.steria.com/fr/carrieres/etudiants-et-jeunes-diplomes/steria-hacking-challenge/>

L'objectif de l'opération est à la fois de communiquer sur sa marque d'employeur potentiel auprès des étudiants et de repérer les meilleurs jeunes talents.¹⁰⁰

Symantec, en partenariat avec le DoD et la NSA organise le même genre de challenge pour recruter¹⁰¹. Plusieurs universités américaines organisent et participent également régulièrement à des challenges, à l'image de l'Université de l'Illinois¹⁰². Le gouvernement américain, avec le tournoi CyberPatriot¹⁰³, réunit enfin 26 équipes d'universités américaines et repère les profils prometteurs.

A noter enfin que lors du FIC 2014, deux challenges ont été organisés en partenariat avec EPITA et l'association ACISSI. Un étudiant a remporté les deux parcours et s'est d'ailleurs vu proposer à l'issue de l'événement une dizaine d'offres de collaboration par des entreprises présentes sur le salon.

Pour les recruteurs, qu'ils soient publics ou privés, les challenges sont clairement un moyen très efficace pour repérer les profils correspondants à leurs besoins : cela permet de réunir sur un temps très court un maximum de candidats potentiels et de les éprouver sur des critères que le recruteur aura lui-même défini.

Figure 26 : le challenge FIC



Intitulé	
Organiser un challenge externe privé	
Descriptif	Steria a organisé en 2014 la deuxième édition de son concours de hacking éthique inter-écoles qui a réuni 170 étudiants spécialisés en sécurité informatique.

¹⁰⁰ <http://business.lesechos.fr/directions-numeriques/0203405346337-steria-repere-les-as-de-la-cybersecurite-61868.php>

¹⁰¹ <http://fcw.com/articles/2014/04/10/symantec-simulation-could-be-a-recruiting-tool.aspx>

¹⁰² <http://southtownstar.suntimes.com/news/26500487-418/future-cyber-warriors-put-through-paces-at-moraine.html#.U7amWrHzG8c>

¹⁰³ <http://www.tweaktown.com/news/35473/us-government-wants-to-inspire-cyber-defense-technologies/index.html>

Résultats	Excellents résultats
Contraintes associées	Organisation relativement lourde au plan logistique et technique. Le travail de préparation d'un challenge de ce type peut être évalué à environ 200 jours-homme.
Intérêt	Intéressant à la fois en termes de recrutement mais également de communication

B17-3 : organiser un challenge national public-privé

Le Cyber Security Challenge UK est composé de plusieurs compétitions de cybersécurité organisées à travers tout le pays. Il propose également des actions de formation et d'orientation professionnelle¹⁰⁴.

Point notable : le challenge est ouvert aux résidents européens demeurant en Grande-Bretagne.

Quatre objectifs sont formellement identifiés :

- Détecter les talents ;
- Susciter les vocations et renseigner sur les carrières en cybersécurité ;
- Informer sur les formations et les entraînements à la sécurité ;
- Valoriser les métiers de la cybersécurité par rapport aux autres secteurs.

La gouvernance du programme rassemble aussi bien des acteurs publics que privé. On retrouve ainsi parmi les sponsors de cette initiative le Cabinet Office, le GCHQ, la NCA, la Banque d'Angleterre, BT, Northrop Grumman, Airbus, PwC, QinetiQ, Raytheon, Sophos, mais aussi des instituts de formation. La participation de ces sponsors est financière mais également matérielle : organisation des compétitions, réalisation de *pen-tests* sur le site du Cyber Security Challenge UK, hébergement de contenus, fourniture de main d'œuvre pour la préparation d'évènements, etc. Ce mode de sponsoring participatif est très intéressant, tant pour les partenaires qui pourront par la suite réutiliser en interne les exercices qu'ils ont préparés, que pour les organisateurs qui bénéficient d'épreuves variées et gratuites en termes de conception.

La principale activité du programme est l'organisation des compétitions tout au long de l'année. Plusieurs types d'épreuves sont possibles : Forensics, Penetration Testing, Défense, Analyse, Continuité d'activité ou Capture the Flag. D'un point de vue pratique, le challenge se déroule en plusieurs étapes. Une première sélection a lieu en ligne pour identifier les candidats qui iront au deuxième tour. Une seconde sélection a lieu au cours de *Face to Face (F2F)*, constituée des épreuves créées par les partenaires. Les F2F se déroulent le week-end et les organisateurs se proposent de payer

¹⁰⁴ <http://cybersecuritychallenge.org.uk/about-us/>

le déplacement et l'hébergement des candidats. A l'issue de cette étape, les candidats se voient proposer de faire partie d'un groupe d'anciens participants au Cyber Security Challenge UK. L'étape ultime, pour les 42 meilleurs candidats se déroule une fois par an : la Masterclass. A l'issue de cette étape, les candidats se voient tous récompensés par les partenaires qui leur proposent notamment un stage ou un emploi. Le site met en avant le cas de Dan Summers¹⁰⁵ qui a remporté le Cyber Security Challenge UK en 2011 : initialement postier, le challenge lui a ouvert les portes de la direction sécurité du Royal Mail Group. Le challenge se présente donc comme un vrai catalyseur de talents et un tremplin pour l'emploi dans la cybersécurité¹⁰⁶ à la croisée du secteur public, de l'industrie et de l'enseignement supérieur.

Le Cyber Security Challenge UK se traduit aussi par des CyberDay qui se déroulent au niveau régional, au cours desquels les candidats peuvent rencontrer les partenaires du programme et assister à des ateliers.



Outre un volet éducation et sensibilisation destiné aux élèves du secondaire, le programme propose enfin des camps de formation sur 3 jours chaque été, le dernier ayant eu lieu à la fin du mois d'août 2014 à la Defence Academy¹⁰⁷. Ces camps s'adressent aux adultes qui ont déjà quelques notions et compétences en cybersécurité. Là encore, les organisateurs prennent en charges l'ensemble des frais afférents.

Intitulé	
Organiser un challenge national public-privé	
Descriptif	Le Cyber Security Challenge UK est composé de plusieurs compétitions de cybersécurité qui ont lieu toute l'année.
Résultats	Excellents résultats

¹⁰⁵ <http://www.itpro.co.uk/631663/postman-crowned-first-uk-cyber-security-champion>

¹⁰⁶ <http://blog.backup-technology.com/13894/cyber-security-challenge-uk-searching-best-hackers-uk/>

¹⁰⁷ <http://cybersecuritychallenge.org.uk/education/cyber-camps/>

Contraintes associées	Organisation relativement lourde. Gouvernance public-privé à animer. Remboursement de tous les frais pour les participants.
Intérêt	Cette initiative offre l'avantage de mutualiser les efforts pour la création d'une compétition nationale de grande envergure. L'organisation de compétitions informatiques est en effet relativement lourde, notamment en termes de préparation technique.

B18 : développer une stratégie de relations privilégiées avec les écoles spécialisées

La société de services informatiques STERIA a développé une stratégie de relations privilégiée avec plus de 70 écoles, qu'il s'agisse d'écoles d'ingénieurs ou d'écoles de commerce¹⁰⁸. Les écoles ciblées doivent répondre aux besoins de l'entreprise, notamment dans des domaines très spécifiques, mais aussi également couvrir tous les territoires. 12 écoles ont été ciblées en 2014 comme partenaires privilégiés : EFREI, EPITA, ECE, EPSI Lyon, Telecom Sud Paris, ESIEA, ESIEE, ENSEEIHT, EPSI Nantes, MIAGE : Orsay, Sorbonne et Dauphine. A noter que les universités sont également ciblées pour pallier la pénurie des ressources en matière d'ingénieurs.

Les relations avec les écoles se traduisent ensuite par différents types d'engagements :

- Un engagement pédagogique : l'entreprise assure des conférences généralistes (métiers de l'informatique, construction du projet professionnel, témoignages d'anciens des écoles, etc.) et conférences thématiques sur des sujets innovants (Green IT, Sécurité des SI, Cloud Computing, SIG, etc.) ;
- Un engagement sociétal via des bourses de la Fondation de l'entreprise, l'immersion dans le monde de l'entreprise de lycéens issus de milieux défavorisés, etc. ;
- Un engagement en matière de recrutement : participation à des forums écoles, à des sessions de recrutement, organisations de manifestations spécifiques par l'entreprise (Jeun'Di, Steria Hacking Challenge, etc.) ;
- Un engagement Institutionnel : participation à des jurys d'admission, de soutenance de stage et de projets, à des tables rondes, etc. ;
- Un engagement financier : soutien des écoles par le versement de la taxe d'apprentissage et sponsoring

¹⁰⁸ Sources : entretiens avec Steria.

Intitulé	Développer une stratégie de relations privilégiées avec les écoles spécialisées
Descriptif	La société de services informatiques STERIA a développé une stratégie de relations privilégiée avec plus de 70 écoles, qu'il s'agisse d'écoles d'ingénieurs ou d'écoles de commerce.
Résultats	Excellents
Contraintes associées	Suppose une forte implication du service RH et la mobilisation des opérationnels, par exemple pour assurer des cours
Intérêt	Détection très en amont des profils. Très efficace en termes de communication « corporate ».

B19 : participer à des événements spécialisés

Dès 2013, et malgré l'affaire Snowden et les scandales provoqués par les écoutes réalisées par la NSA, l'Agence n'a pas hésité à participer en tant qu'exposant à la conférence RSA aux Etats-Unis à l'instar du FBI à la DefCon de Las Vegas – conférence à laquelle elle avait déjà participé. La présence à cet événement avait pour principal objectif de communiquer sur les offres de recrutement de l'agence.

Figure 27 : stands de la NSA à la RSA 2014 et à la Defcon 2012



Certaines entreprises privées participent aussi à des conférences de hacking. OVH était ainsi présent comme sponsor de la onzième Nuit du Hack¹⁰⁹, un évènement qui rassemble sur deux jours des amateurs et des professionnels de la sécurité autour d'ateliers, de conférences et de concours. Henri Roussez¹¹⁰, à l'initiative du projet chez OVH, considère que « *L'état d'esprit de la Nuit du Hack correspond aux profils que nous recherchons, parce que le hacking c'est avant tout une ouverture d'esprit sur la technologie. Un hacker se caractérise essentiellement par son immense curiosité [...] Une édition de la Nuit du Hack est donc, en quelque sorte, un rassemblement massif de candidats potentiels* ».

Au-delà d'un simple stand lors de cet évènement, l'hébergeur en a d'ailleurs profité pour organiser son propre challenge, l'OVHack Contest, et soutenir ses campagnes de recrutement : « *L'objectif final étant de faire connaître nos offres et de repérer des profils intéressants, nous avons cherché à stimuler les participants [...] La communication de recrutement était principalement axée sur les postes du support client avec, à l'appui, toute une campagne sur Twitter et des affiches « Support Héros ». Bien sûr, nous recherchons des talents, mais aussi un état d'esprit, une culture* ».

A noter que l'ANSSI a également participé pour la première fois à la Nuit du Hack 2014 et a pu communiquer sur ses offres. L'agence française a ainsi collecté de nombreux CV, dont des profils qu'elle ne collecte pas par la voie de recrutement classique, son site internet.

Intitulé	Participer à des événements spécialisés
Descriptif	La NSA et la CIA participent directement aux manifestations spécialisées sur la cybersécurité, qu'il s'agisse de manifestations commerciales comme la RSA ou de conférences de hacking comme la Defcon.
Résultats	Excellents
Contraintes associées	Contrats de partenariat avec les organisateurs des événements

¹⁰⁹ <http://www.nuitduhack.com/>

¹¹⁰ http://www.ovh.com/fr/al133.ovhcom_a_la_nuit_du_hack_objectif_recrutement

Intérêt	La participation à ces manifestations est indispensable pour recruter des profils spécialisés. Elle est en outre intéressante en termes de veille technologique et commerciale.
---------	---

B20 : adopter des procédures de recrutement flexibles

Les règles de recrutement sont souvent trop rigides pour permettre aux agences et grandes entreprises de recruter des profils compétents dans un contexte de fortes tensions sur le marché de l'emploi cyber, ce qui les conduit d'ailleurs souvent à externaliser avec les risques que cela comporte. Edward Snowden, sous-traitant de la NSA sans réel diplôme ni longue expérience professionnelle était ainsi rémunéré plus de 100 000 \$ par an.

Pour corriger cette faiblesse, le DoD a assoupli les procédures de recrutement applicables au sein du US Cyber Command en lui donnant la capacité de recruter du personnel civil, voire de recruter directement dans les autres administrations fédérales en remboursant les bourses allouées s'il s'agit d'étudiants boursiers. Pour les capacités de renseignement dans le domaine cyber, les administrations compétentes peuvent enfin utiliser certaines dispositions du Defense Civilian Personnel System pour offrir aux candidats des conditions incitatives permettant de rendre les offres compétitives.

Au plan salarial, la NSA applique enfin une grille spéciale de salaires pour les niveaux GS-5 à GS-12, plaçant ces rémunérations de 24 à 44 % au-dessus du salaire de base pour certaines catégories d'emplois comme les *computer scientists*, *information technology specialists* ou ingénieurs. Ces rémunérations attractives n'enlèvent cependant rien à la lourdeur du processus de recrutement et d'habilitation, souligne néanmoins la RAND.¹¹¹

Intitulé	
Adopter des procédures de recrutement flexibles	
Descriptif	Le DoD a assoupli les procédures de recrutement applicables au sein du US Cyber Command.
Résultats	Inconnus

¹¹¹ http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

Contraintes associées	Suppose une adaptation du cadre RH standard
Intérêt	Permet de recruter plus efficacement dans un contexte de fortes tensions sur le marché de l'emploi cyber. Permet aussi de recruter des profils atypiques.

B21 : adopter un système de cooptation

La société Steria a adopté un système de cooptation permettant d'inciter les salariés à recommander l'une de leurs relations. En cas d'embauche, le salarié touche 1 000 € de prime, celle-ci étant portée à 2 000 pour un recrutement dans le domaine cybersécurité. Thales a également mis en place en 2011 un programme de cooptation incitatif poussant les salariés internes à faire jouer leurs réseaux pour amener des candidats.

A noter que cette forme de recrutement, également appelé « crowd recruiting » se développe tant en interne qu'en externe avec des agences spécialisées¹¹². Le principe est de faire appel à un réseau de coopteurs qui vous flèchent des profils a priori pertinents. Cette démarche est intéressante en termes de sourcing car cela permet de diffuser des offres sur des publics déjà ciblés (« réseaux gris ») même si cela n'évite pas un travail de sélection ultérieur. Ce mode de recrutement est actuellement très utilisé car basé sur le développement des réseaux sociaux et l'intérêt économique pour l'entreprise qui paie moins cher que si elle recourait aux services d'un chasseur de tête traditionnel.

Intitulé		Adopter un système de cooptation
Descriptif	Steria incite les salariés à faire jouer leurs relations pour amener des candidats potentiels. Une prime de 2 000 € est versée au salarié en cas d'embauche.	
Résultats	Très bons résultats	
Contraintes associées	Aucune	

¹¹² Exemples : <https://www.keycoopt.com/>, <http://www.myjobcompany.com/>

Intérêt	Permet de motiver les salariés et de limiter le coût d'un recrutement
---------	---

4.4. **Gestion des carrières**

B22 : créer un référentiel des métiers et des compétences

Le préalable de toute démarche de recrutement et d'entraînement reste la cartographie et l'audit de ses propres besoins. Un référentiel tant des métiers que des compétences requises a vocation à guider la mission de GRH du recrutement à la gestion de carrières. De nombreuses initiatives de référentiels peuvent être identifiées, et constituent à cet égard des illustrations de cette bonne pratique.

- **Le premier pas de l'ONISEP**

L'ONISEP, référence en matière d'orientation professionnelle des jeunes en cours de scolarité, ne propose qu'une seule fiche métier sur le sujet, celle de l'expert en sécurité informatique¹¹³. Cet expert revêtira plusieurs casquettes selon la fiche : en SSII, il sera « expert » ou « consultant » ; en interne en entreprise, il pourra être RSSI. L'ONISEP précise que le profil de l'expert en sécurité informatique peut être complété par certains titres : « *certificat international d'auditeur des systèmes d'information (CISA) ; certified information system security professional (CISSP) ; titre d'auditeur interne certifié (AIC)* ».

Enfin, la pluridisciplinarité propre à la cybersécurité semble être globalement éludée au profit d'une perception très technique du métier. Si la question de la connaissance des normes est abordée dans certaines fiches de poste, l'intervention d'un juriste spécialisé en droit des nouvelles technologies n'est pas, ou peu prévue par les référentiels actuels [uniquement par l'APEC qui lui consacre une fiche métier¹¹⁴ et qui le désigne comme interlocuteur privilégié (relation fonctionnelle) du RSSI].

L'APEC consacre dans son référentiel des « métiers de l'Internet » une fiche au métier de RSSI, et elle reconnaît la montée en puissance des enjeux relatifs à la sécurité informatique. Elle voyait déjà juste en 2005¹¹⁵ en prévoyant « *pour les années à venir des besoins importants dans tous les métiers touchant à la sécurité des systèmes d'information ainsi qu'à l'optimisation et à l'administration des réseaux* », admettant ainsi implicitement l'existence d'une pluralité de métiers relatifs à la sécurité informatique. Elle fait un pas en avant en consacrant une fiche métier à la fonction d'« Ingénieur sécurité web » et de « Juriste spécialisé en droit de l'Internet » ; ainsi qu'en reconnaissant l'existence et la montée en puissance des spécialistes de l'authentification, de l'intrusion, ou encore du chiffrement.

- **Le référentiel de compétences européen (European e-competence framework - e-CF)**



¹¹³ <http://www.onisep.fr/Ressources/Univers-Metier/Metiers/expert-e-en-securite-informatique>

¹¹⁴ Fiche métier du juriste spécialisé en droit de l'Internet <http://annuaire-metiers.cadres.apec.fr/metier/internet--multimedia/juriste-specialise-droit-de-l-internet> - et référentiel 2012 (PDF) :

<http://cadres.apec.fr/Emploi/content/download/442157/977227/version/1/file/R%C3%A9f+m%C3%A9tiers+Internet.pdf>

¹¹⁵ Communiqué de presse : <http://presse.apec.fr/Presse/Communiqués-de-l-Apec/Les-Referentiels/Le-nouveau-referentiel-Apec-des-metiers-de-l-Internet-vient-de-paraitre> et Référentiel (PDF) :

<http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CGgQFjAF&url=http%3A%2F%2Fpresse.apec.fr%2FPresse%2Fcontent%2Fdownload%2F35851%2F132406%2Fversion%2F1%2Ffile%2F17902-eeaaa5dt0j4.pdf&ei=F4m8UJbAEMnDswal7YAY&usq=AFQjCNEGaiqXYwzB15Bx73pudIfdCJcCyg&sig2=QABDVSSZ1K001EISCHMXcw&cad=rja>

Le CIGREF¹¹⁶, qui a mis à jour sa nomenclature Ressources Humaines en juin 2011, propose « *une description de métiers existants dans les Directions des Systèmes d'Information (DSI), des grandes entreprises* ». Cette mise à jour s'est réalisée, à l'échelle de la Commission européenne, dans le cadre des travaux de la structure « ICT-Skills Workshop » qui a décidé en 2005 de créer un Référentiel de compétences européen¹¹⁷ (European e-competence framework - e-CF)¹¹⁸.

Ce référentiel¹¹⁹ présente la sécurité informatique à la fois comme un métier à part entière et comme une compétence transverse. Cette perception duale de la sécurité informatique se retrouve dans le référentiel de la FIAFEC¹²⁰ sur les métiers de l'informatique et dans le Référentiel métier des Technologies de l'Information et de la Communication de l'Université Lyon 1¹²¹.

Le référentiel des compétences européen distingue les 7 grandes familles suivantes :

- Pilotage, organisation et gestion des évolutions du système d'information
- Management de projet
- Cycle de vie des applications
- Mise à disposition et maintenance en condition opérationnelle des infrastructures
- Support et assistance aux utilisateurs
- Support méthode, qualité et sécurité
- Management opérationnel

Ce référentiel classe les métiers relatifs à la sécurité informatique en catégorie n°6 intitulée « *support méthode, qualité et sécurité* » ; catégorie regroupant « *les métiers liés à la définition, la mise en place, le contrôle et suivi (audit) des normes et référentiels qualité, méthode et sécurité* ». Le métier de RSSI peut également être recoupé avec celui de « Responsable d'entité » présenté en catégorie n°7, portant sur le « *management opérationnel* » et rassemblant des métiers « *à responsabilité hiérarchique* ».

Ainsi, si ce référentiel semble complet au sujet des métiers des systèmes d'information en entreprise, il ne présente pas de liste de métiers ou de compétences propres aux métiers de la cybersécurité.

- **L'approche intégrée du NIST**

Fin 2011, le National Initiative for Cybersecurity Education (NICE) publiait un référentiel des métiers de la cybersécurité¹²². A travers ce référentiel, le NICE a souhaité apporter des définitions et un vocabulaire communs en matière de cybersécurité. Cette classification est destinée à être applicable en tout ou partie à toute entreprise ou administration. Le NICE identifie des « zones de spécialité » au sein desquelles on retrouve des métiers divers et variés. Ces zones de spécialité expriment un besoin ; chacun de ces besoins constituant le maillon d'une chaîne plus globale, permettant une approche

¹¹⁶ http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/2011_Metiers_des_SI_dans_Grandes_entreprises_Nomenclature_RH_CIGREF_FR.pdf

¹¹⁷ Référentiel européen des compétences informatiques, version 2.0 (PDF) - http://www.ecompetences.eu/site/objects/download/6068_EUeCF2.0CWAPartIFR.pdf

¹¹⁸ <http://www.ecompetences.eu/>

¹¹⁹ http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/2011_Metiers_des_SI_dans_Grandes_entreprises_Nomenclature_RH_CIGREF_FR.pdf

¹²⁰ Organisme Paritaire Collecteur Agréé, par l'Etat, des entreprises de la Branche de l'informatique, de l'ingénierie, du conseil, des études, des foires, salons, congrès, et des traductions.

¹²¹ http://pmb-soie.univ-lyon1.fr/opac_css/doc_num.php?explnum_id=188

¹²² <http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-Summary-Booklet.pdf>

exhaustive de la menace « cyber ». Les métiers associés viennent ainsi répondre de façon cohérente à un besoin exprimé dans un but précis, à un stade défini de la menace (en amont, pendant, en aval, ou en support). Le NICE opte ainsi pour une segmentation fonctionnelle et opérationnelle des métiers de la cybersécurité¹²³, partant de l'anticipation en amont de la menace, à la gestion et l'analyse en aval.

- Securely Provision
- Operate and Maintain
- Protect and Defend
- Investigate
- Collect and Operate
- Analyze
- Oversight and Development

Le NICE propose de référencer au sein de sept catégories plus de 30 spécialités. Chaque zone de spécialité étant elle-même décomposée en tâches auxquelles sont associées des compétences.

Echantillon des compétences référencées par le NICE :

- Sécurité réseau
- Sécurité des données
- Normes de sécurité
- Architecture de l'entreprise
- Sensibilité aux NTIC
- Sensibilité à la sécurité
- Législation
- Sécurité des infrastructures
- Management du risque
- Gestion des incidents
- Gestion des vulnérabilités
- Informatique embarquée
- Audit du SI
- Langages informatiques
- Sécurité du personnel
- OS
- Technologies Web
- Management de l'identité
- Qualité
- Développement logiciel
- Facteurs humains
- Télécommunications
- Intégration système
- Raisonnement mathématique
- Chiffrement
- Gestion de BDD
- Design d'infrastructures

¹²³ http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_interactive_how_to.pdf

Pour plus de développements, cf. supra.

Dans leur étude intitulée « Survey of Cyber Security Frameworks »¹²⁴, les auteurs émettent quelques critiques à l'égard du référentiel du NICE. Selon eux, le NICE ne tiendrait pas compte du caractère évolutif des menaces. Il devrait ainsi être accompagné de recommandations quant à la mise à jour régulière des contenus. Enfin, le *framework* éluderait les coûts nécessaires à sa mise en œuvre par les différents organismes.

- **La bibliothèque du CNSS**¹²⁵

Le Committee on national security system propose une librairie de guides d'entraînement à destination de professionnels de la sécurité. Ces professionnels ciblés sont :

- Senior Systems Managers
- System Administrators (SA)
- Information Systems Security Officers
- Risk Analysts
- Systems Certifiers

- **Le Department of Homeland Security et le référentiel « IT Security Essential Body of Knowledge » (EBK)**

La National Cyber Security Division, division de l'Office of Cyber Security & Communications du Department of Homeland Security, a développé l'IT Security Essential Body of Knowledge. Ce référentiel des compétences et fonctions nécessaires au recrutement des effectifs en matière de sécurité de l'information a pour ambition d'être le document référence liant les visions du secteur public et du secteur privé et proposant une terminologie commune aux deux secteurs. Cette initiative est complémentaire de celles du NIST et du CNSS.

Ce référentiel¹²⁶ distingue 10 métiers selon le rôle et le statut occupé : les fonctions peuvent être exécutives (Chief Information Officer, Information Security Officer, IT Security Compliance Officer), axées « métier » (Digital Forensics Professional, IT Security Engineer, IT Security Operations and Maintenance Professional, IT Security Professional) ou être des fonctions annexes aux métiers (Physical Security Professional, Privacy Professional, Procurement Professional). Ces classifications sont plus statutaires que fonctionnelles. Il faut toutefois signaler que le référentiel EBK distingue, au sein de sa catégorie axée « métiers », des rôles plus fonctionnels et opérationnels.

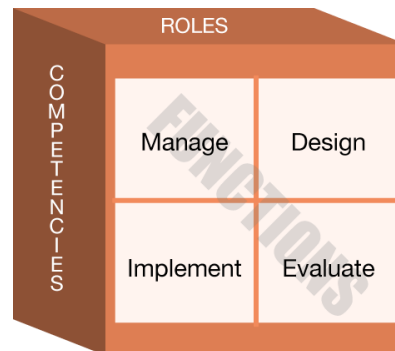
Le référentiel EBK recense 14 zones de compétences clés. Chaque zone de compétence présente plusieurs niveaux d'assimilation : *manage*, *design*, *implement* ou *evaluate*. Ces zones de compétences sont réparties sur tous les métiers, chaque métier devant les maîtriser à des niveaux différents.

¹²⁴ <http://www.ijtcse.com/second%20issue/SURVEY%20OF%20CYBER%20SECURITY%20FRAMEWORK%20S.pdf>

¹²⁵ <https://www.cnss.gov/CNSS/searchForm.cfm>

¹²⁶ http://www.beam-itsec.com/DHS_EBK2007.pdf et <http://www.us-cert.gov/ITSecurityEBK>

Figure 28. Les niveaux d'assimilation des compétences selon EBK



- La sécurité des données
- L'inforensique
- La continuité d'activité
- La gestion des incidents
- L'entraînement et la sensibilisation
- La gouvernance et la maintenance du SI
- Sécurité des réseaux et télécommunications
- La sécurité du personnel
- La sécurité physique et environnementale
- Maîtrise des procédures
- Conformité légale et normative
- Management des risques
- Management de la sécurité (niveau stratégique)
- La sécurité des systèmes et des applications

Chaque zone de compétence présente des mots-clés associés. Chaque zone de compétence est accompagnée du détail des sous-compétences correspondantes, par niveau d'acquisition (*design*, *implement*, *evaluate*, etc.).

Figure 29. Exemple de fiche compétence selon EBK

IT Security EBK: Regulatory and Standards Compliance

Refers to the application of the principles, policies, and procedures that enable an enterprise to meet applicable information security laws, regulations, standards, and policies to satisfy statutory requirements, perform industry-wide best practices, and achieve its information security program goals.

Key Terms and Concepts:

- Assessment
- Auditing
- Certification
- Compliance
- Ethics
- Evaluation
- Governance
- Laws
- Policy
- Privacy Principles/Fair Info Practices
- Procedure
- Regulations
- Security Program
- Standards
- Validation
- Verification

Functions:

- **Manage:** Establish and administer a risk-based enterprise information security program that addresses applicable standards, procedures, directives, policies, regulations and laws
- **Design:** Specify enterprise information security compliance program control requirements
- **Implement:** Monitor and assess the information security compliance practices of all personnel in accordance with enterprise policies and procedures
- **Evaluate:** Assess the effectiveness of enterprise compliance program controls against the applicable laws, regulations, standards, policies, and procedures

Le référentiel EBK distingue enfin le « rôle » des différents « titres » et « métiers » lui correspondant.

Cette approche permet de simplifier la lecture des différents postes, tout en y associant les titres et éléments de langage propres à chaque entreprise.

Les fiches (ou « *role chart* ») EBK adoptent la structure suivante :

- Le rôle ;
- La description du rôle ;
- Les compétences requises et le niveau d'exigence associé à chacune d'entre-elles ;
- Les différents titres et appellations correspondant à ce rôle.

Figure 30. Exemple de fiche métier selon EBK

IT Security EBK: Role Chart

Role: IT Security Compliance Professional

Role Description:

The IT Security Compliance Professional is responsible for overseeing, evaluating, and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities, encompassing compliance from an internal and external perspective. Such activities include leading and conducting Internal Investigations, assisting employees comply with internal policies and procedures, and serving as a resource to external compliance officers during Independent assessments. The IT Security Compliance Professional provides guidance and autonomous evaluation of the organization to management.

Competencies/Functional Perspectives:

- Data Security: *Evaluate*
- Digital Forensics: *Evaluate*
- Enterprise Continuity: *Evaluate*
- Incident Management: *Evaluate*
- IT Security Training and Awareness: *Evaluate*
- IT Systems Operations & Maintenance: *Evaluate*
- Network Security & Telecommunications: *Evaluate*
- Personnel Security: *Evaluate*
- Physical and Environmental Security: *Evaluate*
- Procurement: *Evaluate*
- Regulatory & Standards Compliance: *Design, Implement, Evaluate*
- Risk Management: *Implement, Evaluate*
- Strategic Management: *Evaluate*
- System and Application Security: *Evaluate*

Job Titles:

- Auditor
- Compliance Officer
- Inspector General
- Inspector / Investigator
- Regulatory Affairs Analyst

L'objectif est ici clairement de permettre aux responsables des ressources humaines de se retrouver dans une multitude d'appellations ne correspondant en réalité qu'à un seul et même poste au sein de l'entreprise. Dans l'exemple ci-dessus, le professionnel chargé de la conformité IT aux normes de sécurité sera appelé auditeur, officier conformité ou encore inspecteur sans que cela ne change les compétences requises ainsi que le descriptif de sa fonction. L'avantage de cette démarche est de permettre aux responsables des ressources humaines de tous les secteurs, notamment du public, d'appréhender les emplois dans leurs diverses appellations du secteur privé.

• L'exemple du CSIS

Dans son document intitulé « A Human Capital Crisis in Cybersecurity – technical Proficiency Matters (A White Paper of the CSIS Commission on Cybersecurity for the 44th Presidency) »¹²⁷, le CSIS propose une matrice de développement des effectifs en matière de sécurité de l'information. Le CSIS présente une approche originale, soulignant que la majorité des fonctions clés de la cybersécurité sont exécutées par des acteurs non identifiés comme tels. Ces fonctions essentielles sont les suivantes :

- L'administration du système (client et serveurs)
- L'administration réseau et les opérations de sécurité réseau
- L'audit et l'assurance
- L'analyse des menaces, la détection d'intrusion, l'analyse de données, l'intelligence et la contre-ingérence
- L'inforensique
- La programmation

¹²⁷ http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhiteVersion.pdf

- L'architecture et l'ingénierie
- La gestion d'incidents.

Au sein de ces fonctions, quelques métiers clés sont également mentionnés.

- Chief Information Security Officer
- Systems Operations & Maintenance Professional
- Network Security Specialist
- Digital Forensic & Incident Response Analyst
- Information Security Assessor
- Information Systems Security Officer
- Security Architect
- Vulnerability Analyst
- Information Security Systems & Software Development Specialist
- Chief Information Officer
- Information Security Risk Analyst

Les compétences recensées et nécessaires au développement des effectifs « cybersécurité » sont listées et catégorisées. Le CSIS distingue les compétences « cœur » en *hardware*, logiciel, business et réseau ; celles nécessitant un entraînement spécialisé (l'analyse, l'architecture, le système, l'acquisition et la collecte) ; les compétences offensives (collecte, exploitation, ciblage, analyse et traitement de ces données) ; les compétences défensives (pen test, inforensique, audit, détection et prévention d'intrusion, analyse et traitement de ces données) ; les compétences « support » (politique, légal, contrats et budget) et, enfin, les compétences de leadership.

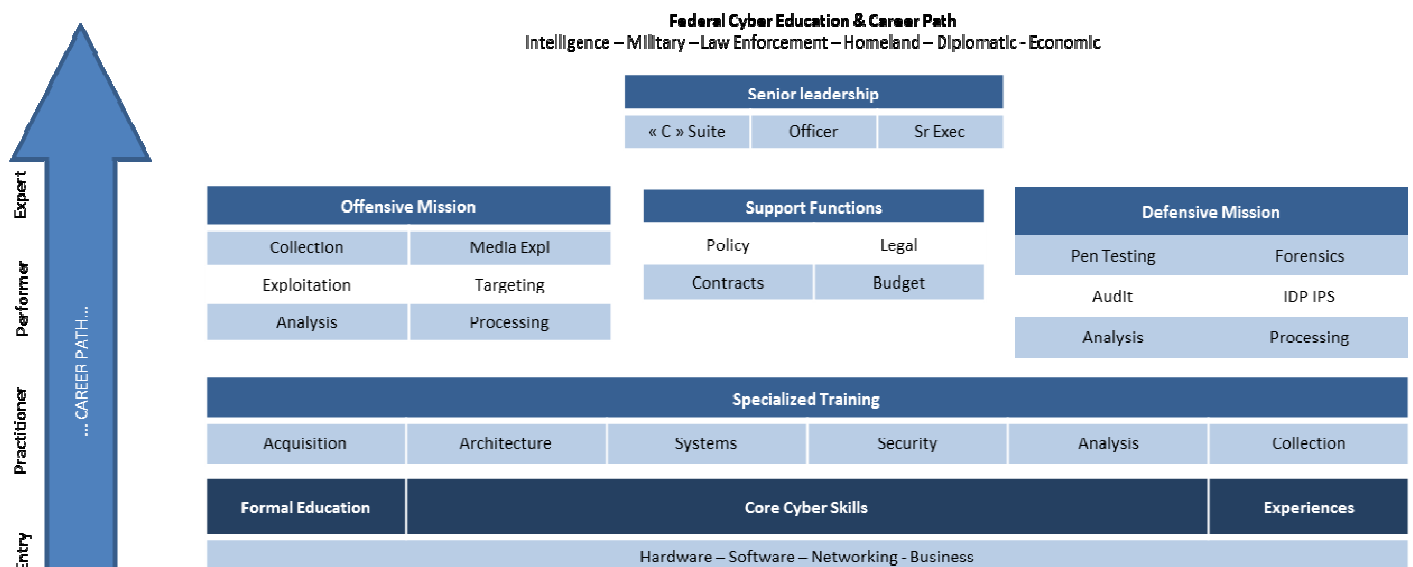


Figure 31. Parcours carrières et compétences, CSIS¹²⁸

¹²⁸ http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkwhteVersion.pdf

Le CSIS complète sa démarche en proposant des modèles de « fiches métier ».

Figure 32. Exemple de fiche « emploi type », CSIS

Systems Operations and Maintenance Professional**: The Systems Operations and Maintenance Professional supports and implements the security of information and information systems during the operations, maintenance, and enhancements phases of the systems development life cycle. The Systems Operations and Maintenance Professional is also responsible for implementing server configurations, operating systems, database systems, firewalls, patch management, and account management to protect the systems against threats and vulnerabilities.				
Performance Level	Description/Complexity	Competencies/Skills	Suggested Credentials	Suggested Learning & Development Sources
I: Entry	<p>Has a basic understanding of computer systems and related information security software and hardware components</p> <p>Ability to perform basic security system administration duties including software and hardware installation, troubleshooting, system backup, network component maintenance</p> <p>Basic understanding of tools and methods for identifying anomalies in system behavior; develops ability to recognize anomalies</p> <p>Applies skills and abilities with supervision on projects, programs, and initiatives with low threat and scope (e.g., inter-office)</p>	<p>Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below.</p> <p>Competency/Skill Proficiency Descriptors</p> <p>I-Entry: Basic understanding of concepts addressed in relevant competency/skill models</p> <p>II-Intermediate: Working knowledge and application of relevant competency/skill models in work activities</p> <p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p>Relevant Competency/Skill Sources:</p> <ul style="list-style-type: none"> OPM GS-2200 Job Family Standard Competencies Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas (www.cio.gov) DHS EBK Competencies FISMA Guidance OPM's IT Workforce Roadmap NIST SP 800-16, Revision 1 ODNI Cyber Subdirectory Competencies DoD Directive 8570 CNSD Policies, Directives, and Reports 	<ul style="list-style-type: none"> 0-3 years experience involving work directly related to systems operations and maintenance (e.g., help desk); OR a Bachelors Degree (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management) Participation in Scholarship for Service program through a designated Center of Academic Excellence in Information Assurance Education (CAEIAE) 	<ol style="list-style-type: none"> Development Resources: <ul style="list-style-type: none"> IT Workforce Roadmap (IT Roadmap) Graduate Programs, USDA IT Programs GoLearn Courses (www.golearn.gov) CIO Council (www.cio.gov) DoD DISA Training GSA's CIO university Program University Information Security Programs: <ul style="list-style-type: none"> National Defense University- IRM College IS/IA Degree Programs- CAEIAE Private University Programs (e.g., GMU, MIT) OPM Development Center: The Federal Executive Institute and the Management Development Centers Participation in coaching/mentoring/job shadowing programs Agency Requirements: organization and business area training identified as required Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4012) Training by external vendors, for security configuration (e.g., Oracle, Computer Associate, IBM, and HP Tools, Sans Institute)
II: Intermediate	<p>Applies an understanding of the information security operational characteristics of a variety of computer platforms, networks, software applications, and operating systems</p> <p>Ability to explain to others the methods and techniques used in installation, testing, network debugging, troubleshooting, and maintenance of PCs, servers, printers, and related equipment</p> <p>Automates repetitive processes (e.g., log reviews, configuration testing) to facilitate information security operations</p> <p>Evaluates and assesses operating practices to determine adequate risk management and compliance standards, with on-going systems monitoring</p> <p>Is responsible for contributing, with limited supervision, to projects, programs, and initiatives with medium-threat and moderate scope (e.g., sub-organization wide)</p>	<p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p>Relevant Competency/Skill Sources:</p> <ul style="list-style-type: none"> OPM GS-2200 Job Family Standard Competencies Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas (www.cio.gov) DHS EBK Competencies FISMA Guidance OPM's IT Workforce Roadmap NIST SP 800-16, Revision 1 ODNI Cyber Subdirectory Competencies DoD Directive 8570 CNSD Policies, Directives, and Reports 	<ul style="list-style-type: none"> Bachelors Degree and 2+ years experience (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 3-5 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs Possession and demonstrated application of relevant certifications <ul style="list-style-type: none"> Core: MCSE, CCNA, CCNP, ISC² CAP Related: CISSP, CISM, ISC² ISSMP, CompTIA, SANS GIAC, FMP 	<ol style="list-style-type: none"> National Defense University- IRM College IS/IA Degree Programs- CAEIAE Private University Programs (e.g., GMU, MIT) OPM Development Center: The Federal Executive Institute and the Management Development Centers Participation in coaching/mentoring/job shadowing programs Agency Requirements: organization and business area training identified as required Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4012) Training by external vendors, for security configuration (e.g., Oracle, Computer Associate, IBM, and HP Tools, Sans Institute)
III: Advanced	<p>Effectively communicates technical information to non-technical audiences; influences others to comply with policies and conform to standards and best practices</p> <p>Designs the organization's working information security systems operations and maintenance strategy and methodology to comply with the organization's standards and mission</p> <p>Understands the needs of the organization and establishes appropriate vendor relationships to manage the proposal and purchasing process</p> <p>Attends and participates in professional conferences to stay abreast of new trends and innovations in the field of information systems</p> <p>Independently manages, plans, evaluates, and advocates for information security compliance systems, plans, and functions, and is responsible for the management of complex projects, programs, and initiatives with high threat and large scope (e.g., agency-wide or inter-governmental), with on-going systems monitoring</p>	<p>III-Advanced: Advanced application and mastery of relevant competency/skill models</p> <p>Relevant Competency/Skill Sources:</p> <ul style="list-style-type: none"> OPM GS-2200 Job Family Standard Competencies Clinger-Cohen Core Competencies with an emphasis on <i>Technical, Desktop Technology Tools, and IT Security/Information Assurance</i> competency areas (www.cio.gov) DHS EBK Competencies FISMA Guidance OPM's IT Workforce Roadmap NIST SP 800-16, Revision 1 ODNI Cyber Subdirectory Competencies DoD Directive 8570 CNSD Policies, Directives, and Reports 	<ul style="list-style-type: none"> Bachelors Degree and 3+ years experience (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 5+ years of experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs Demonstrated experience in managing/supervising a systems operations and maintenance group Possession and demonstrated application of relevant certifications <ul style="list-style-type: none"> Core: MCSE, CCNA, CCNP, ISC² CAP Related: CISSP, CISM, ISC² ISSMP, CompTIA, SANS GIAC, FMP 	<ol style="list-style-type: none"> National Defense University- IRM College IS/IA Degree Programs- CAEIAE Private University Programs (e.g., GMU, MIT) OPM Development Center: The Federal Executive Institute and the Management Development Centers Participation in coaching/mentoring/job shadowing programs Agency Requirements: organization and business area training identified as required Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4012) Training by external vendors, for security configuration (e.g., Oracle, Computer Associate, IBM, and HP Tools, Sans Institute)

Ces fiches d'emplois types présentent les qualités et compétences exigées pour chaque poste, qu'il s'agisse des compétences faiblement maîtrisées, à un niveau intermédiaire ou un niveau avancé.

Figure 33. Fiche « emploi type » décrivant les compétences requises selon le critère « performance level », CSIS

Systems Operations and Maintenance Professional**: The Systems Operations and Maintenance Professional supports and implements the security of information and information systems during the operations, maintenance, and enhancements phases of the systems development life cycle. The Systems Operations and Maintenance Professional is also responsible for implementing server configurations, operating systems, database systems, firewalls, patch management, and account management to protect the systems against threats and vulnerabilities.	
Performance Level	Description/Complexity
I: Entry	<p>Has a basic understanding of computer systems and related information security software and hardware components</p> <p>Ability to perform basic security system administration duties including software and hardware installation, troubleshooting, system backup, network component maintenance</p> <p>Basic understanding of tools and methods for identifying anomalies in system behavior; develops ability to recognize anomalies</p> <p>Applies skills and abilities with supervision on projects, programs, and initiatives with low threat and scope (e.g., inter-office)</p>
II: Intermediate	<p>Applies an understanding of the information security operational characteristics of a variety of computer platforms, networks, software applications, and operating systems</p> <p>Ability to explain to others the methods and techniques used in installation, testing, network debugging, troubleshooting, and maintenance of PCs, servers, printers, and related equipment</p> <p>Automates repetitive processes (e.g., log reviews, configuration testing) to facilitate information security operations</p> <p>Evaluates and assesses operating practices to determine adequate risk management and compliance standards, with on-going systems monitoring</p> <p>Is responsible for contributing, with limited supervision, to projects, programs, and initiatives with medium-threat and moderate scope (e.g., sub-organization wide)</p>

Ces fiches présentent également une liste de formations et de certifications recommandées.

Figure 34. Fiche « emploi type » décrivant les certifications et formations recommandées, CSIS

Suggested Credentials	Suggested Learning & Development Sources
<ul style="list-style-type: none"> ▶ 0-3 years experience involving work directly related to systems operations and maintenance (e.g., help desk); OR a Bachelors Degree (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management) ▶ Participation in Scholarship for Service program through a designated Center of Academic Excellence in Information Assurance Education (CAEIAE) 	<ol style="list-style-type: none"> 1. Development Resources: <ul style="list-style-type: none"> ▶ IT Workforce Roadmap (IT Roadmap) ▶ Graduate Programs, USDA IT Programs ▶ GoLearn Courses (www.golearn.gov) ▶ CIO Council (www.cio.gov) ▶ DoD DISA Training ▶ GSA's CIO university Program 2. University Information Security Programs: <ul style="list-style-type: none"> ▶ National Defense University- IRM College ▶ IS/IA Degree Programs- CAEIAE ▶ Private University Programs (e.g., GMU, MIT) 3. OPM Development Center: The Federal Executive Institute and the Management Development Centers 4. Participation in coaching/mentoring/job shadowing programs 5. Agency Requirements: organization and business area training identified as required 6. Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate 7. Current and emerging legislation, policy, and regulations (e.g., FISMA, NIST SP-800 series, FIPS, OMB directives, CNSSI No. 4012) 8. Training by external vendors for security configuration (e.g., Oracle, Computer Associate, IBM, and HP Tools, Sans Institute)
<ul style="list-style-type: none"> ▶ Bachelors Degree and 2+ years experience (suggested areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 3-5 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs ▶ Possession and demonstrated application of relevant certifications <ul style="list-style-type: none"> ▶ Core: MCSE, CCNA, CCNP, ISC² CAP ▶ Related: CISSP, CISM, ISC² ISSMP, CompTIA, SANS GIAC, PMP 	
<ul style="list-style-type: none"> ▶ Bachelors Degree and 3+ years experience (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); OR 5+ years of experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs 	

• **Le modèle de compétences de l'OPM**

L'OPM¹²⁹ a développé un modèle de compétences dédié à la cybersécurité. L'Organisme précise que ce modèle de compétences est destiné à améliorer la sélection des candidats à un poste, à manager les performances des employés, à planifier la gestion des effectifs et à entrainer et développer les compétences des employés. Ce référentiel qui a été élaboré de concert avec le CIO et le NICE¹³⁰, identifie quatre « occupations », six grades, et distribue les compétences au sein de ces occupations et des grades associés.

¹²⁹ <http://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=3436> et <http://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/>

¹³⁰ <http://www.gao.gov/new.items/d128.pdf>

Occupations	Grades
2210 Information Technology Management Series	9, 11, 12, 13, 14, 15
0855 Electronics Engineering Series	12, 13, 14, 15
0854 Computer Engineering Series	12, 13, 14, 15
0391 Telecommunications Series	9, 11, 12, 13

Extrait : « Occupations and Grades with Confirmed Competencies »¹³¹

Grade 9	Grade 11	Grade 12	Grade 13
Communications	Communications	Communications	Capacity
Security	Security	Security	Management
Management	Management	Management	Communications
Compliance	Compliance	Compliance	Security
Information	Information	Information	Management
Assurance	Assurance	Assurance	Compliance
Network	Network	Physical Security	Network
Management	Management	Security	Management
Personnel Security	Physical Security	Telecommunications	Project Management
and Safety	Security		Security
Physical Security	Technology		Telecommunications
Security	Awareness		
Telecommunications	Telecommunications		

Extrait : compétences techniques exigées pour l'occupation « Telecommunication Series »

Le référentiel liste plus de 110 compétences au total. Ces compétences sont toutes définies dans ce document par ordre alphabétique¹³². Le référentiel identifie notamment des compétences humaines, de l'ordre du « talent » et des qualités propres, tels que : l'attention aux détails, l'honnêteté, l'intégrité, le travail d'équipe.

¹³¹ <http://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=3436>

¹³² <http://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/mosaic-studies-competencies.pdf>

- **Royaume-Uni : l'initiative e-skills**

C'est dans un document datant de mars 2014¹³³ que le gouvernement britannique a rappelé sa volonté de bâtir un véritable vivier de compétences en cybersécurité au service de sa stratégie nationale. La stratégie britannique est animée de concert par le National Cyber Security Programme (NCSP), le Department for Business Innovation and Skills (BIS), le Government Communications Headquarters (GCHQ) et le Cabinet Office.

L'initiative e-Skills¹³⁴ opte pour une subdivision des métiers distinguant les postes commerciaux des postes non-commerciaux. Elle identifie les 28 emplois types suivants :

Commerciaux :	Non-commerciaux :
1. Sales Engineer	1. Information Security Analyst
2. Pre-sales Consultant	2. Information Security Manager
3. Technical Account Manager	3. Information Security Consultant
4. Account Manager (with security)	4. Information Security Officer
5. Business Development Manager (with security)	5. IT Security Analyst
6. Sales Executive (with security)	6. IT Security Manager
7. Sales Manager (with security)	7. IT Security Consultant
8. Sales Director (with security)	8. IT Security Officer
	9. Network Security Engineer
	10. Network Security Consultant
	11. Network Security Analyst
	12. Security Engineer
	13. Security Administrator
	14. CISO/Chief Information Security Officer/Head of Information Security
	15. Security Architect (variants of)
	16. Security Auditor
	17. PCI Consultant/QSA Consultants

¹³³ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf

¹³⁴ <http://www.e-skills.com/research/research-publications/cyber-security-careers/>

	<p>18. Computer/Digital Forensics Analyst/Investigator (variants of)</p> <p>19. Penetration Tester/Pen Tester</p> <p>20. Application Security Specialist (variants of)</p>
--	--

Le référentiel de compétences “IISP Skills Framework”¹³⁵ isole pour sa part un certain nombre de compétences classées par niveau de maîtrise.

Figure 35. Extrait du “IISP Skills Framework”

The following definitions should be used when assessing your score for competencies in discipline J. Examples of experience within these disciplines are shown in Appendix B, and should be consulted before completion.				
Skill	Level 1	Level 2	Level 3	Level 4
Teamwork and Leadership	Works cooperatively and professionally with others.	Is encouraging and supportive and provides a lead within the local area. Task-based team working.	Encourages and challenges others. Provides a lead across an organisation.	Inspires and involves others from inside and outside the organisation, environment in which others may develop leadership qualities.
Delivering	Takes responsibility for completing own tasks.	Responsibility for an element of delivery against one or more business objectives, balancing priorities to achieve this.	Responsible for ensuring delivery is achieved against a portfolio of business objectives, overcoming obstacles to achieve goals.	Responsible for achievement of overall business goals in own professional or functional area.
Managing Customer Relationships	Understands and aims to meet customer requirements.	Negotiates with customers to improve the service to them and to manage their expectations.	Works with customers to ensure that their needs drive business plans.	Uses customer priorities to drive organisations’ plans, resolving the conflicting demands of different customers.
Corporate Behaviour	Understands local objectives and organisations aims. Is cost-effective in own work.	Understands the aims of own and related areas across an organisation.	Takes action to achieve greater corporate efficiency, in line with its strategic aims.	Develops strategy and ensures the long-term cost-effectiveness of an organisation by understanding the influences upon it.
Change and Innovation	Is positive about change, and suggests improvements possible in own area.	Generates creative ideas, and demonstrates sensitivity in implementing local change.	Contributes to change strategies and generates new ideas or approaches, going beyond the local area.	Is innovative and radical. Champions considered, co-ordinated change through policy and planning.
Analysis and Decision Making	Is methodical when making decisions and solves problems which impact on own work.	Makes effective decisions in consultation with others and/or solves complex problems in immediate area.	Makes effective decisions and / or solves complex problems in uncertain situations, or where the impact is greater than in the immediate working area.	Makes effective strategic decisions and / or solves complex problems with strategic impact, or no precedent.
Communications and Knowledge Sharing	Communicates clearly and shares knowledge with colleagues practice.	Encourages and contributes to discussion. Is proactive in sharing information in own work-area.	Is a persuasive communicator. Sets a lead in sharing knowledge effectively in diverse areas across an organisation.	Is influential and diplomatic in negotiations with other organisations and formulates knowledge-sharing.

Intitulé	Créer un référentiel des métiers et des compétences
Descriptif	Référencer selon ses besoins les métiers et compétences nécessaires.
Résultats	Inconnus.
Contraintes	Le préalable de toute démarche de recrutement et d’entraînement reste la

¹³⁵ https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework.aspx

associées	cartographie et l'audit de ses propres besoins.
Intérêt	Un référentiel tant des métiers que des compétences requises a vocation à guider la mission de GRH du recrutement à la gestion de carrières.

B23 : mettre en place un processus normalisé de gestion des compétences

La société STERIA a mis en place au sein de son activité sécurité un processus structuré de gestion des compétences s'articulant autour des points suivants¹³⁶ :

- Des « entretiens performance et développement individuel » (EDPI) qui ont lieu chaque année entre février et avril ;
- Une « People review (mai-août). C'est une réunion collégiale rassemblant le management et les RH. L'objectif est d'examiner le cas de chaque personne de l'entité et de voir comment répondre aux souhaits exprimés lors des EDPI. C'est l'occasion de repérer les talents ou « fast trackers » ainsi que les personnes en situation de perte d'employabilité (EDA)
- Un comité d'évaluation (CEDRE) qui a lieu en septembre et octobre. C'est une revue collective destinée à anticiper les besoins. La veille technologique menée par l'équipe ainsi que les besoins client vont alimenter la réflexion.

Figure 36 : Le processus de management des talents « cybersécurité » de Steria¹³⁷



¹³⁶ Source : entretiens avec Steria

¹³⁷ Source : Steria

Intitulé	
Mise en place d'un processus normalisé de gestion des compétences	
Descriptif	Steria a mis en place pour son activité sécurité un cycle comprenant entretien individuel, « people review » et comité d'évaluation. Pratique habituelle en RH mais déclinée ici dans le domaine de la cybersécurité.
Résultats	Très bons résultats à la fois en termes de gestion des parcours interne et d'anticipation des besoins.
Contraintes associées	Aucune
Intérêt	Faciliter le dialogue entre opérationnels et RH

B24 : se doter d'outils d'évaluation des compétences

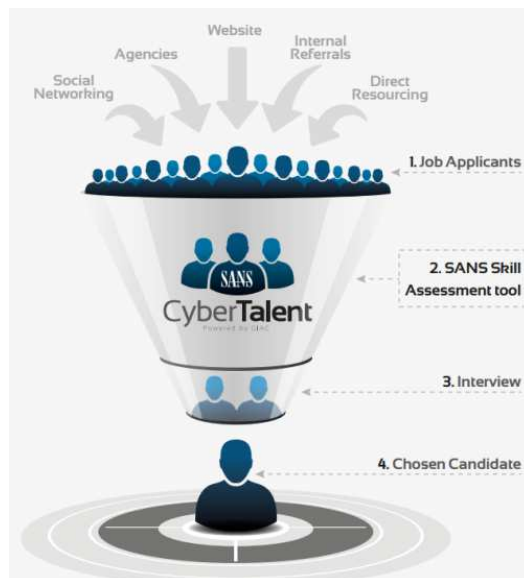
“Organizations need to find a way to keep their stars, and it isn't just about increasing an individual's pay.”¹³⁸

Tom Carver, director of SANS CyberTalent

Si la création d'un référentiel des emplois types et des compétences est une étape essentielle à la gestion des carrières, elle doit s'accompagner d'une évaluation constante et qualitative de ces compétences. Évaluer les compétences c'est, d'une part, mesurer l'écart entre le besoin affirmé en matière de compétences et la réalité. C'est, ensuite, savoir évaluer tant les compétences que les talents et aptitudes plus difficiles à mesurer objectivement. Cette tâche est plus complexe qu'il n'y paraît, notamment pour des responsables des ressources humaines ne disposant évidemment pas des compétences techniques nécessaires. Cette évaluation sera l'un des leviers du recrutement, mais aussi de la formation et de la mobilité interne.

¹³⁸ <http://www.nextgov.com/cio-briefing/wired-workplace/2013/04/new-tool-can-help-agencies-assess-cyber-skills/62576/>

- L'outil « CyberTalent Assessments » du SANS Institute



L'institut SANS a développé un outil d'évaluation des talents en matière de cybersécurité. Le « CyberTalent Assessments »¹³⁹ est un outil en ligne, mis à disposition à plusieurs fins : l'évaluation des candidats aux postes axés cybersécurité ; l'évaluation de leurs équipes en interne ; l'évaluation des partenaires et sous-traitants.

La plateforme entièrement Web (SaaS) est intuitive et se substitue en partie à certaines fonctionnalités d'un SIRH. Elle permet l'enregistrement des profils à évaluer, met à disposition une liste de questions par domaine « item », affiche les scores par profil évalué, ainsi qu'une vue globale de tous les profils évalués.

¹³⁹ <http://www.sans.org/cybertalent/assessments>

Figure 37. Capture de l'outil d'évaluation des compétences du SANS Institute

Jeff			
Date Started: 01/22/2013			
Item	Score	Correct	Rank
Overall	88%	22 / 25	3
Communications Security Domain	100%	5 / 5	1
Defense in Depth Domain	80%	4 / 5	4
Internet Security Technologies Domain	100%	5 / 5	1
Networking Concepts Domain	80%	4 / 5	4
Operating Systems Security Domain	80%	4 / 5	3

Cet outil semble entièrement destiné aux spécialistes des ressources humaines, afin de leur offrir une meilleure compréhension des métiers de la cybersécurité.

Les questions posées aux évalués sont issues du GIAC (Global Information Assurance Certification)¹⁴⁰, référentiel régulièrement utilisé par le SANS lui-même pour les certifications. Mais le DRH n'est pas lié par cette liste de questions : l'employeur peut intégrer ses propres questions, adaptées aux spécificités et aux besoins de son entreprise¹⁴¹.

- **Le « PerformanScore »TM de TeleCommunication Systems**

La société TeleCommunication Systems a développé le « PerformanScore »^{TM142}, outil permettant d'évaluer les compétences, talents et aptitudes des salariés et candidats. L'objectif de l'outil est clairement affiché : il s'agit de s'assurer que les compétences, talents et aptitudes (KSA) de l'individu évalué correspondent bien à son curriculum vitae, et notamment à son expérience annoncée, ses certifications et diplômes. L'outil a vocation à servir de base à la formation et mise à jour des compétences.



¹⁴⁰ <http://www.giac.org/>

¹⁴¹ <http://www.nextgov.com/cio-briefing/wired-workplace/2013/04/new-tool-can-help-agencies-assess-cyber-skills/62576/>

¹⁴² <http://www.telecomsys.com/services/cyber-solutions/performanscore.aspx>

- **S'équiper d'une grille d'évaluation : le modèle de Mark E.S. Bernard, RSSI indépendant**

Le RSSI et Data Privacy Officer indépendant Mark Edward Stirling Bernard propose en libre accès une grille d'évaluation des RSSI (CSSO ou CISO). Ce document liste l'ensemble des compétences exigées pour ce métier. Il tient également compte du niveau attendu d'acquisition des compétences : celui-ci variera selon l'expérience, la formation, le profil et les certifications. Les différents niveaux sont, du plus faible au plus haut : le savoir, la compréhension, l'application, l'analyse, la synthèse et l'évaluation.

Figure 38. Fiche d'évaluation du RSSI, By Mark Edward Stirling Bernard, CyberSecurity /Information Security Program Expert at Independent CCSO or CISO as a Service ¹⁴³

Skills & Competency Assessment Scale							
L1.Knowledge	L2.Comprehension	L3.Application	L4.Analysis	L5.Synthesis	L6.Evaluation		

Sample Questions

L1. Are you aware of the subject, tell me about it? L4. How you would perform root-cause-analysis against related issues?
L2. Can you explain the subject? L5. How would you apply lessons learned to re-deign the approach?
L3. Tell me how you would apply this knowledge? L6. How would you assess the effectiveness of your applied strategy?

Domain	Subject	L1	L2	L3	L4	L5	L6
Security Leadership	Program Management	L1	L2	L3	L4	L5	L6
	Manage Strategic & Tactical Plans	L1	L2	L3	L4	L5	L6
	Manage the Budget	L1	L2	L3	L4	L5	L6
	Manage Communications	L1	L2	L3	L4	L5	L6
	Manage the Team & Projects	L1	L2	L3	L4	L5	L6
	Lead Security Incident Response Team	L1	L2	L3	L4	L5	L6
	Manage Security SLA / OLA	L1	L2	L3	L4	L5	L6
	Manage Compliance	L1	L2	L3	L4	L5	L6
	Manage Vulnerabilities	L1	L2	L3	L4	L5	L6
	Lead Investigations	L1	L2	L3	L4	L5	L6
	Lead Monitoring & Reporting	L1	L2	L3	L4	L5	L6
	Manage related Docs & Records	L1	L2	L3	L4	L5	L6
Manage Audits	L1	L2	L3	L4	L5	L6	
Security Governance	Engage Stakeholders	L1	L2	L3	L4	L5	L6
	Manage Committee ToR	L1	L2	L3	L4	L5	L6
	Facilitate Decision Points	L1	L2	L3	L4	L5	L6
	Allocate Resources	L1	L2	L3	L4	L5	L6
	Allocate Capital	L1	L2	L3	L4	L5	L6
Manage External Inquiries	L1	L2	L3	L4	L5	L6	
Security Risk Management	Manage RM Policy	L1	L2	L3	L4	L5	L6
	Facilitate RM Appetite	L1	L2	L3	L4	L5	L6
	Align with Enterprise Risk	L1	L2	L3	L4	L5	L6
	Lead Risk Assessment	L1	L2	L3	L4	L5	L6
	Lead Risk Treatment	L1	L2	L3	L4	L5	L6
	Manage Risk Registry	L1	L2	L3	L4	L5	L6
	Lead Due Diligence	L1	L2	L3	L4	L5	L6
	Manage Service Provider Risks	L1	L2	L3	L4	L5	L6
Lead Monitoring & Reporting	L1	L2	L3	L4	L5	L6	
Security Architecture	Facilitate Business Architecture	L1	L2	L3	L4	L5	L6
	Oversee Information Architecture	L1	L2	L3	L4	L5	L6
	Consult on Application Architecture	L1	L2	L3	L4	L5	L6
	Consult on Technology Architecture	L1	L2	L3	L4	L5	L6
	Manage the Roadmap	L1	L2	L3	L4	L5	L6

- **Le CyberM³ : l'approche globale de Booz Allen Hamilton**

L'approche de Booz Allen Hamilton est originale¹⁴⁴ : l'outil CyberM³ propose deux types d'évaluations. La première est destinée aux RSSI. Elle s'adapte aux niveaux de certifications, aux spécificités de métier de RSSI et propose une évaluation affinée et poussée. L'outil propose également

¹⁴³ <http://www.slideee.com/slide/assessing-cyber-security-skills-and-competencies>

¹⁴⁴ <http://www.boozallen.com/media/file/cyber-m3-close-up-cyber-skills-assessments-organizational-analysis.pdf>

l'évaluation des compétences à l'échelle organisationnelle. Cette brique s'adresse à tout le personnel amené, tôt ou tard, à gérer de l'information sensible.

Ainsi, au-delà de la simple évaluation des compétences, l'outil a une vocation plus générale d'évaluation du niveau de cybersécurité d'une équipe, d'une entreprise ou d'une institution.

Intitulé	
Se doter d'outils d'évaluation des compétences	
Descriptif	Se doter d'un outil d'évaluation des compétences plus ou moins interactif.
Résultats	Inconnus.
Contraintes associées	Former les responsables des ressources humaines. Adapter l'outil à ses spécificités. Choisir un outil externe représente un coût non-négligeable.
Intérêt	S'assurer de la concordance entre besoins et capacités réelles en interne ; s'assurer de la concordance entre le curriculum vitae et compétences réelles ; auditer ses partenaires ; évaluer les candidats.

B25 : organiser la mobilité des profils

B25-1 : créer une véritable filière de mobilité interne

L'US Air Force (USAF) a très tôt fait l'analogie¹⁴⁵ entre cyberspace et espace, et ainsi rapidement intégré les cyberopérations comme faisant partie de son scope de compétences. Elle distingue dans ses effectifs cybersécurité les quatre catégories suivantes :

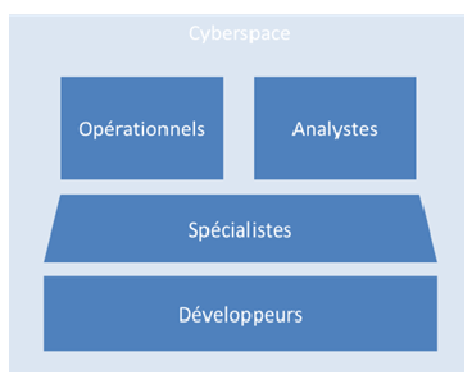
- les cyberspace operators,
- les cyberspace specialists,
- les cyberspace analysts,
- et les cyberspace developers.^{146 147}

¹⁴⁵ "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field", Katrina A. Terry, Air Force Institute of Technology, 2011, 124 pages

¹⁴⁶ <http://www.af.mil/News/ArticleDisplay/tabid/223/Article/123109/cyberspace-career-fields-training-paths-badge-proposed.aspx>

¹⁴⁷ <http://www.dtic.mil/dtic/tr/fulltext/u2/a510497.pdf>

Figure 39. Schéma illustrant la complémentarité des 4 types de postes au sein de l'USAF¹⁴⁸



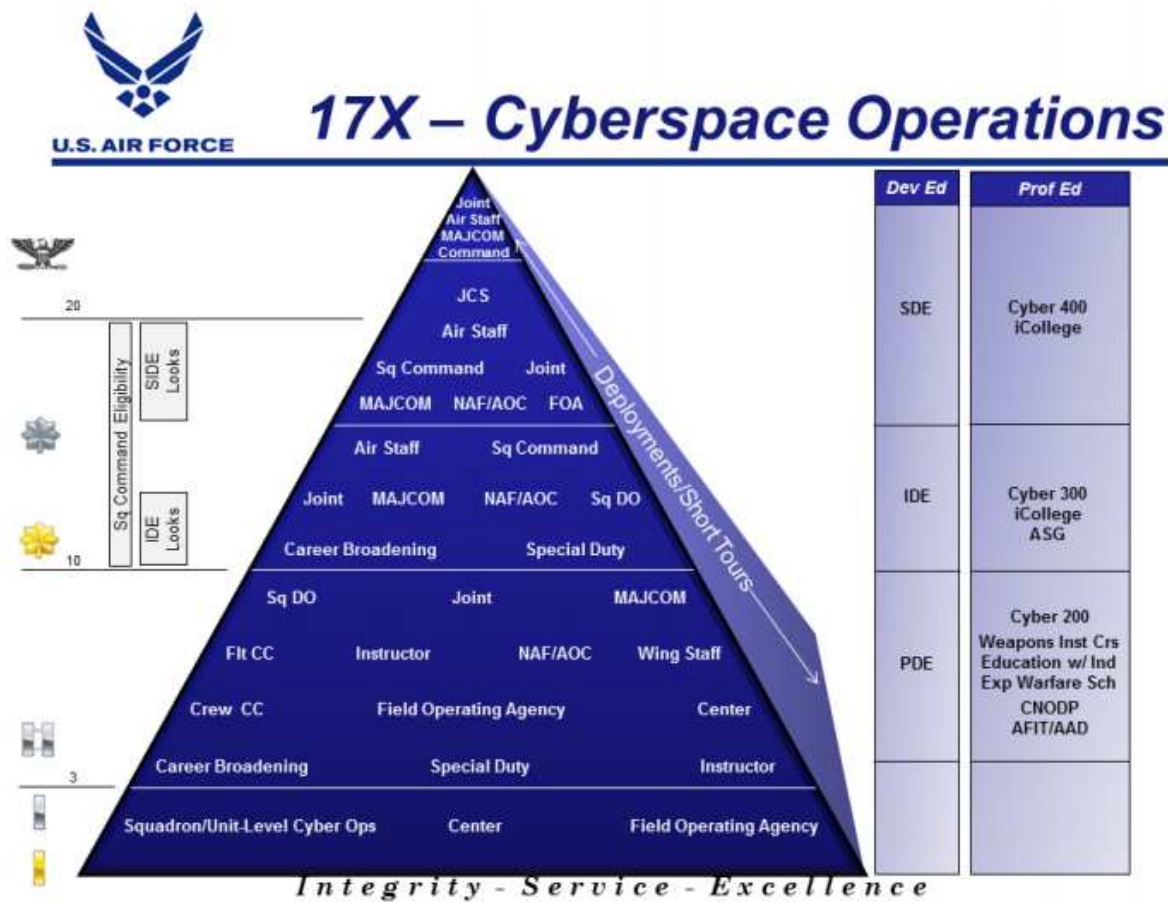
L'US Air Force souhaite assurer ses effectifs au sein de ces quatre catégories, par le recrutement de militaires, réservistes, civils et sous-traitants (« contractors personnel »). Objectif : transformer d'ici 2018 les plans de carrières d'officiers de service et des simples soldats en organisant une transition vers les nouveaux parcours « cybersécurité ». Les plans de carrières « cybersécurité » engloberont et anticiperont la totalité de la carrière d'un militaire, de son recrutement à sa retraite. Ce plan de carrière sera jalonné de formations, d'entraînements et d'opportunités permettant d'osciller du niveau tactique à l'opérationnel. Cette transformation se traduit par :

- la création du statut de Cyberspace Warfare Officer (CWO) ;
- l'intégration des plans de carrière préexistants (électronique, management de l'information, informatique) au sein d'un unique parcours intitulé « cyberspace operations career field ».

Le CWO peut choisir son orientation dans une liste de 14 spécialités.

¹⁴⁸ CEIS

Figure 40. « Career Field Pyramid », USAF¹⁴⁹



Cette mutation intègre au sein du plan de carrière deux parcours, le parcours « technique » et le parcours « leadership »¹⁵⁰. Cette subdivision est essentielle, car elle permet de ne pas faire du leadership le seul et unique vecteur d'évolution de carrière. Ainsi, un Cyberspace Warfare Officer peut choisir d'être « leader technique ». Ce système a également le mérite de ne pas éloigner de l'opérationnel, en cas de promotion, des acteurs excellant sur la technique et indispensables au terrain.

“In the officer ranks, only a small fraction ever takes part in on-keyboard or operational missions where the effects of cyber are leveraged for exploitation, attack or defense. Yet, all of the personnel wear the badge and identify themselves, some cynically so, as part of the cybercommunity.” 1st Lt.

Robert M. Lee, USAF, 2013¹⁵¹

Toutefois, cette initiative est entachée du manque de coordination et de standardisation à l'échelle de l'ensemble des forces armées américaines. Chacune développe en effet ses capacités « cyber » selon sa propre stratégie, et non dans une démarche globale de complétion des effectifs cyber dans leur globalité.

“Most do not understand the domain or how to operate within it.”

¹⁴⁹ http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfotp17x/cfotp17x.pdf

¹⁵⁰ « USAF Cyber Capability Development: A Vision for Future Cyber Warfare & a Concept for Education of Cyberspace Leaders », Williams, Paul D, avril 2009, <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA539513>

¹⁵¹ <http://www.afcea.org/content/?q=node/11855>

De plus, cette démarche a comme conséquence de gonfler artificiellement les effectifs dédiés à la cybersécurité, en intégrant des spécialistes des communications, signaux et télécommunications. Bien qu'ils se recoupent, ces domaines ne se confondent pas. Ce gonflement des effectifs, justifié par une vision globale du cyberspace, fausse donc la perception et noie les effectifs réels. Une perception peu fiable va à l'encontre d'une démarche globale de gestion et de valorisation des effectifs, ne permet pas la mise en œuvre efficace et opérationnelle d'une stratégie globale. Enfin, faire de spécialistes des télécommunications des experts en cyberoperations est susceptible de nuire à la qualité et à l'efficacité de l'action de l'US Air Force ; considérer le cyberspace comme un domaine à part entière, c'est en effet reconnaître ses spécificités. Ce dernier point souligne l'importance croissante de la formation pour les personnels spécialistes de matières proches ou se superposant à la cybersécurité.

Intitulé	
	Créer une véritable filière de mobilité interne
Descriptif	L'US Air Force propose une seule et unique filière cybersécurité.
Résultats	Contestés.
Contraintes associées	Veiller à ne pas noyer les véritables postes « cybersécurité » dans les problématiques IT et télécommunications.
Intérêt	Simplifier les parcours et plans de carrière ; mutualiser les efforts de recrutement et de formation ; opter pour une vision globale.

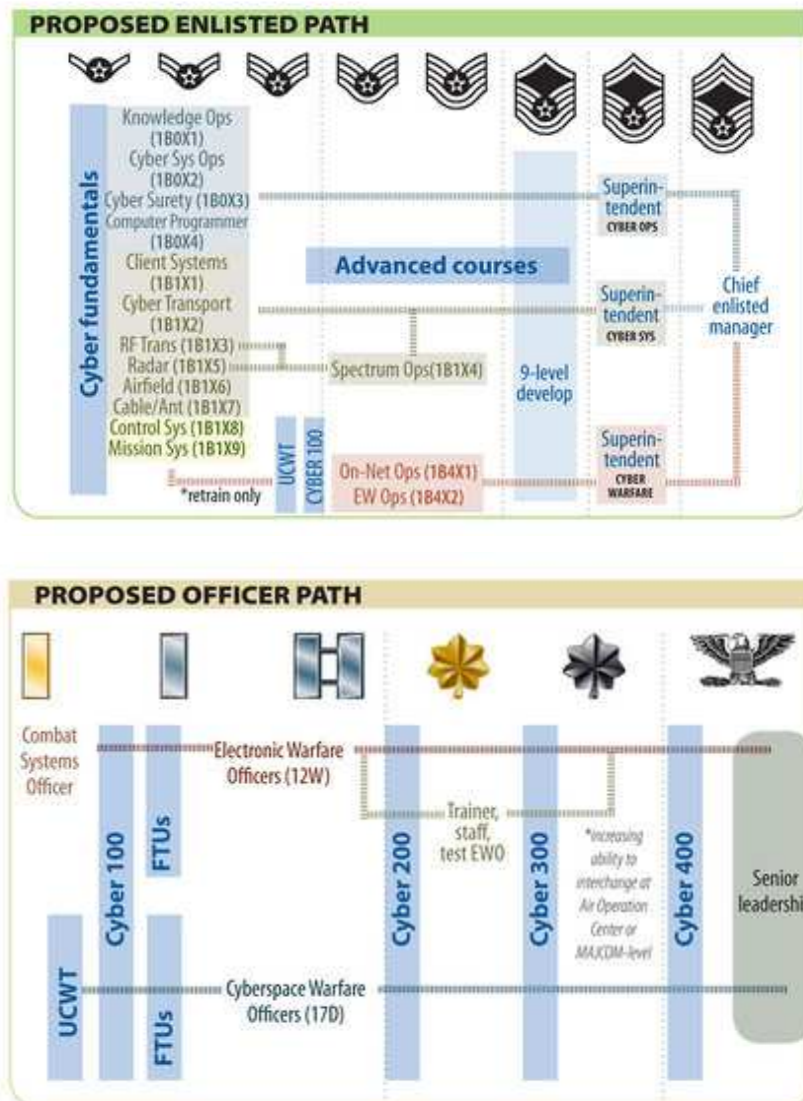
B25-2 : proposer des plans de carrière

L'US Air Force¹⁵³ propose des parcours de carrière tant horizontale que verticale, jalonnés de séances d'entraînement et de formation. L'infographie ci-dessous schématise les parcours pré-identifiés.

¹⁵² <http://www.afcea.org/content/?q=node/11855>

¹⁵³ http://www.publicdomainfiles.com/show_file.php?id=13511199019528

Figure 41. Plans de carrière, USAF



Intitulé	
Descriptif	Proposer des plans de carrière
Résultats	L'US Air Force communique sur des plans de carrière.
Contraintes associées	Inconnus.
Contraintes associées	Aucune.

Intérêt	Appâter les candidats grâce à des parcours simples, intelligibles et valorisants.
---------	---

B25-3 : développer les échanges entre le public et le privé

Le budget 2010 autorise le DoD à mettre en place un « pilot program for the temporary exchange program (ITEP) ». Il autorise les échanges temporaires. En plus de travailler dans le champ IT et d'être un excellent élément, le personnel concerné doit être prévu pour occuper des responsabilités managériales et être d'un niveau GS 11 ou équivalent. Les détachements peuvent être de 3 à 12 mois et peuvent être poursuivis encore 1 an. Ce programme pilote ne peut pas accueillir plus de 10 salariés en même temps.

L'army school of information technology de Fort Gordon travaille sur des coopérations avec le secteur privé dans le cadre du DoD training with industry program (TWI). A travers ce programme, l'Army a envoyé 4 militaires par an à des entreprises (Cisco, General Dynamics et Microsoft). Le même programme de rotation existe pour la Navy. Il existe enfin le Intergovernmental Personnel act (IPA) mobility program qui offre des rotations au sein des agences fédérales et avec l'industrie.

Intitulé		Développement des échanges entre public et privé
Descriptif	Le DoD américain met en place un programme pilote autorisant les échanges temporaires entre public et privé.	
Résultats	Inconnus.	
Contraintes associées	Bonne coordination avec les entreprises privées. Cadre juridique nécessaire.	
Intérêt	Varier l'expérience du personnel. S'enrichir des expériences dans le privé. Adapter le niveau de compétence.	

B25-4 : accompagner la transition professionnelle des militaires

CompTIA, une organisation destinée à développer l'activité IT, a lancé « Armed for IT Careers » qui propose un cursus de transition pour le personnel militaire¹⁵⁴.

¹⁵⁴ <http://armedforitcareers.org/>



L'organisation propose aux anciens militaires de les accompagner dans leur transition vers le secteur privé. Elle propose 7 certifications¹⁵⁵ appuyées par une liste conséquente de partenaires. La *roadmap* « information security » propose une liste de certifications « jalons » du niveau débutant au niveau expert.

Figure 42. Exemple de certification niveau "débutant", par CompTIA

Information Security

Average Salary*: USD \$103,314 | Current Demand: High

Design and implement security measures that thwart attacks on computer systems, networks and data.

Mouse over the certification name for a full description of the exam. Click on the certification name to get more information.

BEGINNER/NOVICE

- CompTIA A+
- Microsoft Technology Associate: Security Fundamentals

Start with CompTIA A+ and 2 or 3 other certifications from this list.

Intitulé	Accompagner la transition professionnelle des militaires
Descriptif	CompTIA, une organisation destinée à développer l'activité IT, a lancé « Armed for IT Careers » qui propose un cursus de transition pour le personnel militaire.
Résultats	Inconnus.
Contraintes associées	Coûts.

¹⁵⁵ http://www.digitalgovernment.com/media/Knowledge-Centers/asset_upload_file555_2024.pdf

Intérêt	Valoriser l'expérience acquise dans le secteur public. Faire des vétérans des ambassadeurs du secteur public.
---------	---

B26 : valoriser par le salaire

Les salaires du secteur de la cybersécurité sont amenés à augmenter dans le privé. Les récentes cyberattaques et leur impact considérable (Target, Code Space) se comptant en milliards de dollars de pertes, voire en dépôt de bilan pur et simple, encouragent les entreprises à investir massivement dans la cybersécurité, au point d'accorder des salaires surévalués à des profils jeunes et sans expérience. Face à cette offensive des entreprises du secteur privé sur le marché du travail, difficile pour les acteurs publics de s'aligner sur cette inflation des salaires. Ainsi, si les acteurs publics peuvent certainement prévoir des mécanismes garantissant un très bon salaire, ils peuvent également avancer d'autres arguments tout aussi intéressants.

Les salaires élevés du secteur privé peuvent en effet être perçus comme de véritables « sursalaires compensateurs », permettant de retenir des profils ne bénéficiant pas de conditions de travail avantageuses, ou de stabilité de l'emploi. La stabilité, les horaires fixes ou en rotation, les conditions de travail agréables peuvent être des arguments permettant de compenser le manque à gagner lors d'une transition du secteur privé au secteur public. Ces avantages, couplés à ceux de l'attrait pour un poste unique dans les rangs de l'Etat, sont de solides arguments pour renforcer l'intérêt pour ces métiers, et retenir les talents se sentant valorisés par la nature même de leur emploi.

- **Le programme « critical skills retention bonuses » (CSRB) et le « National Defense Authorization Act for fiscal 2015 » du Department of Defense**

A l'origine, il s'agit d'une mesure financière¹⁵⁶ de rétention destinée à certains militaires dotés de compétences clés, mais éligibles à la retraite à l'issue de 25 années de service. Ces « compétences militaires critiques » sont spécifiquement identifiées, et leur rétention justifie l'activation d'une prime, bonus ou « salaire spécial » (*special pay*) forfaitaire allant de 25 000\$ à 35 000\$ en échange de trois années supplémentaires de service. Ce programme est en vigueur pour l'US Army¹⁵⁷, les marines¹⁵⁸ ou encore la Navy¹⁵⁹. Si, dans le principe, l'application d'un bonus de salaire reste un argument majeur de rétention des effectifs, l'application du CSRB à la cybersécurité est restée très rare au sein de l'armée américaine.

¹⁵⁶ <http://usmilitary.about.com/od/armybonuses/1/blcritskillbonu.htm>

¹⁵⁷ <http://www.armyreenlistment.com/csr.html>

¹⁵⁸ <http://www.marines.mil/News/Messages/MessagesDisplay/tabid/13286/Article/165967/fy15-critical-skills-retention-bonus-csr-program.aspx>

¹⁵⁹ <http://www.public.navy.mil/bupers-npc/enlisted/community/specwarops/Documents/CSRB%20Guidelines%20FEB2014.pdf>

Notons que le « National Defense Authorization Act for fiscal 2015 »¹⁶⁰ prévoit d'épauler, en cas de besoin, le DoD en matière de recrutement de talents « cyber ». Le document prévoit en effet que le DoD audite ses besoins, et indique d'ici 2015 au regard de l'état de son effectif cybersécurité, si le déblocage de fonds à des fins de primes, bonus et augmentations de salaires est nécessaire à des fins de rétention du personnel.

Selon Tim Kane, dans son ouvrage "Bleeding Talent: How the US Military Mismanages Great Leaders and Why It's Time for a Revolution"¹⁶¹, le CSRB aurait bien trop coûté à la communauté (un demi-milliard de dollars) pour un taux de rétention non-prouvé. Selon l'auteur, la quasi-totalité des profils ayant bénéficié de ce large bonus comptait déjà se réengager pour quelques années supplémentaires.

¹⁶⁰ <http://www.armed-services.senate.gov/imo/media/doc/SASC%20NDAA%20markup%20release%2005-23-14.pdf>

¹⁶¹ "Bleeding Talent: How the US Military Mismanages Great Leaders and Why It's Time for a Revolution" Palgrave Macmillan, 11 déc. 2012 - 288 pages

- **Le Department of Homeland Security (DHS) “Cybersecurity Workforce Recruitment and Retention Act” de 2014**

“When we get good people, we can generally keep them.”

Peter Gouldmann, directeur du “information risk programs” du State Department’s Office of Information Assurance¹⁶²

Le State Department dispose d’un « *retention bonus program* » lui permettant d’attribuer des bonus et salaires compétitifs avec le privé, afin d’attirer et de conserver les talents en matière de cybersécurité. Même constat pour le Department of Defense ou la NSA qui peuvent embaucher et retenir des profils de haut vol, grâce à des salaires compétitifs avec le privé.

Un projet de loi¹⁶³ a été déposé en ce sens en 2014 afin d’étendre ce système très avantageux au Department of Homeland Security¹⁶⁴. Le « *DHS Cybersecurity Workforce Recruitment and Retention Act of 2014, S.2354* », toujours en attente de vote du Sénat.

En contrepartie, le DHS devrait faire état chaque année de la mise en œuvre concrète du programme, afin de s’assurer de la transparence des processus de recrutement¹⁶⁵.

- **Le Calculateur de salaire du « MeriTalk Cyber Security Exchange (CSX)”, interface public/privé¹⁶⁶**



MeriTalk est chargé de favoriser les échanges entre secteur public et secteur privé afin d’améliorer les performances des systèmes d’information gouvernementaux américains. Au nombre de ses missions, la cybersécurité tient un rôle majeur car d’actualité. Le « MeriTalk Cyber Security Exchange (CSX) » est une communauté dite « verticale » d’acteurs de la cybersécurité à l’échelle fédérale, ayant pour objectif d’améliorer les échanges public-privé et de développer les bonnes pratiques. A travers le CSX, MeriTalk fournit des applications pratiques et concrètes, à l’image de son “Calculateur de salaire”. L’application est évidemment un outil de communication majeur. Elle propose aux candidats ou aux profils souhaitant évoluer, d’estimer le salaire qu’ils méritent selon leur formation, leurs certifications et leur zone géographique en temps réel.

A CYBER SECURITY PROFESSIONAL WITH YOUR QUALIFICATIONS CAN EXPECT TO MAKE

\$129,913

PER YEAR.

¹⁶² <http://www.fedtechmagazine.com/article/2014/06/should-cybersecurity-workers-get-bonuses>

¹⁶³ <https://beta.congress.gov/bill/113th-congress/senate-bill/2354>

¹⁶⁴ <https://beta.congress.gov/113/crpt/srpt207/CRPT-113srpt207.pdf>

¹⁶⁵ <http://www.hsgac.senate.gov/media/majority-media/committee-reports-legislation-to-enhance-dhs-cyber-personnel-authorities>

¹⁶⁶ <http://www.meritalk.com/csx/calculator>

Véritable produit d'appel, le Calculateur de salaire saura séduire tous les salariés s'estimant « mal payés ». Il permet également aux acteurs, grâce à la base de données l'appuyant, de connaître les prix du marché.

HELP IMPROVE OUR CALCULATOR

Does this match your current salary? (+/- 10K)

Yes No Not currently working as a Cyber Professional

Intitulé		Valoriser par le salaire
Descriptif	Ces programmes autorisent une augmentation de salaires pour la rétention des « compétences critiques »	
Résultats	Contestés.	
Contraintes associées	Coûts. Risques d'abus : certains profils n'auraient pas eu besoin de cette prime pour rester en poste. Fiabilité des données.	
Intérêt	Conserver les profils talentueux. Rivaliser avec le secteur privé. Séduire les salariés qui s'estiment mal payés. Favoriser la collecte de données afin de connaître les prix du secteur privé	

B27 : créer une communauté

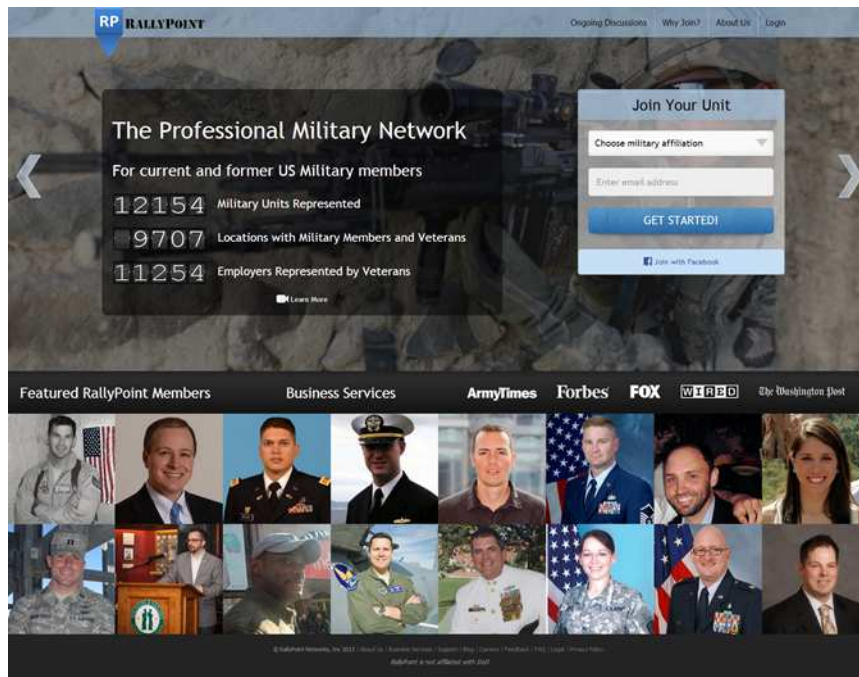
- **Le réseau social, l'exemple de Rally Point**

Rally Point, surnommé le « LinkedIn des militaires » américains, est un réseau professionnel à destination des militaires en service et vétérans.

Figure 43. Rally point, le LinkedIn de l'armée américaine


The screenshot displays the Rally Point website interface. At the top, there is a blue banner for 'The Military's Professional Network' with a sign-up form including a dropdown for 'Choose military affiliation', an 'Enter email address' field, and a 'JOIN YOUR UNIT!' button. Below the banner, a navigation bar includes categories like 'Military Discussions', 'Employment & Transition', 'Post-Military Life', and 'General Interest'. The main content area features 'Most recent discussions' with several threads, each showing a question, the author, date, and response/vote counts. A sidebar on the right titled 'Want input from the community?' contains 'Start a Discussion' and 'Trending Discussions' with various topics and their respective response counts. At the bottom, a 'Popular Topics' section lists various military-related terms and their associated counts.


Ce réseau offre aux militaires, grâce à ses fonctionnalités et aux nombreuses mises en relation, la possibilité d'orienter leur carrière.



Rally Point permet également, grâce à des fonctionnalités classiques, la création d'un profil, le lancement de conversations, etc. Les militaires y exposent leur expérience, y posent leurs questions, se renseignent et découvrent ainsi de nombreuses opportunités de carrière. La cybersécurité n'est pas en reste et de nombreuses conversations portent sur les opportunités de carrière dans le domaine.

Figure 44. Exemple de conversation sur RallyPoint

25D Cyber Network Defender; Now open to all Soldeirs! 

SFC (Join to see), Fort Detrick, MD 

25D Specifications & Qualifications | STAR MOS | Reclassification | Options | SMAPP | MOS Conversion Bonus
 MILPER Message 14-085 establishes reclassification strategy for MOS 25D, Cyber Network Defender (CND). Soldiers serving in MOS 25D will protect against unauthorized activity in the cyberspace domain and perform assessments of threats and vulnerabilities within the network environment.
 Reclassification into 25D is available to all Soldiers regardless of their MOS strength listed on the current in/out call message.

For more information please visit the following link:
<http://www.armyreenlistment.com/reclass-25d.html>

Avec RallyPoint, c'est l'esprit de communauté et de corps qui est renforcé. RallyPoint constitue également une vitrine considérable pour l'armée américaine. Enfin, la mise en relation de différents profils permet une meilleure circulation de l'information, une meilleure visibilité sur les opportunités de carrière, mais aussi un recrutement plus qualitatif.

Le réseau social d'entreprise reste enfin une option extrêmement intéressante pour favoriser le partage d'information et la création d'une communauté. A l'image de Steria, intégrer cette logique relationnelle au sein de l'entreprise permet de créer une logique de corps et d'affirmer la cohésion d'une équipe.

- **La communauté de pratique, l'exemple du CSIAC**

Ces communautés permettent aux professionnels de « réseauter » et d'échanger. Elles peuvent être internes¹⁶⁷ ou externes. Le DoD américain a ainsi mis en place le CSIAC (Cyber Security & Information Systems Information Analysis Center) qui est issu de la fusion de plusieurs dispositifs existants. Il est géré par le Defense Technical Information Center (DTIC).

Le portail propose notamment :

- Des forums de discussions thématiques (accessibles sur inscription à des utilisateurs étrangers) ;
- Une base documentaire sur la cybersécurité (études, bonnes pratiques...)
- Des webinars et podcasts ;
- L'accès à différents outils et bases de données.

- **Créer une communauté de valeurs, l'exemple de Symantec**

“We believe that involved, engaged employees are happier and more satisfied, and that communities in which Symantec is located will be healthier and more vibrant because of our presence.”

Symantec

Afin d'attirer les profils ouverts d'esprit, mais aussi de combler les manques de talents en matière IT et cybersécurité, Symantec opte pour une vision corporate originale, axée sur la diversité et l'ouverture des profils recrutés. De la sorte, Symantec se dote d'une image positive éthique et humaine, attirant ainsi certains profils. La qualité de vie et les valeurs diffusées par la société semblent être des points clés de leur stratégie de rétention des talents.

La société met en avant la protection de l'environnement¹⁶⁸ ainsi que la protection et la promotion des droits de l'Homme¹⁶⁹ ; elle récompense elle-même également les employés allouant leur temps libre à l'accomplissement de tâches humanitaires.

¹⁶⁷ La société STERIA a ainsi mis en place un réseau social interne pour son équipe cybersécurité.

¹⁶⁸ http://www.symantec.com/content/en/us/about/media/environmental_policy_statement.pdf

¹⁶⁹ http://www.symantec.com/content/en/us/about/media/sym_human_rights_policy_statement.pdf

Figure 45. Article sur la semaine du volontariat de Symantec

Interns Volunteer Over 100 Hours During Symantec Intern Volunteer Week 2014

Created: 07 Aug 2014 • Updated: 07 Aug 2014



Monica Ipong

+1

1 Vote

Symantec. | Official Blog

LinkedIn reddit this! Tweet

Similar to Symantec's **Volunteer of the Quarter** initiative, which highlights and rewards employees who dedicate their time and talents to those in need, our University Relations Team hosts an **Intern Volunteer Week Competition**, July 19th through July 27th. Symantec strongly encourages employees to volunteer in their local communities, providing volunteer resources and opportunities. **We believe that involved, engaged employees are happier and more satisfied, and that communities in which Symantec is located will be healthier and more vibrant because of our presence.**

During Intern Volunteer Week, interns took on the challenge and **volunteered over 100 hours** at various non-profit organizations such as the **Humane Society Silicon Valley**, **Food for Lane County**, **Stanford Blood Center**, and various others mentioned below.

Symantec mise énormément sur sa capacité à attirer les profils atypiques. Une tâche relativement difficile, comme le rappelait Michel Van Der Berghe, Atos, en octobre 2013 : certains sont issus d'une culture plutôt anarchisante et sont rétifs à l'approche " *bassement mercantile* " des sociétés. " *Ils préfèrent souvent se regrouper plutôt que de rejoindre une société bien établie commercialement. Pour les attirer, il faut avoir déjà recruté un gourou, un guide dans lequel ils se reconnaissent* " ¹⁷⁰. La stratégie de développement de valeurs humanitaires de Symantec prend donc tout son sens, bien qu'élignée du cœur de métier de la société. Cette démarche se rapproche de celle adoptée par Lockheed Martin ¹⁷¹.

Intitulé	Créer une communauté
Descriptif	Ces différentes initiatives tendent à rassembler les professionnels de la cybersécurité grâce à des rencontres virtuelles ou des évènements réels
Résultats	Inconnus.
Contraintes	Fiabilité des profils. Risques d'image en raison du manque de contrôle des contenus. Quelques animateurs relativement disponibles sont nécessaires.

¹⁷⁰ <http://pro.01net.com/editorial/604212/les-hackers-nouveaux-chouchous-des-entreprises/>

¹⁷¹ <http://www.lockheedmartin.com/us/who-we-are/community/education.html>

associées	
Intérêt	Fédérer et animer la population « cybersécurité ». Favoriser la mobilité et l'échange

4.5. Formation et entraînement

B28 : favoriser les labs et l'auto-formation afin de stimuler l'innovation

Le « tutorat » ou « mentoring »¹⁷² et l'auto-formation sont deux concepts faisant appel aux ressources internes à des fins d'amélioration et de renforcement des compétences des salariés. L'auto-formation fait appel à l'émulation des connaissances par les salariés eux-mêmes, grâce à la liberté de recherche et de réflexion proposée, soutenue par la mise à disposition d'outils dédiés (labs, blogs, matériel). La stratégie de l'entreprise Steria en est l'illustration. La société propose des espaces de réflexion, véritables « laboratoires », où les salariés y sont libres d'innover. Elle propose également des environnements de tests des derniers produits du marché. De quoi stimuler l'innovation de ses experts en cybersécurité.

Intitulé	Favoriser les labs et l'auto-formation afin de stimuler l'innovation
Descriptif	Steria propose à ses salariés des espaces de réflexion, véritables « laboratoires », où les salariés y sont libres d'innover
Résultats	Très bons.
Contraintes associées	Coûts. Gestion du temps.
Intérêt	Favoriser l'innovation.

B29 : promouvoir le tutorat interne

Le « mentoring » permet aux effectifs en poste d'accompagner les nouveaux venus, qu'ils soient fraîchement recrutés ou en transition professionnelle.

¹⁷² <http://www.sans.edu/research/management-laboratory/article/horwath-421-leader>

Les pratiques de gestion prévisionnelle des emplois, des effectifs et des compétences (GPEC) dans les collectivités territoriales¹⁷³ peuvent également être sources d'informations et de pratiques innovantes. Les collectivités organisent en effet des bourses internes à la mobilité, des stages d'immersion professionnelle à destination des agents déjà en poste, pour acquérir de nouvelles compétences ou découvrir de nouveaux métiers auprès d'autres services. Pour les nouveaux arrivants, un parcours d'intégration est prévu ; les plus anciens devenant les tuteurs des nouveaux. Ces tutorats sont de plusieurs ordres : tutorats d'intégration suite à l'activation d'un mécanisme de mobilité interne, ou tutorats d'expertise permettant la transmission d'une compétence pointue, toujours en interne entre agents.

Intitulé	
Le tutorat entre collègues	
Descriptif	Les collectivités organisent des bourses internes à la mobilité et des stages d'immersion professionnelle à destination des agents déjà en poste.
Résultats	Inconnus.
Contraintes associées	Gestion du temps.
Intérêt	Valoriser les profils internes. Economiser le coût d'un formateur externe. Favoriser la création de liens.

B30 : faire de la formation continue une récompense et un moteur de mobilité interne

Symantec¹⁷⁴ présente une approche globale valorisant l'employé et ses compétences. Symantec défend le concept de « talent management ». Selon l'éditeur de logiciels de sécurité, cultiver et stimuler les compétences des employés permet une meilleure compétitivité sur le marché. Elle souligne que sa valeur ajoutée est de disposer de salariés performants. En ce sens, elle propose un système de formation relativement complet, continu, jalon accessible à chaque étape de la carrière. Cette

¹⁷³ Les pratiques de gestion prévisionnelle des emplois, des effectifs et des compétences (GPEC) dans les collectivités territoriales http://www.cnfpt.fr/sites/default/files/etude_GPEC_0.pdf

¹⁷⁴ http://www.symantec.com/corporate_responsibility/topic.jsp?id=talent_management

formation accrue répond à un double objectif : satisfaire le salarié tout en l’orientant vers les compétences dont la société a besoin pour répondre à une demande, se réorienter sur le marché, innover. L’avantage de cette pratique est de fournir au salarié une formation à jour des réalités du marché du travail.

Si le système de formation est ouvert à tous les salariés, Symantec réserve les formations de talents clés aux profils les mieux notés durant l’année écoulée. La formation intervient ici comme un produit extrêmement qualitatif, réservé aux meilleurs. A l’issue de cette formation-récompense, ces salariés de haut vol pourront envisager plusieurs options de mobilité.

Faire de la formation continue une récompense et un moteur de mobilité interne	
Intitulé	
Descriptif	Symantec propose un système de formation relativement complet, continu, accessible à chaque étape de la carrière.
Résultats	Inconnus.
Contraintes associées	Rétention des talents en interne.
Intérêt	Favoriser la mobilité. Rétention des talents en interne.

B31 : animer un centre de formation et d’entraînement mutualisé

Le National Initiative for Cybersecurity Careers and Studies (NICCS) américain propose un environnement d’entraînement et de formation baptisé « FedVTE » (Federal Virtual Training Environment)¹⁷⁵. Cette bibliothèque en ligne, qui compte plus de 30 000 utilisateurs inscrits, offre 800 heures de formation¹⁷⁶, 150 démonstrations et un environnement de simulation technique¹⁷⁷.

L’environnement est aujourd’hui utilisé par de très nombreux départements et agences fédéraux, dont le DoD.

¹⁷⁵ <http://niccs.us-cert.gov/training/fedvte>

¹⁷⁶ <http://niccs.us-cert.gov/sites/default/files/documents/files/fedvte-courselist.pdf>

¹⁷⁷ <https://www.fedvte-fsi.gov/Vte.Lms.Web>

A noter que les États-Unis disposent de plus environnements de simulation et d'entraînement « cyber ». Lancé par la DARPA, et réalisé par Lockheed Martin pour un budget de plus de 500 millions de dollars, le DoD dispose notamment du National Cyber Range dont la gestion a été transférée en octobre 2013 au département DT&E (developmental test and evaluation) du TRMC (Test Resource Management Center).

Figure 46 : Saisie d'écran de FedVTE : un exemple de quizz

Assessment results – QUIZ - ARP

Export (csv) Print

Stats

Passing Score: 40 / 50
 Pass: 40 / 50
 Fail: 10 / 50
 Pass Ratio: 80 %
 Total: 50 / 50

Assessment results – QUIZ - ARP

Date: 06/11/2012
 Score: 80.0 % (40 / 50)
 Passing Score: 80 %
 Status: Passed

Questions


#	Question	Points	Correct Answer(s)	Actual Answer(s)	Correct?
1	When a router broadcasts an ARP request to find the MAC address associated with a particular IP address, it should receive the following in reply:	10	A single ARP reply packet from the host with the correct IP address.	A single ARP reply packet from the host with the correct IP address.	Yes
2	Until Ethernet switches cache the MAC address of a host, they repeat IP packet transmissions on all hosts, just like Ethernet hubs.	10	True	True	Yes
3	To use ARP spoofing to launch a man-in-the-middle attack and intercept traffic between a target host on the LAN and the network gateway, an attacker needs to know:	10	The IP and MAC addresses of the gateway and target host	Only the MAC and IP addresses of the target host	No
4	When an Ethernet switch's buffer memory is overloaded with MAC addresses, the switch typically refuses to forward any packets until timeouts clear the buffer.	10	False	False	Yes
5	In order to transmit a spoofed MAC address, an	10	Only a driver that permits	Only a driver that permits	Yes

QUIZ: ARP

Figure 47 : Saisie d'écran de FedVTE : un exemple de « bac à sable »

Ctrl-Alt to free mouse

Right-click for menu



Launchpad

Analyzing Log Files with Microsoft Log Parser and Splunk

This lab is an introduction to Microsoft Log Parser 2.2 and Splunk. Using these tools, you will be able to analyze logs from a compromised host after an attack has taken place.

It is important to note that you cannot always rely on the logs from a machine that has been compromised. Often an attacker will take measures to erase the log files or to eliminate the signs of his attack. The absence of log files can also be an indicator that an attack has taken place.


While you may not be able to rely on the logs that are resident on a compromised host, there is always the chance that an attacker has left some traces of his attack or of the activity that took place on the host. This is why Log Parser can be a useful resource when analyzing log files.

Log Parser is a free, command line tool from Microsoft that allows you to process log files using SQL-like queries. The Log Parser utility allows an investigator to read data from many different formats including XML, W3C, IIS, Event Logs (EVT), Registry Keys, and text to name a few. Log Parser will also format its output in a variety of different ways. Examples include XML, SQL tables and CSV. You can also send the output to a centralized Syslog server.

An additional feature of Microsoft's Log Parser includes the ability to adjust timestamps in log files. This is a very useful feature when you are comparing logs from different hosts that may be in different time zones or when the clocks are not synchronized.

After analyzing a web log file using the Log Parser command line tool the same file will be imported into Splunk for additional review. Splunk is an application that enables log searching and navigation in real time. A variety of input methods are supported including file import, syslog and SNMP. Logs, configurations, traps, alerts, and other messages can be captured, indexed, and rapidly searched using Splunk without the need for complicated SQL queries or regular expressions.

Your lab environment consists of 1 virtual computer system.



VTE-Launchpad
10.0.254.254

A Windows Server 2003 launchpad system on which you will install and use Microsoft's Logparser and Splunk. This system's hostname is VTE-Launchpad and its IP address is **10.0.254.254**

Adjusting timestamp...

> Installing Splunk

Figure 48 : Liste des cours proposés par la DISA dans FedVTE (par durée décroissante)¹⁷⁸

¹⁷⁸<http://fr.slideshare.net/jderienzo/disa-fed-vte-2014-training-sorted-by-duration-in-descending-order>

Hours	Title
45	Certified Ethical Hacker (CEHv6)
40	US-CERT TM Incident Handler
34	CCNA Security
32	CompTIA Security+ (SY0-301) Prep
	DISA ACAS Version 4.0
	DISA ACAS Version 4.6
	DISA HBSS Admin MR4 (2012 Version)
	DISA HBSS Admin MR5 (2013 Version)
	DISA HBSS Advanced MR4 (2012 Version)
	DISA HBSS Advanced MR5 (2013 Version)
	DISA Symantec Endpoint Protection 12.1
30	US-CERT TM Network Analyst
27	(ISC)2™ CISSP (R) Certification Prep Version 2
21	Certified Ethical Hacker (CEHv7)
	ISACA Certified Information Security Auditor
20	(ISC)2™ CISSP Certification Prep
	CompTIA A+ Prep
19	Mobile Security
18	ISACA Certified Information Security Manager
17	CompTIA Network+ Certification Prep
16	(ISC)2™ Systems Security Certified Practitioner
	DISA Vulnerability Management System (VMS)
	Windows Operating System Security
15	(ISC)2™ CISSP Concentration: ISSAP
	*(ISC)2 CISSP Concentration: ISSMP 2013
14	Penetration Testing
13	(ISC)2™ CISSP Concentration: ISSMP
	Emerging Cyber Security Threats (2010)
	NCSD TDP Information Security Fundamentals
12	(ISC)2™ CISSP Concentration: ISSEP
	*CompTIA A+ 220-801 Certification Prep
	Malware Analysis
11	Cyber Risk Management for Managers
	Cyber Risk Management for Technicians
	ISACA Certified Information Security Manager 2013
10	(ISC)2™ CAP (R) Prep
	Software Assurance for Executives
9	*Demilitarized Zone (DMZ) with IDS/IPS
	Cisco Network Security 1
	Cisco Network Security 2
	Linux Operating System Security
	Wi-Fi Communications and Security

Intitulé	
Création d'un centre de formation et d'entraînement mutualisé	
Descriptif	FedVTE est un centre d'entraînement et de formation en ligne proposant des formations sous forme de cours en ligne ou de quizz, mais aussi des environnements de simulation technique.
Résultats	30 000 utilisateurs inscrits, 800 heures de formation, 150 démonstrations, de nombreux exercices pratiques.
Contraintes associées	Disposer d'un environnement de simulation et concevoir des contenus adaptés.
Intérêt	Permet de démultiplier l'efficacité des formations et de toucher un public à moindre coût.

B32 : former et sensibiliser les élites

Le National Defense University, une institution fondée par le DoD dans le but de former les décideurs publics et privés aux problématiques nationales et internationales de sécurité, a créé dès 1988 une entité dédiée au management de l'information, le iCollege (Information Resources Management College). Au sein de cette entité, le CIIO Department (Cyber Information and Integrated Operations) propose des formations portant sur la sécurité de l'information, les stratégies gouvernementales en la matière ainsi que la place de l'information dans la planification et l'exécution des stratégies militaires. De nombreuses certifications sont délivrées parmi lesquelles « Information Systems Security standard », « National Security Systems standard for Risk Analysts » ou encore « Chief Information Security Officer »¹⁷⁹.

Ces formations sont réservées à certaines catégories : les fonctionnaires civils employés par les agences du DoD, les fonctionnaires fédéraux, étatiques ou locaux, les personnels du secteur privé dont la société est un sous-traitant du Ministère de la Défense ou de l'une de ses agences, les militaires d'active, opérationnels ou administratifs, ainsi que les réservistes de l'armée et les membres de la garde nationale. Ces formations sont gratuites pour les personnels du DoD, civils comme militaires, et

¹⁷⁹ NDU, iCollege, catalogue de formation 2014

coûtent de 10 750\$ pour un fonctionnaire à 16 900\$ pour une personne issue du secteur privé. Si le stagiaire justifie de 7 ans d'étude auparavant, la formation peut alors être diplômante (Master of Science), ce qui est relativement intéressant en termes d'évolution professionnelle.

Deux programmes s'intéressent particulièrement à la cybersécurité :

- Le Cyber Leadership (Cyber-L) Program

Ce programme s'inscrit dans une optique de partage de l'information entre les agences gouvernementales américaines, la communauté internationale et le secteur privé, le but étant de sécuriser, protéger et défendre le capital informationnel d'une entité. Les matières abordées sont structurées autour de quatre « compétences clés » : Cyber Governance, Privacy and Civil Liberties, National Security in Cyberspace, Inter-Agency Collaboration and Cyber Workforce Protection, Global Cyber Commerce and Technology.

- Le Cyber Security (Cyber-S) Program

Cette formation beaucoup plus pratique est destinée aux RSSI, officiers SSI des agences gouvernementales et Risk managers.

Cette formation met notamment l'accent sur :

- Des exercices stratégiques, impliquant la conception et l'utilisation de stratégies, de plans, de politiques et de procédures de cybersécurité ;
- Le développement de compétences en matière d'analyse de risque, de *security awareness*, de réponse à incident, de continuité et reprise d'activité ;
- Le partage de l'information entre les différents acteurs du cyberspace ;
- La communication vis-à-vis des décideurs civils et militaires, grâce à des méthodes et éléments de langage uniformisés.

Cette formation, qui peut également être réalisée à distance, a pour avantage d'accueillir des personnels du secteur public et du secteur privé, favorisant ainsi le dialogue entre ces deux mondes, ce qui favorise du même coup le partage de retours d'expérience. Parallèlement, des formations en management sont proposées pour tous les niveaux d'expérience (junior, expérimenté, senior) afin de doter les stagiaires des « soft skills » nécessaires pour le management de leurs équipes.

Intitulé	
Formation et sensibilisation des élites	
Descriptif	Le National Defense University a mis en place deux programmes de formation en cybersécurité ciblant un public de décideurs publics et privés.
Résultats	Très bons résultats
Contraintes associées	Corps enseignant et contenus.
Intérêt	Permet à des décideurs de se doter de compétences additionnelles en sécurité, voire d'effectuer une transition vers des emplois à dominante « cyber ». Facilite la création d'une communauté « cyber ».

B33 : mettre en place un centre de formation pour les personnels internes et externes

Airbus Defence & Space (ex-Cassidian), a mis en place depuis 2 ans un centre de formation continue, le CyberSecurity Training Centre. Ce centre, dont les prestations sont également vendues à des sociétés tierces, propose des programmes de formation à destination de ses employés¹⁸⁰. Une cinquantaine de cours sont proposés et sont adaptés à plusieurs niveaux de compétences (débutants professionnels, experts et formateurs). Dispensés en Allemagne, en France et au Royaume-Uni pour les différentes entités du groupe, ces cours sont répartis dans quatre domaines de formations :

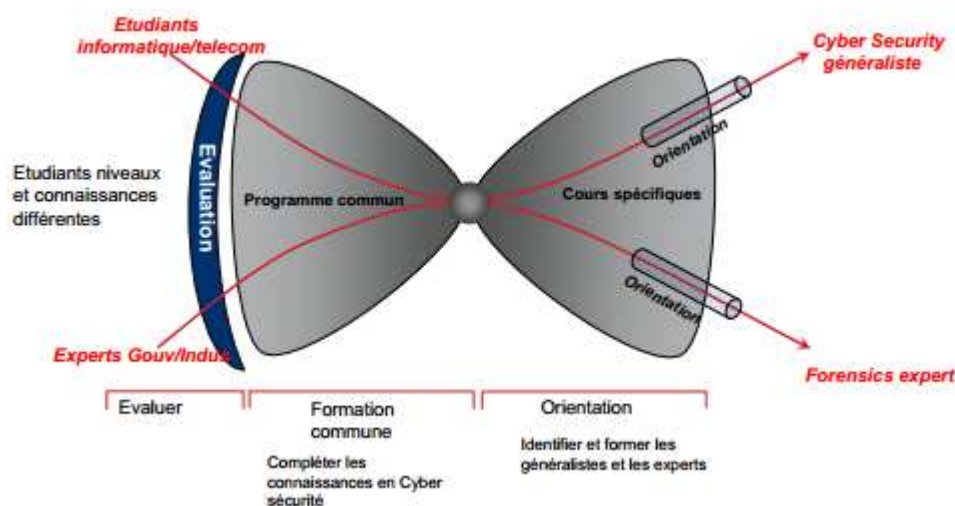
- Panorama : ce domaine propose une sensibilisation aux enjeux cyber, tant sur les aspects techniques que juridiques. Cette formation s'adresse plus aux débutants, en particuliers aux dirigeants qui ont besoin d'un seuil de connaissance minimal en cyber ;
- Prévention : destiné à enseigner les méthodes de protection des systèmes d'information, ce domaine s'adresse aux personnels ayant besoin de maîtriser les normes et les politiques de cybersécurité ;

¹⁸⁰ <http://www.defenceandsecurity-airbusds.com/fr/web/guest/cybersecurity/cybersecurity-training-centre>

- Détection : ce domaine de formation s'adresse aux personnels des SOC (opérateur, analyste, administrateur, etc.) dans le but de les former à la détection et à l'alerte en cas de cyberattaques ;
- Réaction : le dernier domaine est destiné aux équipes dédiées à la sécurité des SI, afin de les former et de maintenir à jour leurs compétences en matière de réponse à incident et de forensics.

A l'issue des formations théoriques, les participants sont évalués à travers des scénarios dont le déroulement se fait au sein d'une plateforme virtuelle. A l'issue de cette formation, les personnels dont le potentiel a été repéré pour intégrer les équipes cyber peuvent être détectés grâce à un système d'évaluation, qui passe notamment par l'organisation d'un challenge interne : ainsi, une personne appartenant au support informatique du groupe ou à un des métiers peut intégrer les équipes cyber.

Figure 31. CyberSecurity Taining Center : Evaluer, Former et Orienter¹⁸¹



Ce centre de formation permet de répondre au besoin du groupe dans la mesure où celui-ci assure la formation des personnels sur des compétences précises afin de les spécialiser ou de les maintenir en condition en fonction des besoins internes, qui se base sur une matrice des compétences qui décrit les niveaux de connaissances exigés pour chaque poste. Il faut noter que ces formations sont aussi des prestations proposées aux personnels extérieures à l'entreprise, à l'image de la formation sur la sécurité des SCADA et développées en partenariat avec Siemens pour les aspects métiers.

Northrop Grumman propose le même genre de formation¹⁸², destiné à la fois à ses personnels mais aussi à ceux du DoD, du renseignement américain et des agences fédérales dans leur ensemble. Les programmes sont d'une difficulté graduée et sont de courte durée (entre 2 heures et 4 jours). Les cours sont destinés pour moitié aux décideurs (Fundamentals and Hands-on Labs ou Cybersecurity for Business Developers par exemple) et pour moitié aux techniciens (Cyber Architecture Analysis &

¹⁸¹ <http://forumatena.org/LB47/07juin2012/sponsor-CASSIDIAN.pdf>

¹⁸² http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/CyberAcademy_overview.pdf

Application par exemple). Le but étant de sensibiliser l'ensemble du personnel et de former en continu les spécialistes :

Figure 49. Cyber Academy Training Framework



La NSA a également développé un centre de formation destiné en premier lieu à son propre personnel¹⁸³. Le College of Cyber propose en effet de la formation continue et de l'entraînement pour les personnels de l'agence, spécialistes et non-spécialistes de la cyber, mais aussi au personnel du Cyber Command. Le centre propose un catalogue de formations auxquelles les employés peuvent s'inscrire. Mais le centre est également ouvert aux étudiants des écoles militaires mais aussi des écoles privées et des universités destinés à intégrer le DoD, la NSA, la police ou le renseignement.

Intitulé	Mettre en place un centre de formation continue destiné aux personnels internes et externes
Descriptif	Dispense de cours pour les personnels internes à l'entreprise et externes à celles-ci pour tout niveau, de débutant à expert
Résultats	Bons résultats
Contraintes associées	Difficulté de maintenir à niveau l'ensemble des personnels compte tenu de la rapidité de l'évolution technologique

¹⁸³<http://www.military.com/education/2014/08/29/the-nsas-school-of-cyber.html>

Intérêt	Permet à l'entreprise de former sa masse salariale à ses besoins
---------	--

5. Analyse forces / faiblesses de la Défense par rapport à l'emploi « cyber »

L'objectif de ce chapitre est de confronter les bonnes pratiques identifiées au chapitre précédent aux caractéristiques propres de l'environnement défense, à travers une analyse SWOT, et ainsi d'orienter les recommandations qui seront formulées par la suite.

5.1. Aperçu global

Recrutement	
<p>Forces :</p> <ul style="list-style-type: none"> ▪ Excellente image en tant qu'employeur (équité, formation, sens de l'engagement). ▪ Intérêts des missions proposées. ▪ Rémunérations compétitives en début de carrière ou sous contrat. ▪ Capacité avérée à détecter et transformer des talents internes. 	<p>Faiblesses :</p> <ul style="list-style-type: none"> ▪ Cadre de travail à l'image rigide. ▪ Processus de recrutement de la fonction publique peu adapté et pas de processus spécifique. ▪ Organisation du recrutement pour la Défense peu adapté aux besoins cyber. ▪ Difficultés à proposer un parcours de carrière aux contractuels. ▪ Passage forcé par une première carrière de « Transmetteur » pour certains postes. ▪ Réservoir potentiel limité à la main d'œuvre française et disposant d'un casier judiciaire vierge. ▪ Désignation des postes ouverts souvent différente de celle du privé.
<p>Menaces :</p> <ul style="list-style-type: none"> ▪ Concurrence des entreprises qui ont, pour certaines (industriels de Défense notamment), déjà anticipé la tension du marché des ressources humaines cyber. 	<p>Opportunités :</p> <ul style="list-style-type: none"> ▪ Problématiques organisationnelles et processus identifiées par l'axe 3 du Pacte Cyber Défense et faisant l'objet d'un plan d'action à 2 ans. ▪ Offre de formations adaptées aux besoins cyber en constante augmentation, aussi bien quantitative que qualitative. ▪ Image du « cyber-soldat » claire et attrayante restant à construire. ▪ Retentissement d'un futur cyber-challenge national et public potentiellement plus important que celui des challenges privés. ▪ Réservoir important de personnels qualifiés télécoms et services informatiques.

Formation

Forces :

- Un dispositif de formations initiales et continues, performant et adaptable.
- Des infrastructures d'entraînement existantes et d'excellent niveau.
- Une capacité à envoyer en formation dans le secteur privé.

Faiblesses :

- Pas de tests spécifiques cyber préalables aux mises en formation.
- Pas de cursus de formations initiales dédié aux emplois cyber.
- Nécessités d'adaptation et de remise à jour très fréquente des formations contraires à l'inertie de processus administratifs de validation des parcours de formation.
- Peu de structures d'entraînement (sandbox) décentralisées.
- Pas de label de formations reconnu dans le privé.
- Peu de coopérations internationales.
- Peu de coopérations « public-privé ».

Menaces :

- Pas de cursus LIO contrairement à plusieurs Etats étrangers.

Opportunités :

- Les axes 3,4 et 6 du Pacte Défense Cyber ainsi que la qualité des infrastructures du Pôle d'excellence en cyber défense de Bretagne devraient permettre de répondre sous 2 ans aux problématiques de cursus dédiés et de création d'une offre nationale de formation.

Gestion Des Carrières & Compétences

Forces :

- Une capacité d'anticipation des besoins RH supérieure aux entreprises privées.
- Une grande variété des emplois cybers offrant une multitude de possibilités aux gestionnaires de carrières.

Faiblesses :

- Pas de référentiel des emplois dédiés.
- Pas de gestionnaire RH spécialisé ou dédié au pilotage des ressources cybersécurité.
- Pas de cursus de carrière dédié à la cybersécurité.
- Pas de dispositif de rétention interne des talents.
- Des salaires inférieurs au secteur privé après 4 ans d'expérience.
- Difficultés à proposer une progression attractive aux contractuels.

Menaces :

- Une variété et une évolutivité des besoins, en compétence cyber difficile à maîtriser.
- Une gestion RH des réserves perfectible, et dont la qualité pourrait nuire à la volonté de développer la réserve, affichée par l'axe 6 du Pacte de Cyber Défense (Action 48).

Opportunités :

- Une volonté affichée par l'Axe 3 (Action 29) du Pacte de Cyber Défense de mieux utiliser les procédures de détachement de personnels permettant des mobilités inter-administrations.
- L'axe 3 ainsi que l'axe 1 (Action 6) du pacte de Cyber Défense devrait répondre au besoin de parcours professionnels dédiés.

5.2. Analyse détaillée

5.2.1. Recrutement aujourd'hui : forces et faiblesses

Ce paragraphe ne traite que du recrutement externe. La détection et la réaffectation des talents internes est traitée au chapitre « Gestion des carrières et compétences ».

La qualité d'une politique de recrutement repose sur ¹⁸⁴:

- Une identification fine des clients et de leurs besoins ;
- Une cartographie précise des sources d'approvisionnement en talents ;
- Un réseau de recrutement spécialisé et multicanal ;
- Une offre claire et attractive ;
- Un processus d'évaluation et de sélection adapté à chaque métier ;
- Un fort taux de sélection.

En matière de recrutement, le Ministère de la Défense dispose de plusieurs avantages concurrentiels majeurs sans liens avec la cybersécurité :

- Une diversité et un intérêt des missions particulièrement attractifs ;
- Une image d'employeur moderne et exemplaire. S'adressant avant tout à des populations jeunes, le ministère sait proposer un projet, ou une « étape de vie », alliant un engagement porteur de sens, un traitement équitable de tous les talents et des parcours de développement professionnel aux règles claires et établies ;
- Un réseau de recrutement étendu et multicanal (agences, sites internet, médias, prospection directe en écoles et salons, etc.) ;
- Une tradition d'adaptation permanente des services de recrutement aux besoins mouvants de la Défense (nouveaux métiers ou évolutions des compétences nécessaires, modification du format des armées, etc.), aux attentes des populations cibles, et aux outils de recrutement.

Ces forces traditionnelles sont complétées par des particularités liées à l'offre de postes cyber de la Défense :

- La promesse d'un équipement de pointe ;
- Des postes n'existant qu'au sein de la Défense (LIO, cybersécurité de systèmes d'armes, etc.).

Pour autant, il convient de remarquer que concernant le recrutement de compétences cyber, le Ministère de la Défense souffre aussi d'importantes faiblesses aux causes diverses :

- Tout d'abord la multiplicité des métiers de la cyber défense et leur complexité rend difficile leur maîtrise par les professionnels du recrutement, qu'ils soient d'ailleurs publics ou privés ;
- De plus, le réservoir de recrutement des armées est limité à une main d'œuvre française, au casier judiciaire vierge, alors même qu'au sein des cursus universitaires intéressant la cyber défense les étudiants étrangers sont pléthore.
- A ces étudiants souvent diplômés de l'enseignement supérieur, la majorité des postes proposés correspond à des postes de sous-officier et à des salaires de catégorie B. Les carrières SSI proposées aux militaires nécessitent souvent une première période plus

¹⁸⁴ Critères issus des entretiens avec des Associés et Directeurs des cabinets de recrutement Michael Page, Korn Ferry, et Mercuri Urval.

spécifiquement Telecom ou Réseau, et comportent toute une formation militaire importante pouvant déstabiliser un candidat. Il semble difficile d'expliquer à un jeune talent intéressé par une carrière en cyber défense que celle-ci ne commencera qu'après 6 à 7 ans minimum dans un régiment de Transmission, et à l'issue d'examens militaires (BSTAT SSIC par exemple).

- De surcroît, l'accès aux postes d'officier de carrière est presque exclusivement soumis au passage par une école de formation d'armée (ESM, EMIA, ENSIETA, Ecole de l'Air ou Ecole Navale) sans aucune garantie d'être employé en cyber défense. Si le « cyber soldat » doit, bien évidemment avant tout être un soldat, l'attente longue et l'incertitude sur le métier pour lequel il s'engage ne sont cependant pas de nature à favoriser les vocations.
- L'engagement de contractuels, qui permet souvent de contourner les difficultés précédemment évoqués en affectant directement un talent à un besoin tout en étant compétitif d'un point de vue salarial, ne permet cependant pas de lui proposer un parcours professionnel de qualité.
- Les systèmes de recrutement propre des armées, généralistes, sont pour leur part peu à même de détecter et de renseigner les talents qui se présentent à leurs portes. En théorie, un CERFA doit estimer le potentiel d'un candidat et l'orienter. Mais comment le recruteur peut-il être efficace sans tests dédiés à l'évaluation et à l'orientation d'un talent très technique, et sans cursus de carrière clair à lui proposer ?
- Il convient d'ajouter que le nom même des postes existants en cyber défense diffère souvent de leurs équivalents civils, ce qui est de nature à complexifier la compréhension par les candidats des postes ouverts, y compris aux contractuels¹⁸⁵. Le processus de diffusion des offres d'emploi cyber défense est lui aussi complexe (offres sur le site de l'ANSSI, emplois ouverts sur le site du ministère, etc.) et de nature à perdre les talents cyber intéressés par la Défense.
- Concernant enfin le recrutement de réservistes engagés et compétents, qui constitue l'un des piliers de la cyber défense nationale, aucun répertoire des postes à pourvoir et des compétences recherchés n'est disponible, et aucun test pour les évaluer n'est mis en place. Le candidat potentiel à la réserve doit par conséquent tout d'abord démontrer sa motivation en cherchant arduement une porte d'entrée puis convaincre oralement de sa compétence.

Fort de son adaptabilité et de son réseau aguerri de recruteurs, le Ministère de la Défense n'a cependant pas encore pris en compte toute la spécificité du recrutement cyber.

Si la satisfaction de certains besoins, liés à la SSI notamment, est maîtrisée et si certains canaux de recrutement (DGSE par exemple) sont habitués à travailler sur mesure, il reste cependant que le système doit encore être adapté.

L'exemple des sportifs de haut niveau de la Défense ou des médecins militaires, disposant d'un profil exceptionnel et d'un mode de recrutement ou de gestion de carrière adapté, montre que la Défense sait faire du recrutement « sur mesure » sur des volumes de plusieurs centaines de talents. Ces retours d'expérience peuvent probablement être sources d'inspiration quant aux adaptations possibles.

¹⁸⁵ Lors de notre étude, une liste des emplois « cybers » de la Défense a été remise à des chasseurs de tête afin de comparer les salaires proposés. Ces derniers n'ont souvent pas pu répondre, faute de comprendre le type de poste proposé.

5.2.2. Recrutement demain : menaces et opportunités

Le Pacte Cyber Défense a déjà clairement fait le constat d'un besoin futur grandissant en compétences cyber et proposé des mesures fortes. L'amélioration, dans les deux ans à venir, de l'offre de formation ainsi que la création d'un pôle d'excellence sont notamment de natures à améliorer le bassin de recrutement et la visibilité ou l'attractivité de l'offre d'emploi proposée.

La principale menace future pesant sur le recrutement de talents cyber par la Défense est par conséquent la concurrence accrue, notamment au niveau national.

En effet, alors que les volumes recrutés aujourd'hui par le ministère restent faibles (de l'ordre de quelques centaines par an) et sont pourvus relativement facilement avec une qualité satisfaisante, de nombreuses entreprises anticipent dès maintenant les futures tensions à venir sur le marché de l'emploi cyber.

La bataille pour les compétences étant le cœur de la compétitivité future de la cyber défense nationale, il convient de ne pas se limiter à la satisfaction actuelle des besoins et de rechercher une augmentation permanente du taux de sélection ou du bassin de recrutement.

En effet, la ressource créée par le développement de l'offre de formation française sera également ciblée par l'ensemble des concurrents du ministère sur le marché du recrutement cyber.

Les secteurs de l'industrie de Défense, de l'aéronautique, des télécoms ou de l'informatique sont aujourd'hui des domaines d'excellence nationale dont les contraintes de recrutement sont proches de celles du ministère. A cela s'ajoute également la concurrence d'autres administrations telle que le ministère de l'Intérieur ou celui de l'Economie et des Finances, dont les besoins en talents sont souvent similaires.

Ces concurrents ont pour la plupart aujourd'hui des atouts concrets à faire valoir (salaires proposés, carrières lisibles et spécialisées) avec lesquels le Ministère de la Défense aura du mal à être compétitif. Ces acteurs n'hésitent pas non plus à développer leurs réseaux de formation (Ecole 42 de Free) ou de recrutement spécialisés (ex : nomination d'un responsable et d'une équipe dédiée « relations écoles » chez Steria) disposant de processus de recrutement novateurs (ex : Steria Hacking Challenge).

Pour anticiper l'évolution de cette concurrence, la Défense a donc l'opportunité de :

- S'aligner sur la modernité des pratiques de recrutement cyber en cours, et dont le détail fait l'objet du chapitre recommandation de la présente étude (tests de recrutement spécialisés dont challenges, équipe de recrutement dédiée centralisant les besoins, recensement des besoins en ligne sous un portail unique) ;
- Mettre en valeur ses spécificités positives et développer une image claire et attrayante de ce que sont les cyber soldats d'aujourd'hui et de demain (ingénieurs DGA, SSI, LIO, etc.) et leurs missions. Sur ce point, l'expérience menée en 2007 par la Marine Nationale peut être prise en exemple. La direction du recrutement de la Marine Nationale avait à l'époque fait le constat que la nature du métier de Marin évoluait et qu'un fort besoin de recrutement concernait des personnels très au fait des nouvelles technologies, ayant soif d'aventure, et capables de rester

de longues périodes face à une interface homme machine. En conséquence, une frégate virtuelle avait été envoyée dans le monde virtuel phare de l'époque « Second Life », afin de rencontrer des candidats potentiels¹⁸⁶.

Figure 50. Illustration : La Marine recrute dans un monde virtuel



Cette initiative à très faible coût avait permis une communication efficace vis-à-vis des communautés visées puisque réalisée sous un mode convivial, très ciblées, et utilisant le bon vecteur de mise en relation.

5.2.3. Formation aujourd'hui : forces et faiblesses

S'agissant de formation, il convient de distinguer trois domaines différents :

- La formation initiale, destinée à créer un socle de compétences professionnelles, et pour laquelle les enseignements en cyber défense peuvent être centraux ou annexes (5 niveaux de formation ont été définis allant de la sensibilisation des généralistes à la formation d'experts) ;
- La formation continue, destinée à développer ou remettre à jour un socle de compétences professionnelles existant ;
- L'entraînement, destiné à améliorer la maîtrise de techniques ou des processus déjà enseignés.

¹⁸⁶ Vidéo en ligne à: http://www.dailymotion.com/video/x3jyho_la-marine-nationale-fait-escale-dan_news

La performance de chaque catégorie de formation repose sur l'articulation entre :

- Des objectifs opérationnels de la formation clairement exprimés ;
- Des compétences maîtrisées et formalisées pédagogiquement par des supports d'enseignement ;
- Un corps enseignant compétent ;
- Des infrastructures permettant l'apprentissage théorique comme la mise en situation.

Ces conditions sont aujourd'hui partiellement remplies par le Ministère de la Défense :

- Les objectifs opérationnels à assigner aux formations sont encore en cours de finalisation suite à la mise en place en 2013 d'une « démarche exploratoire d'expression de besoin pour la mise en place de capacités distribuées en matière d'expérimentation, de formation et d'entraînement de cyber défense ». L'ensemble des membres de la chaîne de cyber défense a été identifié et leurs besoins recueillis ;
- Les compétences maîtrisées et à développer ont été identifiées, ainsi que formalisées sous forme de supports pédagogiques destinés aux stagiaires des formations spécialisées de l'ETRS et de l'ESCC (DT CYBER, BSTAT SSIC, FA PAREFEU – TECHNICIEN SSIC – CONTROLE TECHNIQUE SSI – ADJOINT SI – SUPERVISION DE SECURITE – PRIMO FORMATEUR HIGYENE CYBER) ;
- Le corps enseignant est en cours de montée en puissance aux seins de l'ETRS, de l'ESCC ;
- La construction d'une infrastructure de formation et d'entraînement, érigé en priorité du pacte Cyber Défense, est elle aussi en cours. Fondée sur l'interconnexion de plates-formes spécialisées autour d'un noyau dur CALID – DGA/MI, elle dispose déjà d'une capacité de formation et d'entraînement des niveaux 1 (hygiène cybernétique) à 4 FA des personnels affectés en unités cyber. Equipée des systèmes de virtualisation Malice V2 et Hynesim (virtualisation de SCADA ou systèmes hybrides), l'infrastructure de formation et d'entraînement cyber de la Défense est potentiellement capable de reproduire tout type de situation sur tout type de SI ;
- A ce développement de contenus et d'infrastructures propres doit être ajouté la capacité de la Défense à envoyer ses personnels en formation externe, qu'elles soient privées ou dispensées par des armées alliées, chaque fois que de besoin.

Il convient donc de mettre en valeur qu'en matière de formation à la cyber défense, le Ministère de la Défense peut aujourd'hui compter sur des infrastructures modernes, un plan d'amélioration largement partagé et piloté par une entité unique, ainsi que sur un soutien politique affirmé.

En revanche, plusieurs points d'amélioration peuvent être identifiés :

- Comme toute spécialité complexe, la cyber défense demande une montée en compétence longue. Or si les formations d'adaptation disponibles sont de plus en plus nombreuses, aucune formation initiale n'y est pour l'instant consacrée ;
- L'impact d'une formation dépend grandement de l'unicité du niveau des stagiaires au premier jour de cours. Cependant, aucun dispositif de contrôle des connaissances et de préparation au stage n'est en place aujourd'hui ;

- L'évolution des connaissances cyber est bien plus rapide que pour la plupart des autres savoirs. Pour autant, les contenus des formations et la composition des cursus évoluent aujourd'hui au même rythme que pour les autres formations de la Défense. Plusieurs mois sont donc nécessaires entre la détection d'un besoin en formation et sa satisfaction. Sur ce point un cycle court d'adaptation des formations aux évolutions des besoins et des technologies semble indispensable ;
- De même, la plate-forme unique de formation en cours de développement permet la montée en compétence d'un noyau dur, mais n'est pas encore complétée par un réseau de d'infrastructures décentralisées d'entraînement (sand boxes). Un tel réseau semble pourtant nécessaire à l'atteinte d'une capacité de réaction opérationnelle de toute la chaîne cyber défense ;
- Enfin, les formations internes mises en place en par le Ministère de la Défense n'ont pas valeur de label civil ou interministériel. Elles sont créées et adaptées par rapports aux stricts besoins de la Défense, ce qui est en contradiction avec l'ambition ministérielle de constituer le cœur d'un dispositif public-privé national.

5.2.4. Formation demain : menaces et opportunités

L'évolution de la menace cyber, et donc des anticipations nécessaires, doit être considérée sous plusieurs angles :

- Géopolitique, pour anticiper les confrontations futures ;
- Militaire, afin d'évaluer l'évolution des rapports de forces ;
- Technologiques, afin d'investir sur les bons domaines de compétence qu'il s'agisse de recherche ou de formation.

L'évolution géopolitique et technologique de la menace est largement anticipée par le Livre Blanc et le Pacte de Cyber Défense dont les axes 3, 4 et 6 visent à rester compétitifs dans le domaine des compétences tout en disposant de structures d'entraînement de bon niveau.

Cette ambition vise clairement à faire de la France une « cible dure » dans le domaine cyber et à développer une capacité de protection et de réaction dissuasive même pour des attaquants disposant d'une capacité offensive développée.

Cependant, la LIO reste le parent pauvre de cette cyber stratégie française, notamment dans le domaine de la formation ou aucun cursus n'existe officiellement et aucune ambition n'est affichée. Si cette « pudeur » nationale est compréhensible de par les conséquences géopolitiques et juridiques de disposer d'une capacité offensive, il n'est reste pas moins que pour développer une formation performante (infrastructures, contenus, volumes formés), le ministère devra à terme faire le choix d'une ambition assumée dans le domaine offensif. Comme pour toute autre arme, disposer d'une capacité ne signifie pas l'employer à mauvais escient.

La limitation à une capacité de « contre-attaque », telle qu'exprimée actuellement, empêche le développement d'une doctrine offensive, et donc la capacité à former et entraîner pour améliorer notre rapport de forces vis-à-vis d'adversaires potentiels.

5.2.5. Gestion des carrières et compétences aujourd'hui : forces et faiblesses

La cyber défense est un domaine récent pour lequel, au moins en France, les carrières clairement identifiées et structurées n'existent pas encore de manière formelle. A ce titre, la création cette année 2014 du premier département spécialisé dans le recrutement cyber par le cabinet Michael Page traduit la jeunesse des métiers « cyber » autant que leur potentiel de développement.

Il s'agit donc avant tout d'un challenge futur à relever, pour lequel le Ministère de la Défense dispose aujourd'hui de forces évidentes :

- Sa capacité d'anticipation des besoins RH, développée suite à de nombreuses réformes des armées, est indéniable. La DRHMD et les DRH d'armée savent intégrer de nouveaux métiers, évaluer l'évolution des besoins quantitatifs et qualitatifs par anticipation, planifier la satisfaction de la demande. Sur ces points, la capacité de la Défense est sans conteste supérieure à celle de la totalité des entreprises privées mais aussi de la plupart des administrations ;
- La complexité et la diversité des emplois de la filière cyber est un frein à leur bonne gestion pour la plupart des employeurs. A contrario, la taille du Ministère de la Défense et sa capacité à gérer des carrières complexes en fait l'un des employeurs les plus aptes à offrir un véritable parcours professionnel, riche et diversifié ;
- La qualité des dispositifs de formation existant, telle qu'expliquée au chapitre précédent, est également une force indéniable pour faciliter la mobilité interne et permettre une gestion plus souple des carrières.

Pour autant, ces forces ne sont pas encore exploitées, et les atouts de la Défense restent trop souvent inexploités :

- Concernant la chaîne de gestion RH tout d'abord :
 - Le référentiel des emplois de la filière cyber n'existe pas, ce qui empêche par définition toute structuration formelle de carrières. Dès lors comment inciter des talents à s'investir dans une voie sans leur présenter les avenir qu'elle offre ;
 - Les gestionnaires RH des personnels cybers peuvent être spécialisés SI, Commandement-Renseignement, Armement, mais la filière « cyber » n'existant pas, ils n'appréhendent pas la chaîne de cyber défense comme un ensemble cohérent. Par conséquent ils ne peuvent pas non plus se spécialiser pour approfondir leur compréhension du besoin et de ses particularités ;
 - Le recours fréquent aux ressources contractuelles masque les lacunes internes et complexifie la mise en place d'une montée en puissance planifiée. Sur ce point les opérationnels confrontés à des besoins urgents prennent régulièrement la main sur une chaîne RH qui n'est pas encore prête à satisfaire leurs attentes. La satisfaction de court terme masque alors la problématique de long terme.

- Concernant ensuite les dispositifs RH disponibles :
 - A l'issue de 4-5 ans de carrières, le Ministère de la Défense ne sait pas aligner ses rémunérations proposées sur celles de la concurrence, et ce quelles que soient la qualité ou la rareté de la ressource. L'échelle des salaires du Ministère de la Défense allant de 1 à 10 (hors primes) favorise la cohésion, mais pas l'attraction des talents hors normes ;
 - En termes de carrière et de responsabilités, la Défense ne sait pas aujourd'hui offrir aux contractuels, même d'excellent niveau, une progression équivalente à celle des militaires de carrières ou des fonctionnaires civils du ministère.

Alors que les entreprises privées intéressées par la cyber sécurité (industriels Défense et Aéronautique, Telecoms, SSII) ont su réagir et s'adapter rapidement à la gestion des personnels cyber, la Défense affiche aujourd'hui un léger retard. Ce décalage est explicable, tant par la difficulté à structurer un ensemble cyber dans le contexte particulier du ministère que par le défi majeur de la déflation que relève actuellement la DRHMD. Il devrait donc être corrigé rapidement pour peu que les initiatives présentées par le Pacte de Cyber Défense soient menées à termes et même complétées.

5.2.6. Gestion des carrières et compétences demain : menaces et opportunités

S'agissant de gestion de carrières et de compétences, le succès repose majoritairement sur la capacité d'anticipation de tendances longues et sur la qualité de la planification.

Cette capacité de planification est particulièrement difficile à maîtriser pour les besoins cyber tant le domaine est récent et évolutif. Il convient cependant de noter que l'axe 3 du Pacte de Cyber Défense prévoit une montée en puissance de cette planification et propose également de mieux utiliser les dispositifs de détachement inter-administrations existant afin d'accroître la souplesse de gestion.

Cette dernière mesure est particulièrement importante car elle pourrait permettre de développer, et à terme de gérer de manière spécifique, un réservoir de managers cyber défense interministériel sur le modèle de la gestion interministérielle des hauts potentiels.

En revanche l'utilisation et de la gestion d'une réserve cyber, qui constitue un élément clé de la future capacité nationale de cyber défense (cf. action 48 du Pacte Cyber Défense), apparaît beaucoup plus inquiétante. En effet :

- La réserve cyber défense actuelle n'est qu'une réserve citoyenne, cantonnée à des tâches de réflexion et d'évangélisation. Ce choix de ne pas en faire un renfort opérationnel est compréhensible tant que les armées n'ont pas achevé la structuration de leur cyber défense. Il serait en revanche dommage de se passer de l'apport potentiel de talents nationaux une fois l'organisation en place pour les accueillir.
- La réserve actuelle des armées (toutes fonctions confondues) souffre d'une gestion particulièrement défailante au regard de nombreux autres exemples européens. Le recrutement des réservistes est effectué au coup par coup, sous l'impulsion des opérationnels, selon leurs besoins du moment et leurs connaissance directe des talents disponibles ;

- En outre, aucune étude globale du besoin en compétence devant être satisfait par des réservistes n'a été menée et aucun portail ne recense les besoins ou les postes ouverts.

Au regard des initiatives déjà prises par le Pacte de Cyber Défense cette création d'une réserve cyber opérationnelle organisée et régulièrement mobilisée apparaît clairement être une opportunité majeure, cohérente avec les savoir-faire disponibles et les contraintes budgétaire ainsi qu'avec la nécessité de fédérer une communauté nationale de cyber défense.

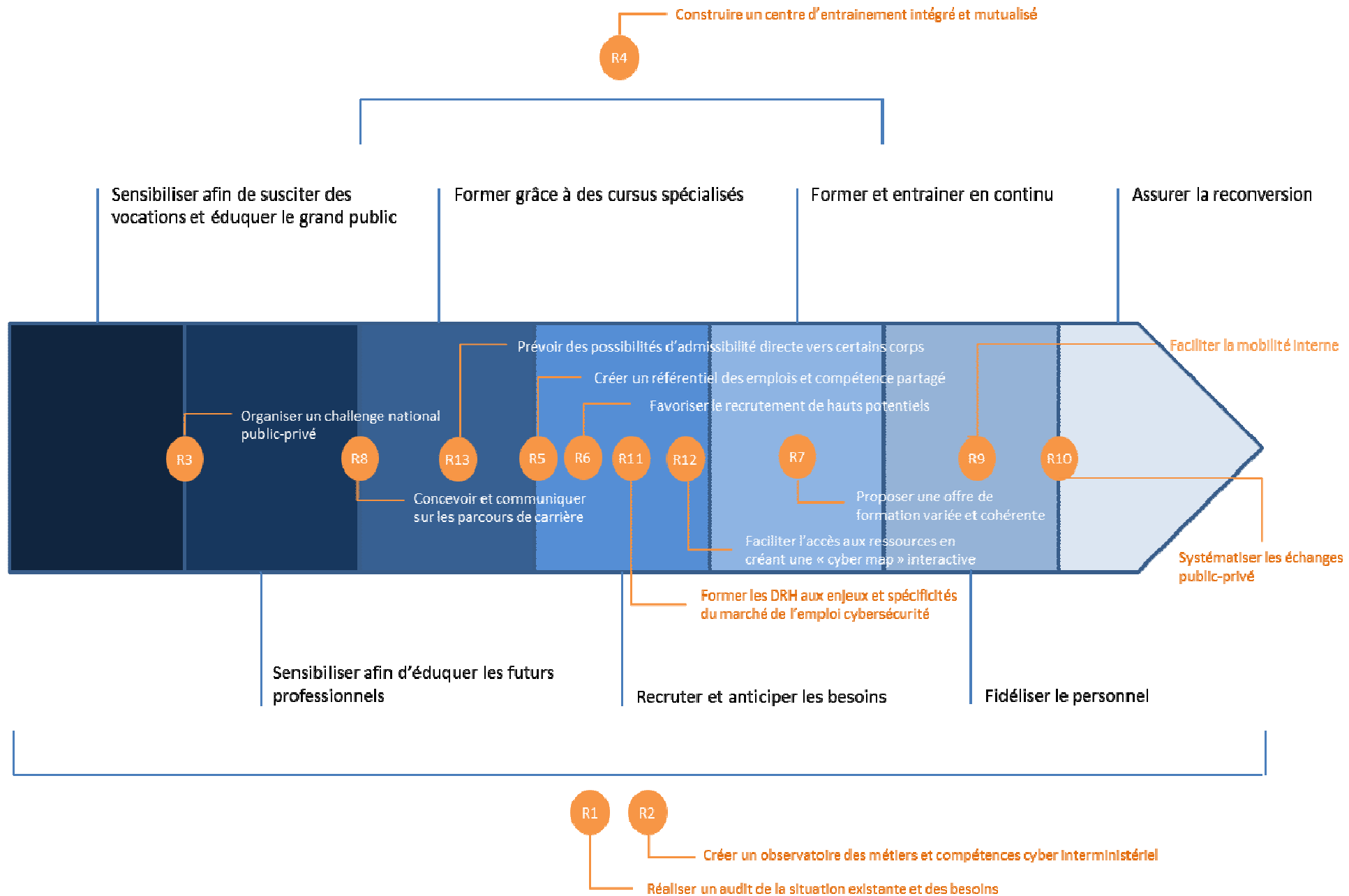
6. Recommandations

En s'appuyant sur les bonnes pratiques détectées, ainsi que sur les forces et opportunités du monde de la Défense, il est possible de définir quelques recommandations prioritaires, couvrant l'ensemble du *pipeline* cybersécurité, qu'il s'agisse de son alimentation en amont, du recrutement, de la gestion de carrières, ou de la formation et de l'entraînement.

Certaines de ces recommandations concernent spécifiquement le Ministère de la Défense et s'intègrent dans l'axe 3 du pacte Défense Cyber (actions 27 à 30). D'autres ont une portée plus globale et pourraient être mises en œuvre au niveau interministériel.

Notons à ce propos que le DoD américain a publié en décembre 2013 une *Cyberspace Workforce Strategy*¹⁸⁷ proposant 5 types de mesures : l'établissement d'une politique RH cohérente à l'échelle du Ministère, l'utilisation d'une approche « multidimensionnelle » pour le recrutement, l'institutionnalisation de l'apprentissage continu, la fidélisation du personnel qualifié, le développement des connaissances en matière de menaces, le renforcement des capacités de gestion de crise (via notamment l'utilisation de forces de réserve).

¹⁸⁷ http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed%28final%29.pdf



R1 : réaliser une évaluation de la situation existante

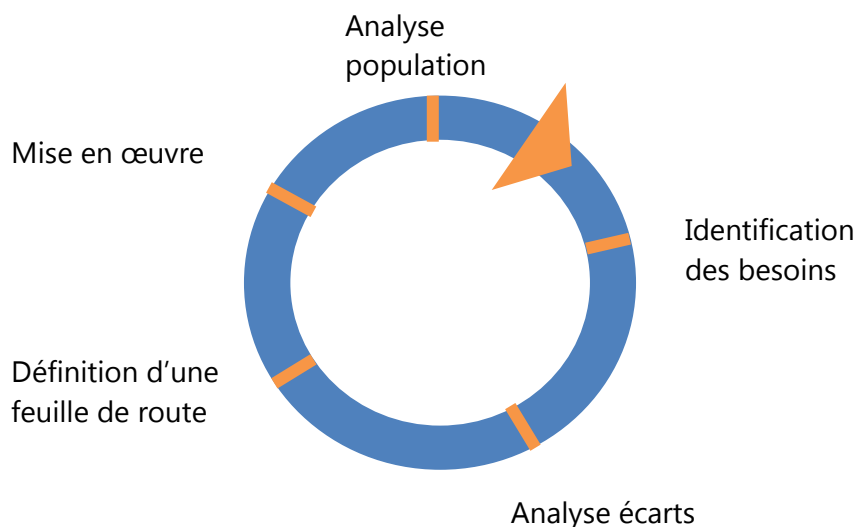
Les acteurs français interrogés dans le cadre de cette étude, qu'il s'agisse d'offreurs, d'institutions ou d'organisations professionnelles, possèdent en réalité peu d'information sur la population active française en cybersécurité.

L'objectif serait donc de réaliser une évaluation de la situation comprenant analyse de l'existant, identification des besoins, *gap analysis*, puis définition d'une feuille de route. Cette analyse serait réalisée *a minima* au niveau des personnels de la Défense et idéalement au niveau interministériel. La feuille de route en résultant, régulièrement remise à jour pour tenir compte des évolutions du marché, permettrait d'orienter les écoles et universités dans la définition de leurs programmes et contenus en matière de cybersécurité et d'engager au niveau de la filière toute entière les actions nécessaires. A l'issue, il serait intéressant d'appliquer cette démarche à tous les acteurs de la cybersécurité.

L'étude, d'une durée de 6 mois, serait menée à partir de questionnaires électroniques adressés aux professionnels de la sécurité.

A noter que la méthodologie ainsi développée pourrait aussi constituer un kit d'évaluation utilisable au sein des organisations désireuses d'évaluer leur situation et d'identifier leurs besoins. Une déclinaison spécifique pourrait en être réalisée pour le Ministère de la Défense.

Figure 51 : méthodologie d'audit



besoins	
Descriptif	L'évaluation comprendrait différentes phases : analyse de la population active, identification des besoins, gap analysis, définition d'une feuille de route et mise en œuvre. Cette analyse serait réalisée <i>a minima</i> au niveau des personnels de la Défense et idéalement au niveau interministériel.
Résultats escomptés	Meilleure évaluation et anticipation des besoins
Ressources nécessaires	Méthodologie d'évaluation, panel d'organisations et de personnes à cibler.
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	3
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	1

R2 : créer un observatoire des métiers et compétences cyber interministériel

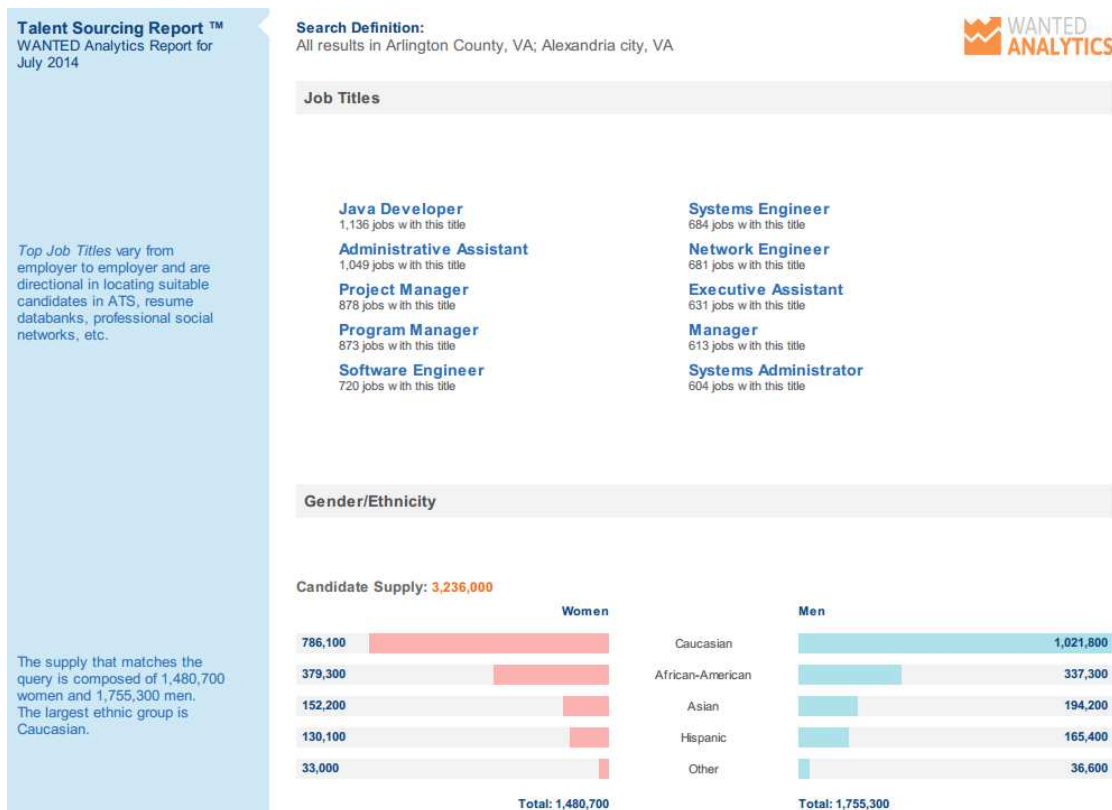
Afin de soutenir la mise en œuvre et la cohérence de toutes les recommandations retenues, la mise en place d'un Observatoire des métiers et compétences cybersécurité est recommandée. Cet observatoire, placé au niveau interministériel pour disposer de la taille critique suffisante en termes de population active et favoriser la mobilité inter-administrations, aurait les missions suivantes :

- Assurer le lien entre stratégie, besoins et recrutement ;
- Assurer le suivi et l'usage à bon escient des compétences ;
- Proposer un référentiel des métiers, un référentiel des compétences ;
- Orienter et certifier les formations clés ;
- Auditer régulièrement les acteurs et leurs besoins ;
- Réaliser des enquêtes afin de mieux comprendre les contraintes et mieux les adresser.

Cet observatoire produirait mensuellement un baromètre de l'emploi cyber basé notamment sur une analyse permanente de l'offre et de la demande.

Cette recommandation s'inscrit dans l'action n°30 du pacte Défense Cyber.

Figure 52 : exemple de baromètre de l'emploi cyber (Wanted Analytics)



Intitulé	Créer un Observatoire des métiers et compétences cyber interministériel
Descriptif	L'Observatoire des métiers et compétences cybersécurité permettra de s'assurer d'une continuité entre la stratégie globale, les besoins et le recrutement. Il permettra de développer un référentiel des métiers en adéquation avec les besoins de chacun des acteurs et les formations existantes. Cette recommandation s'inscrit dans l'action n°30 du pacte Défense Cyber.
Résultats escomptés	Adaptation permanente des ressources humaines aux besoins

Ressources nécessaires	Structure permanente en relation avec un référent chez tous les acteurs concernés
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	2
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	1

R3 : organiser un challenge national public-privé

A l'image du Cyber Challenge UK (voir point [B17-3](#)), il s'agirait d'organiser une compétition informatique nationale permettant d'identifier des talents et de communiquer sur les emplois et carrières dans le monde de la cybersécurité.

Le coût d'organisation de ces compétitions est en effet assez élevé et la mutualisation des efforts est indispensable pour atteindre la taille critique nécessaire.

Cette compétition permanente serait organisée en 4 étapes :

- Sélection en ligne ;
- Compétitions régionales organisées en partenariat avec les différents acteurs régionaux existants (clusters, pôles de compétitivité...);
- Demi-finales ;
- Finales au moment du Forum International de la Cybersécurité.

Le projet serait financé par des contributions financières et des apports en nature sous la forme de développement d'épreuve par des partenaires privés et publics.

Intitulé	Organiser un challenge national public-privé
Descriptif	Cette compétition permanente serait organisée en différentes étapes (4 séries d'épreuve) réparties dans toute la France pour s'appuyer sur les différentes initiatives régionales qui voient le jour dans le domaine

Résultats escomptés	Forte médiatisation des emplois sécurité. Détection de nouveaux talents.
Ressources nécessaires	Contenus techniques. Organisation.
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	1
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	1

R4 : construire un centre d'entraînement intégré et mutualisé

L'obsolescence très rapide des compétences cyber, notamment au plan technique, exige la mise en place d'une politique intensive de formation continue et d'entraînement. Or, celle-ci requiert la création d'un centre d'entraînement intégré et mutualisé.

Ce dispositif répondrait aux besoins suivants :

- Couvrir les différents niveaux d'entraînement (élémentaire, supérieur...);
- Répondre aux besoins des différents types de population concernés au sein du Ministère de la Défense et des acteurs civils et privés :
 - o spécialistes en systèmes d'information (socle commun) ;
 - o généralistes de la chaîne « cyber » ;
 - o spécialistes SSI ;
 - o personnels experts affectés en unités « cyber ».
- répondre aux besoins génériques des forces armées (tronc commun) mais aussi à leurs besoins spécifiques en proposant des contenus variés, régulièrement mis à jour ;
- Optimiser les ressources de fonctionnement afin de concentrer le personnel sur des actions à forte valeur ajoutée en matière d'accompagnement, de préparation des scénarios et de formation.

Au plan fonctionnel, le centre d'entraînement comprendrait :

- Un module « simulation technique », basé sur un environnement de virtualisation et la reproduction d'un environnement informatique simplifié proche de celui du Ministère de la Défense ;

- Un module « jeu de rôle », lequel serait utilisé non seulement pour le jeu stratégique mais aussi pour introduire le facteur humain dans l'ensemble des exercices et entraînements ;
- Un module de préparation et de pilotage unifié.

Plusieurs modes d'entraînement seraient proposés : mode présentiel ou mode distanciel, avec un pilotage de jeu manuel, semi-automatique ou automatique.

Intitulé	Construire un centre d'entraînement intégré et mutualisé
Descriptif	Ce dispositif serait basé sur un environnement d'entraînement comprenant une partie simulation technique et une partie jeu de rôle. Il proposerait des contenus clés en mains variés.
Résultats escomptés	Démultiplier le nombre de formations et d'entraînements réalisés
Ressources nécessaires	Contenus, environnement d'entraînement et équipes de formation
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	1
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	1

R5 : créer un référentiel des emplois et compétence partagé

Il est essentiel de disposer d'un référentiel des emplois et compétences. L'intérêt est multiple : développer d'une vision partagée ; structurer les cursus de formation ; faciliter l'orientation des personnes intéressées ; faciliter l'émission d'offres d'emploi et donc la recherche de candidats adaptés. Disposer d'un référentiel permet en outre d'orienter le marché en fonction de ses besoins et est donc très intéressant en termes d'influence.

Attention, cependant, à éviter plusieurs écueils. Il n'existe de référentiel miracle, universel et adapté à toutes les situations. Une partie de ce référentiel sera spécifiques au Ministère de la Défense, du fait des spécificités de celui-ci et des contraintes qui sont les siennes. De plus, il faut régulièrement mettre à jour ce référentiel en fonction du marché et de l'évolution des concepts opérationnels. Il ne faut pas

construire un référentiel trop « globalisant » ; le terme « cyber » renvoie ainsi à des réalités très différentes et trop larges. Enfin, un référentiel n'est pas autonome au sens où les emplois et compétences qu'il catégorise et décrit ont nécessairement des liens avec d'autres activités. L'objectif est plutôt de disposer d'un référentiel adapté à son organisation avec un niveau de granularité suffisant pour que l'ensemble des acteurs s'y retrouvent facilement. Ce référentiel doit être partagé et cohérent, au moins en partie, avec les autres acteurs du marché sur lequel on évolue. Il doit être ciblé sur l'ensemble des emplois liés aux opérations dans le cyberspace. Son scope doit donc selon nous dépasser la cybersécurité pour prendre en compte également des aspects « métiers » comme par exemple le renseignement « cyber », les opérations d'information dans le cyberspace, etc., ou tout au moins prévoir un lien avec les référentiels concernés.

Même s'il n'est pas dans les objectifs de l'étude d'élaborer un référentiel complet des emplois et compétences cyber, il paraît utile de détailler sa structure et son fonctionnement et, pour ce faire, de s'appuyer sur une première version de ce document (voir annexe)¹⁸⁸.

Les métiers

Un référentiel des métiers de la cybersécurité se doit d'être le plus opérationnel possible. Distinguer les métiers selon leur statut ne suffit pas. Une telle segmentation, prise isolément, nuit à l'efficacité en entachant la vision globale et la complémentarité des métiers, au profit d'une vision hiérarchique et contre-productive.

A contrario, une classification opérationnelle des métiers permet :

- Une vision globale de la gestion de la menace ;
- Une traduction opérationnelle de la stratégie vers les métiers ;
- Une meilleure gestion des effectifs grâce à l'identification des écarts entre les besoins et la réalité ;
- Une mise à jour plus aisée et flexible, adaptable aux mutations de la cybermenace, en évolution constante ;
- Une gestion plus efficace des compétences clés, directement adaptées aux besoins métiers, besoins métiers eux-mêmes calqués sur la stratégie plus globale de cybersécurité.

La définition des métiers dépend du canevas développé dans le droit fil de la stratégie élaborée. Les fonctions suivantes peuvent être reprises afin de classer les différents métiers de la cybersécurité :

1. La sécurité en amont
2. L'analyse des risques et menaces
3. L'administration et la maintenance du SI
4. La protection du SI
5. Les opérations cyber
6. L'investigation numérique

A ces 6 fonctions de la cybersécurité, peuvent être ajoutées les fonctions support suivantes :

¹⁸⁸ Les travaux ont pris pour base le référentiel élaboré dans le cadre du groupe de travail n°3 du RCC.

- Conseil et appui juridique
- Vente
- Marketing
- Entraînement et formation

Ces fonctions sont complémentaires et interdépendantes. Elles se recourent et se superposent tout au long du cycle de gestion de la menace. A ces fonctions sont associés des emplois types.

Figure 53. Schéma récapitulatif : exemples de grandes fonctions de la cybersécurité

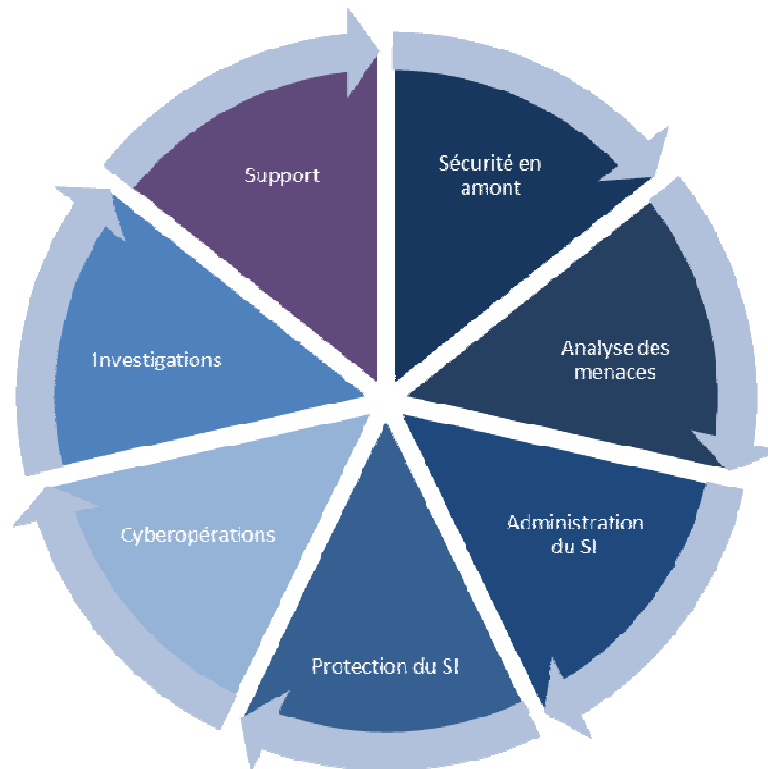


Figure 54. Extrait du référentiel des emplois types sur les fonctions « sécurité en amont » et « protection du SI »

Fonction	Détail	Exemples d'emplois types
1. Sécurité en amont	a) R&D	Ingénieur R&D
	b) Assurances, audit et compliance	Assureur
		Auditeur organisationnel
		Auditeur conformité
		Professionnel qualité
	c) Anticipation du risque	Auditeur technique
		Consultant/expert gestion du risque
		Risk manager
	d) Architecture des infrastructures et systèmes d'information	Consultant gestion de crise
		Architecte système
		Architecte réseau
		Architecte application
		Développeur
		Architecte sécurité
		Référent sécurité projet
		Chef de projet (MoE/MoI)
Intégration	Cryptologue	
	Développeur / concepteur	
	Chef de projet	
Déploiement	Intégrateur	
	Technicien réseau-télécoms	
4. Protection du SI	a) Gouvernance et exploitation SSI	Intégrateur d'exploitation
		Ingénieur sécurité
		RSSI
		Administrateur sécurité
		Technicien sécurité
		Télé-assistant
	b) Mise à l'épreuve	Expert produit/technologie (IAM, MDM, IDS, IPS, etc.)
		Red Team
		Blue Team
	c) Collecte et détection	Pentesteur
Ingénieur spécialiste en collecte et analyse de journaux d'événements		
		Ingénieur chargé d'analyse en

La version intégrale de ce modèle de référentiel est consultable en annexe.

Les compétences et « talents » ou « appétences »

Déterminer les fonctions clés du référentiel permet de définir une vision globale des métiers de la cybersécurité. Les catégories ainsi définies reflètent une vision, une perception de la fonction cybersécurité, et une stratégie. Il est également important de référencer les compétences, talents ou appétences des personnels, afin d'orienter au mieux leur carrière en leur proposant les formations adaptées à leur profil et correspondant à leurs ambitions.

Si la matrice des compétences est le document le plus objectif à réaliser, une matrice des talents et appétences est également importante afin de mieux comprendre les profils et leurs ambitions.

Figure 55. Extraits de matrice de compétences générales

Type de compétences	Compétences
Conception	Développement
	Architecture
Intégration	Déploiement des systèmes
	Intégration des systèmes
Juridique et normatif	Régulation et législation
	Maîtrise des outils SSI (PSSI, charte, etc.)
	Normes et compliance
	Veille et intelligence juridique
	Données à caractère personnel
	Propriété intellectuelle
	Droit pénal informatique
	Règlementations sectorielles
	Droit du travail
	Export et relations internationales

Le croisement des métiers et des compétences

Pour accompagner la mobilité, il est indispensable de flécher un parcours cohérent et réaliste. Pour ce faire, le référentiel métier peut indiquer auprès de chaque poste, à l'aide d'indicateurs, la densité métier, IT ou sécurité nécessaire.

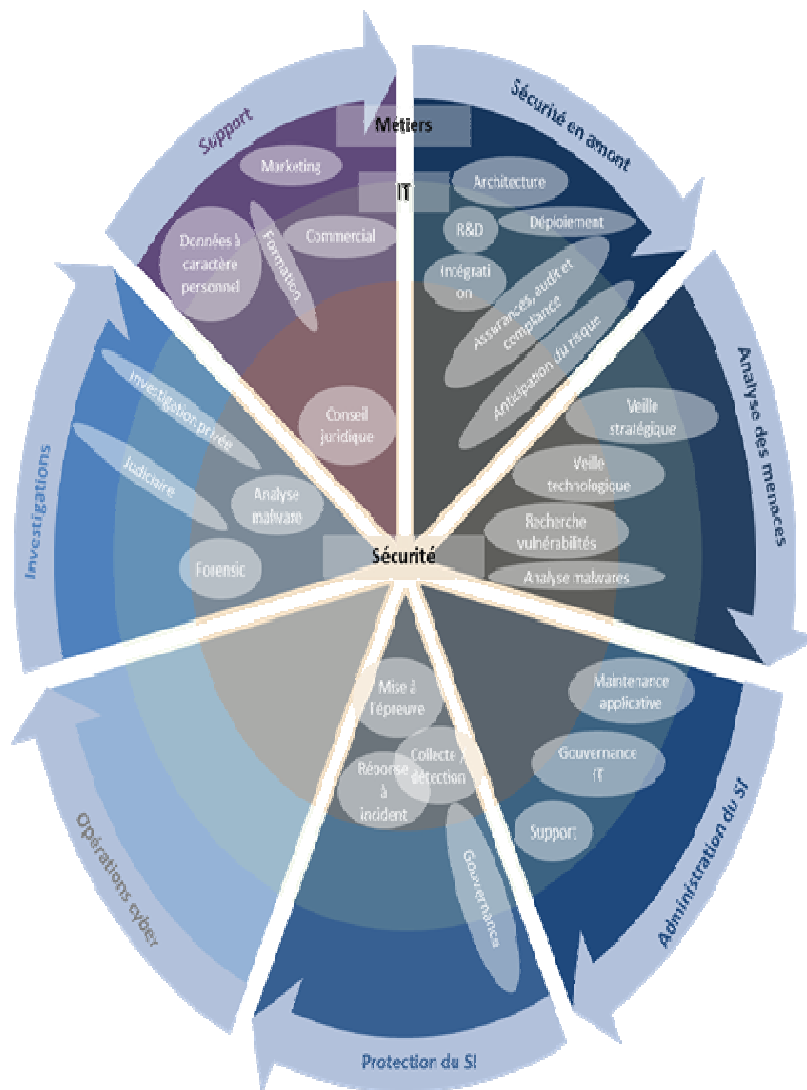
- L'indicateur de « densité IT » traduit la part plus ou moins technique du métier ;
- L'indicateur de « densité sécurité » indique l'importance de la culture sécurité ;
- L'indicateur de « densité métier » souligne l'importance de la connaissance du secteur d'activité constituant l'environnement de travail du professionnel de la cybersécurité.

Ces indicateurs sont mis en correspondance avec les compétences et talents requis pour chacun des postes. La présence ou l'absence de telle compétence ou tel talent permettra d'évaluer, *in fine*, la densité IT, sécurité ou métier d'un poste en cybersécurité.

Figure 56. Extrait du référentiel d'emplois, avec indications de densités

Fonction	Détail	N°	Emplois types	Indicateurs - densité		
				IT	Sécurité	Métier
1. Sécurité en amont	a) R&D	E1	Ingénieur R&D	■	■	
		E2	Assureur qualité	■	■	■
	b) Assurances, audit et compliance	E3	Auditeur organisationnel	■	■	■
		E4	Auditeur conformité	■	■	■
		E5	Professionnel qualité	■	■	■
		E6	Auditeur technique	■	■	■
	c) Anticipation du risque	E7	Consultant/expert gestion du risque	■	■	■
		E8	Gestionnaire de Risques	■	■	■
		E9	Consultant gestion de crise	■	■	■
	d) Architecture des infrastructures et systèmes d'information	E10	Architecte système	■	■	
		E11	Architecte réseau	■	■	
		E12	Architecte application	■	■	
		E13	Développeur	■	■	
		E14	Architecte sécurité	■	■	
		E15	Référent sécurité projet	■	■	
		E16	Chef de projet (MoE/Mol)	■	■	■
		E17	Cryptologue	■	■	■
	e) Intégration	E19	Développeur / concepteur	■	■	■
		E20	Chef de projet	■	■	■
		E21	Intégrateur	■	■	■
	f) Déploiement	E22	Technicien réseau-télécoms	■	■	
		E23	Intégrateur d'exploitation	■	■	

Figure 57. Récapitulatif des métiers selon leur densité



Intitulé	Créer un référentiel des emplois et compétence partagé	
Descriptif	Le référentiel détaille les emplois-type par famille puis liste les compétences nécessaires. Des indicateurs de densité permettent de déterminer le niveau de profondeur demandé pour chaque dimension (sécurité, IT, métiers).	
Résultats escomptés	<ul style="list-style-type: none"> - Développer d'une vision partagée ; - Structurer les cursus de formation ; - Faciliter l'orientation des personnes intéressées ; - Faciliter l'émission d'offres d'emploi et donc la recherche de candidats adaptés. 	
Ressources nécessaires	Réunir les acteurs du sujet pour élaborer un référentiel selon une vision partagée. Auditer les besoins.	
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)		2
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)		1

R6 : favoriser le recrutement de hauts potentiels dans le domaine

Les étudiants ayant intégré les grandes écoles militaires bénéficient d'une formation basée sur un socle commun. L'objectif serait de les aiguiller dès leur sortie de l'école sur une spécialité cyber. Le Ministère ne propose en effet aujourd'hui aucune spécialisation de premier niveau en cyberdéfense, ce qui contraint ces personnes à attendre une spécialisation de deuxième niveau pour travailler dans ce domaine. Ces spécialistes disposeraient ainsi rapidement d'une expérience significative en cyberdéfense et pourraient se reconvertir dans le privé au bout de 10 ou 15 ans.

Intitulé	Favoriser le recrutement de hauts potentiels
Descriptif	Il s'agit de proposer des spécialisations cyber dès la sortie de l'école de formation (Air, Terre et Mer) afin de se doter de personnels réalisant des carrières courtes et susceptibles de se reconvertir aisément dans le privé au bout de 10-15 ans de carrière.
Résultats escomptés	Attirer des profils techniques de haut niveau
Ressources nécessaires	Modification des cursus de formation initiale
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	3
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	2

R7 : proposer une offre de formation variée et cohérente

Les offres de formation doivent être variées pour répondre aux besoins de l'ensemble de l'écosystème cyber interne. L'ensemble des formations proposées par les différentes organisations de la défense doivent s'inscrire dans ce schéma.

5 niveaux peuvent être distingués :

- Niveau 1 : sensibilisation à l'hygiène numérique pour l'ensemble des personnels utilisant les systèmes d'information ;
- Niveau 2 : renforcement des compétences cybersécurité pour les spécialistes SIC ;
- Niveau 3 : approfondissement des compétences cybersécurité pour les spécialistes SSI ;
- Niveau 4 : formation cyberdéfense
- Niveau 5 : formation « culture générale » cyber pour les généralistes intervenant dans la conduite des opérations

Intitulé	Proposer une offre de formation variée et cohérente
Descriptif	L'objectif est de définir un cadre de référence composé de plusieurs niveaux de formation qui seront ensuite utilisés par l'ensemble des formations proposées par les organisations de la défense.
Résultats escomptés	Homogénéiser les offres de formation
Ressources nécessaires	Cadre de cohérence
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	4
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	2

R8 : concevoir des parcours et communiquer des carrières, pas uniquement sur des emplois

Un individu peut faire une carrière entière dans la cybersécurité mais peut aussi occuper de façon ponctuelle un emploi comprenant une part plus ou moins importante de cybersécurité. Ces interactions doivent être mises en valeur, notamment dans un contexte où la population « cybersécurité » va nécessairement vieillir, malgré l'arrivée croissante de juniors, compte tenu du vieillissement des « pionniers » présents sur cette activité depuis quelques années. Il s'agit donc de communiquer assez largement sur les perspectives de carrière offertes par la cybersécurité à travers des exemples de parcours types.

Plusieurs types d'interaction peuvent être distingués :

- Les interactions avec les métiers de l'organisation. Exemple : un responsable « métier » d'activité devient responsable de la sécurité des systèmes d'information côté maîtrise d'œuvre. Dans un contexte Défense, il s'agirait ici de définir des passerelles entre la cybersécurité et des spécialités telles que la guerre électronique, le renseignement, les opérations d'information etc. ;
- Les interactions avec l'IT « généraliste » et plus globalement avec les emplois scientifiques et techniques. Exemple : un technicien support informatique devient ingénieur sécurité.

Pour chaque parcours type identifié serait proposée une interview d'une personne ayant suivi ce cursus.

Ces parcours doivent non seulement montrer comment on accède à un emploi cyber mais également comment on est susceptible d'en sortir, tant en termes de spécialités que de type d'évolutions (management ou expertise). Plusieurs RSSI interrogés témoignent en effet de leurs interrogations quant à leurs évolutions de carrière après leur poste actuel.

Ces contenus seraient ensuite diffusés à travers plusieurs canaux : site internet (comportant notamment quelques jeux interactifs, des fiches de poste, des fiches parcours), réseaux sociaux, publicités dans la presse.

Intitulé	Elaborer et communiquer sur les parcours de carrière, pas uniquement sur les emplois	
Descriptif	L'objectif est de constituer, sur la base d'un référentiel des emplois et compétences, des parcours type proposant des passerelles entre métiers et cybersécurité, IT et cybersécurité.	
Résultats escomptés	Meilleure information des juniors et seniors sur les parcours proposés	
Ressources nécessaires	Définition des parcours-type grâce à un groupe de travail, campagne de communication	
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	3	
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	2	

R9 : faciliter la mobilité interne

L'inventaire des facteurs de mobilité pour mieux les adresser

Conserver ses effectifs est un challenge. L'employeur peut être déstabilisé par la volonté de ses effectifs de changer de poste. Ce désir de changement se traduit régulièrement en départs, en raison de l'impossibilité pour l'employeur de satisfaire les désirs d'évolution de ses effectifs.

Pour conserver ses effectifs, l'employeur se doit d'anticiper les désirs d'évolution et de changement des nouvelles recrues. Pour mieux anticiper et organiser la mobilité, il est impératif de comprendre les

raisons qui peuvent motiver un expert en cybersécurité à changer de poste. Ces raisons sont à l'origine de mobilité de type vertical (évoluer vers plus de responsabilités) ou horizontal (métier). :

- Evoluer vers des fonctions de management ;
- Changer d'équipe et renouveler les rapports humains ;
- Découvrir un nouveau métier ;
- Se spécialiser dans son propre métier ;
- Renforcer une appétence découverte lors du précédent poste ;
- Etc.

Objectif : proposer, en interne ou en proche périphérie, les parcours de mobilité satisfaisant leurs besoins, le tout dans un environnement familier.

L'emploi des seniors dans l'IT est de ce point de vue un véritable enjeu. Leur proportion est relativement faible (moins de 6%) dans un domaine qui pratique une sorte de jeunisme avec une moyenne d'âge de 34 ans¹⁸⁹, alors même que les projets sont de plus en plus importants et complexes. Le maintien des seniors, qui sont souvent perçus à tort comme moins au fait des innovations et moins adaptables, dans le domaine IT est ainsi une priorité. D'une part, pour répondre à des besoins d'expertise toujours plus pointue. « *La complexité revalorise les parcours centrés sur l'expertise technique* », souligne Marie-Pierre Fleury de la société Camden dans un livre blanc consacré à l'emploi des seniors dans l'IT¹⁹⁰. D'autre part, parce que la pyramide managériale et la pratique de l'externalisation ont réduit les opportunités dans les entreprises.

Il faut donc revaloriser les parcours techniques, les carrières de manager n'étant pas la seule voie de valorisation. D'autant que les aspirations des seniors sont souvent relativement différentes. « *Avant la quarantaine, les critères d'une carrière réussie sont objectifs : le salaire, le périmètre de responsabilité... Après 45 ans, les critères deviennent subjectifs : ma carrière est un succès si je m'y sens bien, si mon activité et mes relations me plaisent – ainsi que l'équilibre avec ma vie personnelle* », explique Vincent Giolito, directeur Nouvelle Carrière¹⁹¹.

Un outil favorisant cette mobilité pourrait être développé : un personnel qui souhaite évoluer dans sa carrière pourra visualiser les postes qui lui sont proposés, avec ou sans formation supplémentaire, ou rechercher quelles sont les compétences qui devra acquérir pour prétendre à un poste qu'il vise.

¹⁸⁹ <http://www.fnmt.fr/fr/communiqués-de-presse/emploi-des-seniors-IT-une-fin-carri%C3%A8re-45-ans-nouvelles-voies>

¹⁹⁰ http://gallery.mailchimp.com/9f370712e6e307699d008e784/files/SeniorIT_LivreBlanc_NvelleCarriere_28jun12.pdf

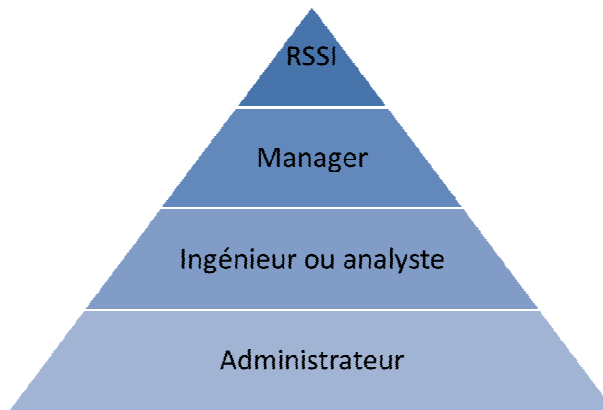
¹⁹¹ http://gallery.mailchimp.com/9f370712e6e307699d008e784/files/SeniorIT_LivreBlanc_NvelleCarriere_28jun12.pdf

Intitulé	Faire l'inventaire des facteurs de mobilité pour mieux les adresser
Descriptif	<p>Dans une démarche <i>bottom-up</i> : mieux comprendre les raisons qui poussent les agents à quitter leur poste pour mieux adresser la situation.</p> <p>Cette mobilité serait facilitée par une plateforme permettant aux personnels de se voir proposer (mode push) des évolutions de carrières et de rechercher des postes en fonction de leurs compétences.</p>
Résultats escomptés	Conserver les talents. Proposer les parcours types adéquats.
Ressources nécessaire	Observatoire dédié.
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	3
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	2

Proposer des parcours-type

Il est possible de flécher la mobilité du personnel, en influençant les choix selon les besoins : besoins en expérience, besoin en type de profil, etc. Les parcours types peuvent ainsi être proposés à tout nouvel arrivant, comme garantie d'opportunités de carrière au sein de l'organisme recruteur.

Figure 58. Exemple de parcours SSI



Exemple de parcours type, jalonné de formations ◆, de prise en compte de l'expérience ◆, ou de processus de reconversion/transition ◆ :

Figure 59. Exemple de parcours type 1

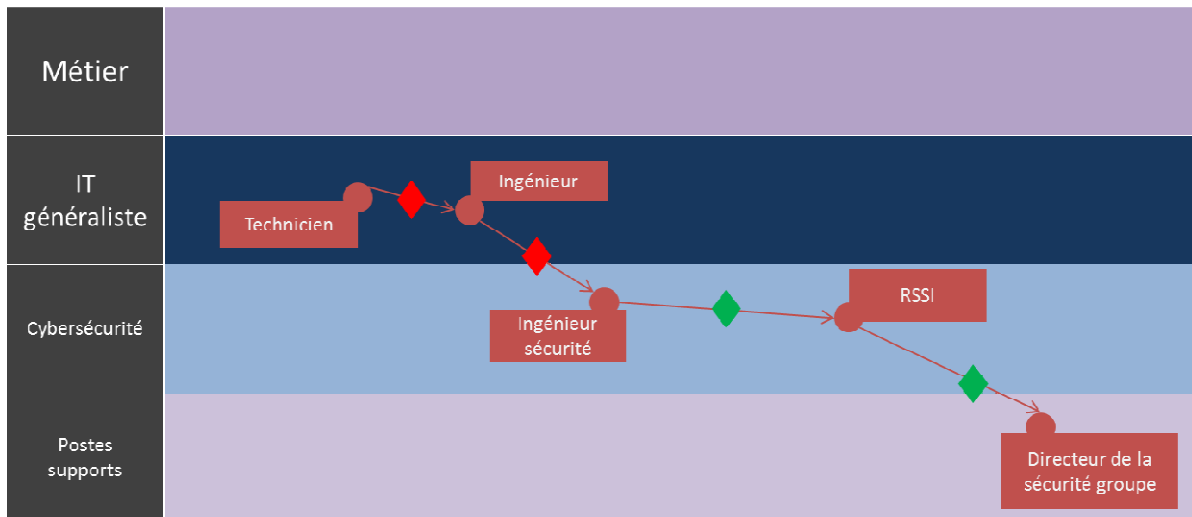
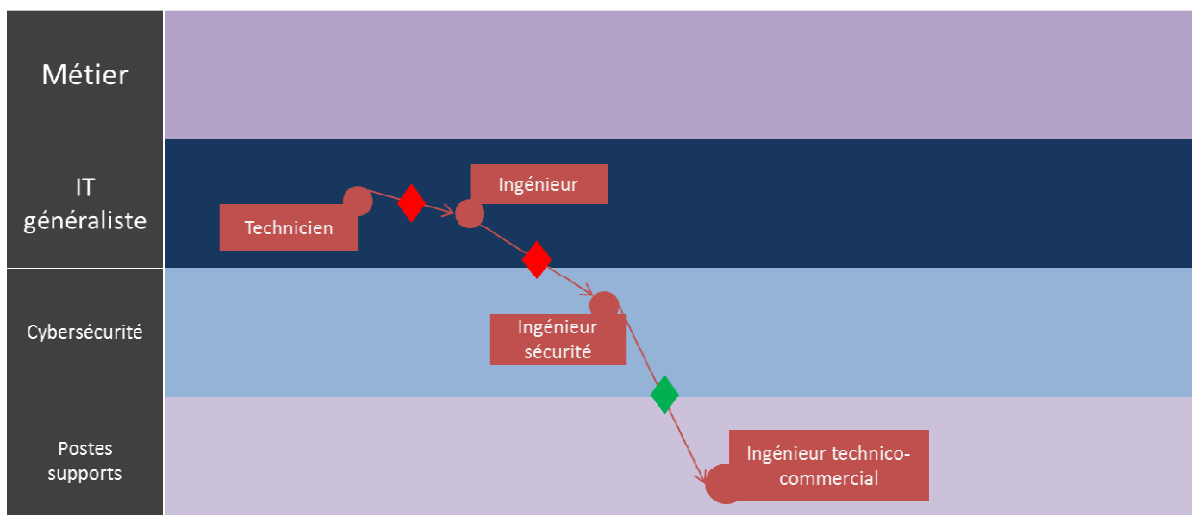


Figure 60. Exemple de parcours type 2

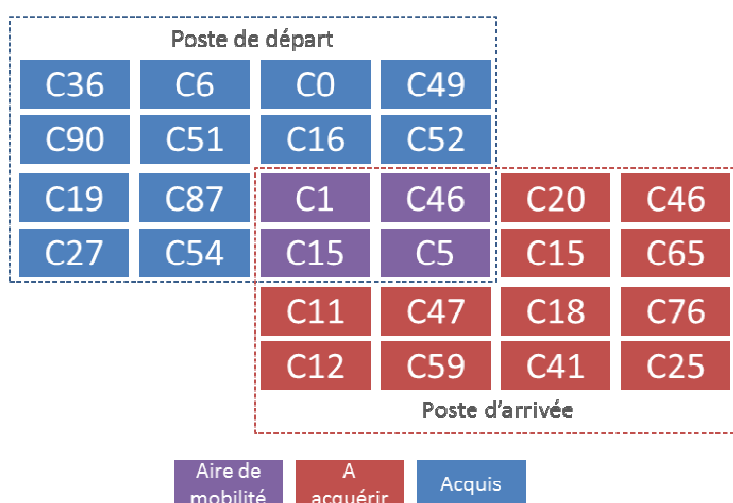


Intitulé	Proposer des parcours types
Descriptif	Proposer des plans de carrière exemplaires. Objectif : flécher les talents selon les besoins RH, tout en satisfaisant les désirs d'évolution et de mobilité.
Résultats escomptés	Conserver les talents. Mieux répartir les ressources humaines. Bénéficier de flexibilité.
Ressources nécessaire	Référentiel des compétences et des métiers. Audit préalable.
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	3
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	1

Laisser une liberté dans la mobilité grâce aux « aires de mobilité »

Le référentiel de compétences et l'affectation de compétences pour chacun des emplois types permettent d'organiser la mobilité de tous les profils. En superposant le poste de départ au poste d'arrivée, il est possible de visualiser les compétences manquantes, et ainsi d'organiser la transition par le biais de formations ciblées, voire de réaliser des équivalences en raison de l'expérience.

Figure 61. Illustration d'une aire de compétence entre le poste de départ et le poste désiré



Ce concept d'aire de mobilité favorise la mobilité sur des parcours non-nécessairement anticipés, voire proposés aux salariés. Il laisse en effet une marge de liberté à celui optant pour une transition originale d'un métier A à un métier B. Le ratio de compétences communes du poste A au poste B définira la réalisabilité de l'opération de mobilité, et le temps nécessaire à sa mise en œuvre (formation, etc.).

Intitulé	Créer des « aires de mobilité »
Descriptif	Anticiper la mobilité hors des plans de carrière anticipés.
Résultats escomptés	Conserver les talents.
Ressources nécessaire	Référentiel des compétences.
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	2
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	2

Créer le statut de « leader technique »

La mobilité verticale des cadres de la cybersécurité se résume souvent à une montée en puissance au niveau managérial. Elle a pour conséquence indirecte de dépouiller les équipes opérationnelles de leurs meilleurs éléments.

Créer un profil de leader technique permet de faire évoluer verticalement des profils souhaitant faire carrière dans leur métier, sans les éloigner du terrain. Ce procédé présente plusieurs avantages :

- Récompenser et valoriser les meilleurs ;
- Conserver les talents et leur expérience au plus près des missions opérationnelles ;
- Conserver ces profils comme tuteurs ;
- Valoriser les profils qui n'ont pas d'appétence au management traditionnel.

Intitulé		Créer le statut de « leader technique »
Descriptif	Proposer aux profils techniques une mobilité verticale d'expertise.	
Résultats escomptés	Conserver les talents au plus près des missions ; proposer des carrières innovantes.	
Ressources nécessaire	Stratégie RH	
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	2	
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	2	

Créer une communauté

Cette communauté peut être à vocation générale, à l'image de Rally Point. Elle peut également être plus spécialisée, comme la communauté de bonnes pratiques du CSIAC. Il est toutefois essentiel de la consacrer aux profils cybersécurité. Cette communauté permettrait, comme Rally Point, la mise en relation, l'entraide sur les choix de carrières, constituant ainsi une véritable vitrine de l'armée dans sa version publique. Elle permettrait aussi l'échange de bonnes pratiques professionnelles.

Intitulé		Créer une communauté
Descriptif	Créer une communauté permettant la mise en relation, l'entraide sur les choix de carrières, l'échange de bonnes pratiques professionnelles.	

Résultats escomptés	Renforcement du réseau, identification et attraction de talents non-militaires, renforcement des compétences par l'échange.
Ressources nécessaire	Compétences Web.
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	2
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	4

R10 : systématiser les échanges public-privé

Outre le développement de capacités de réserve¹⁹² permettant notamment de faire face à des situations de crise, il paraît intéressant de concevoir un programme d'échange public-privé permettant à des personnels du Ministère de la Défense d'effectuer des périodes de détachement dans des emplois équivalents dans le secteur privé et à des civils, issus du secteur privé ou d'administrations, d'effectuer la même chose au sein du Ministère pendant des périodes de 6 à 12 mois.

Ces détachements pourraient faire partie du parcours professionnel proposé à ces personnes et être valorisés au même titre que des périodes de formation ou l'acquisition de certifications. Il est en effet essentiel que la personne détachée puisse être certaine de réintégrer son service d'origine sans être pénalisé.

Intitulé	Créer un programme de détachement public-privé
Descriptif	Ce programme d'échange permettrait à des personnels du Ministère de la Défense d'être détachés dans des emplois

¹⁹² Ce sujet n'est pas traité dans la présente étude puisqu'il a fait l'objet d'une étude par l'un des groupes de travail du Réseau Cyberdéfense de la Réserve Citoyenne.

	équivalents dans le secteur privé et réciproquement.
Résultats escomptés	Fertilisation croisée des compétences. Création d'une véritable communauté public-privé en cybersécurité.
Ressources nécessaires	Cadre juridique à adapter
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	3
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	3

R11 : former les DRH aux enjeux et spécificités du marché de l'emploi cybersécurité

L'une des premières difficultés en matière de recrutement et de gestion des carrières en cybersécurité réside souvent dans les incompréhensions entre les directions RH et les opérationnels ainsi que sur l'ignorance par les RH des spécificités du marché de l'emploi dans le domaine, à l'exception notable des directions RH des offreurs de services et de solution dans le domaine.

Il semble donc pertinent de proposer aux directions RH des secteurs public et privé des formations spécifiques autour des thèmes suivants :

- Comprendre le marché
 - o Principaux acteurs (écoles, offreurs, utilisateurs finaux, certifications...)
 - o La population active cyber
 - o Les emplois, compétences et parcours type
 - o Perspectives d'évolution
- Evaluer et anticiper vos besoins
 - o Analyser l'existant
 - o Identifier les besoins
 - o Analyser les *gaps*
 - o Définir une stratégie
- Recruter grâce à une stratégie multicanal
 - o Relations avec les écoles
 - o Participation à des événements
 - o Communication dans la presse spécialisée
 - o Utilisation de *job boards*

- Mettre en place une stratégie de formation continue
 - o Tutorat
 - o Certifications
 - o Formation interne et externe

Ces formations déboucheront sur la remise d'un kit RH sur la cybersécurité.

Intitulé	
Former les DRH aux enjeux et spécificités du marché de l'emploi cybersécurité	
Descriptif	L'objectif est de proposer aux directions RH des secteurs public et privé des formations spécifiques sur le marché de l'emploi cybersécurité.
Résultats escomptés	Meilleure appréhension du marché de l'emploi cybersécurité par les DRH
Ressources nécessaires	Kit de formation RH
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	4
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	3
<p>Le recrutement dans la communauté du renseignement américain</p> <p>La NSA (40 000 agents au total) s'appuie pour le recrutement sur :</p> <ul style="list-style-type: none"> - 80 personnes qui ont comme mission principale le recrutement ; - 300 personnes pour lesquelles c'est une mission additionnelle ; - 1 500 autres qui sont impliqués à un moment ou un autre dans le processus de recrutement¹⁹³. 	

¹⁹³ http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

Ce dispositif lui permet aujourd'hui de détecter dès la sortie des écoles les meilleurs éléments, 80 % de ses recrutements ciblant des postes de jeunes diplômés, pour la plupart à des niveaux licence (bac +4 ans). La NSA fabrique donc, plus qu'elle n'achète ses experts cyber. Elle a pour ce faire développé un système de formation interne très performant, le cursus pouvant durer 3 ans pour certains recrutés. Elle utilise par ailleurs beaucoup le système de bourse SFS dont elle aspire la plupart des étudiants à la sortie. La NSA tire avantage de son image et d'un taux de turnover très faible, ce qui rend l'investissement en formation interne rentable. Toute la question est de savoir si l'affaire Snowden est susceptible d'avoir des conséquences durables sur l'attractivité de l'agence. La CIA investit également lourdement dans la formation interne et n'hésite pas, comme la NSA, à participer directement à des conférences de hacking comme la Black Hat ou la Defcon ou à participer aux salons de l'emploi. Elle pioche également largement dans le vivier que constitue son département IT. L'externalisation croissante de l'IT des agences fédérales constitue de ce point de vue une faiblesse car elles pourraient à terme perdre ce vivier important de candidats.

R12 : faciliter l'accès aux ressources en créant une « cyber map » interactive

Cette carte aurait pour objectifs de recenser et de flécher au niveau national l'ensemble des ressources disponibles.

Principales catégories :

- Universités et écoles ;
- Administrations et institutions ;
- Incubateurs et accélérateurs ;
- Pôles et cluster ;
- Offreurs de services et de solutions.

La publication des offres d'emplois, de stages et de formation correspondant à ces acteurs constituerait évidemment un plus.

Le risque de flécher les ressources stratégiques en matière de cybersécurité pour des investisseurs étrangers semble limité puisque l'ensemble des informations publiées sur le site seront publiques. Par ailleurs, il apparaît aujourd'hui vital, pour développer la base industrielle et technologique, de valoriser les acteurs français et de communiquer sur leurs offres, notamment à l'international.

Le site pourrait être géré gratuitement par un acteur privé qui se rémunérerait grâce à des prestations à valeur ajoutée (réalisation d'études de marché, intermédiation...).

Intitulé

Faciliter l'accès aux ressources en créant une « cyber map »
interactive

Descriptif	L'objectif est de recenser et de flécher au niveau national l'ensemble des ressources disponibles
Résultats escomptés	Visibilité accrue des ressources disponibles et des offres d'emplois proposées
Ressources nécessaires	Développement de la plateforme et animation quotidienne
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	3
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	4

L'exemple de la Cyber Maryland Map.

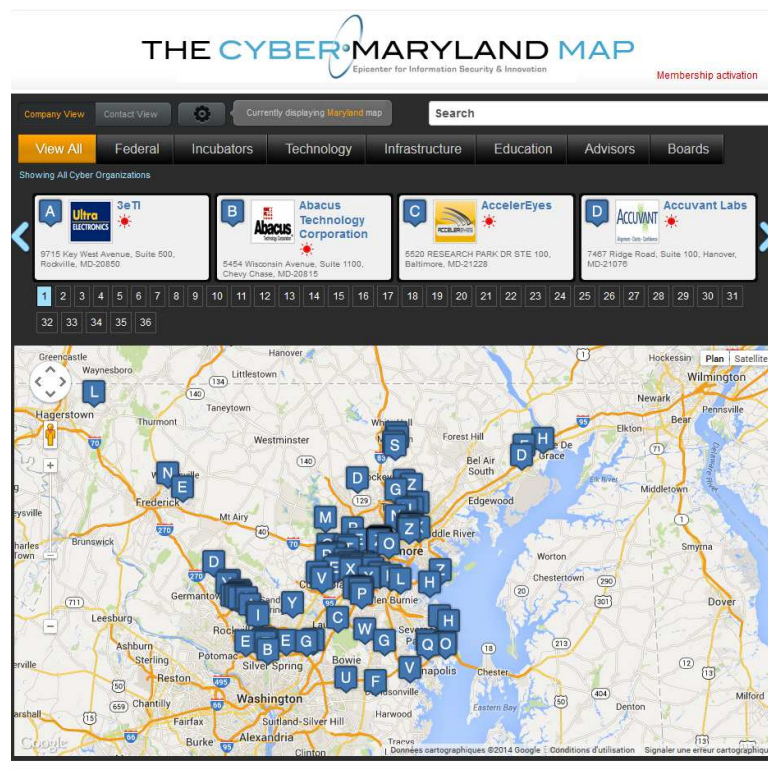
Cette carte permet de flécher l'ensemble des nombreuses ressources « cybersécurité » situées sur le territoire du Maryland : organisation fédérales, entreprises, incubateurs, universités, consultants.

Le dispositif est donc utile pour un étudiant cherchant un cursus spécialisé, un jeune diplômé cherchant un emploi etc.

Le système possède aussi un vrai intérêt en termes de business puisqu'il permet aussi de connecter offre et demande en matière de cybersécurité, notamment grâce au menu « technologies » permettant de sélectionner des offreurs de telle ou telle catégorie.

L'ergonomie du site est cependant assez moyenne. Elle pourrait facilement être améliorée en prévoyant des profils de navigation (vous êtes en recherche de stage, d'emplois, d'un offreur de services ou de solution etc.).

Figure 62 : Page d'accueil de la Cyber Maryland Map



R13 : prévoir des possibilités d'admissibilité directe vers certains corps

L'objectif de cette recommandation est de favoriser l'intégration d'ingénieurs spécialisés en informatique au sein des corps techniques de la Direction Générale de l'Armement en offrant aux étudiants issus de différentes écoles ou universités habilitées CTI et proposant des spécialités informatique et cyberdéfense d'intégrer directement sur dossier les corps techniques de la Direction Générale de l'Armement après l'obtention de leurs diplômes d'ingénieur.

Intitulé	Prévoir des possibilités d'admissibilité directe vers certains corps
Descriptif	L'objectif est d'offrir aux étudiants la possibilité d'intégrer directement les corps techniques de la Direction Générale de l'Armement après l'obtention de leurs diplômes d'ingénieur.
Résultats escomptés	Intégration de spécialistes informatiques de haut niveau
Ressources nécessaires	Modification des conditions d'accès aux corps de l'armement
Coût prévisionnel (de 1 : très coûteux à 4 : moins coûteux)	4
Niveau de priorité (de 1 : très prioritaire à 4 : moins prioritaire)	4

7. Conclusion

Faire face aux défis que la cybersécurité pose en matière de gestion des ressources humaines signifie mettre en œuvre un ensemble de solutions. Des solutions qui doivent concerner en amont la gouvernance de la filière, le processus d'alimentation du *pipeline*, le recrutement, la gestion des carrières, la formation et l'entraînement. Des solutions qui doivent également s'adapter aux secteurs d'activité et aux types d'organisation considérés et surtout s'inscrire dans une approche globale des technologies de l'information. L'emploi cyber est en effet un emploi hybride, s'appuyant, à des dosages variés selon les emplois, sur trois ingrédients que sont la sécurité, les systèmes d'information, et les métiers de l'organisation.

Ces mesures doivent enfin s'intégrer dans une approche de long terme car elles mettront pour certaines à produire leurs effets. La pénurie constatée par tous les observateurs sur le marché devrait donc se poursuivre encore quelques années même si elle devrait à terme se réduire en raison du développement en amont du *pipeline*. La réduction de la demande en professionnels en cybersécurité est en effet peu probable. Les besoins vont continuer à croître, et ce même si les systèmes intègrent davantage la sécurité de façon native, même si la mutualisation de certaines capacités de sécurité est indispensable et même si les organisations standardisent leurs systèmes d'information.

Les besoins en sécurité augmentent en effet au rythme de progression très rapide de la place du numérique dans l'ensemble des secteurs d'activité et, plus globalement, dans l'ensemble des activités humaines. Or la sécurité doit, au moins pour une part, être proche, voire embarquée dans les métiers et tenir compte des spécificités de l'activité. Difficile, donc, de la mutualiser totalement et de l'externaliser sans risques.

8. Liste des entretiens

- Edwige de Pontbriand, ANSSI
- Frédéric Lau, CIGREF
- Matthieu Boutin, CIGREF
- Lazaro Pejsachowicz, CLUSIF
- Bruno Chapuis, DGGN
- Guy Poulain, IBM
- Julien Badiola, Korn Ferry
- Guillaume Le Masne de Chermont, Mercuri Urval
- David Majorel, Michael Page
- Cécile Rolland, Steria
- Henri Lavigne, Steria

9. Bibliographie indicative

Documents officiels :

- DEPARTMENT OF DEFENSE, *Cyber Operations Personnel Report - Report to the Congressional Defense Committees*, US Department of Defense, Washington DC, 2011, 84 pages.
- DEPARTMENT OF HOMELAND SECURITY, *Cybersecurity Recruitment and Development Programs - Proud to Protect*, US Department of Homeland Security, Washington DC, 2 pages.
- NATIONAL CYBERSECURITY EDUCATION OFFICE, *2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC)*, US Department of Homeland Security, CIO Council, 2013, 131 pages.
- HM GOVERNMENT, *Cyber Security Skills – Business perspectives and Government next steps*, Londres, 2014, 34 pages.
- SENATE OF THE UNITED STATES, *S2354 – To improve cybersecurity recruitment and retention*, 113th Congress 2d Session, US Government, Washington DC, 2014, 9 pages.
- UNITED STATES GOVERNEMENT ACCOUNTABILITY OFFICE, *Cybersecurity Human Capital – Initiative need Better Planning and Coordination*, US GAO, Washington DC, 2011, 86 pages.
- US Navy, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Navy Cyber Power 2020, USA, 2012, 16 pages.

Rapports:

- AFDEL, *Livre Blanc: Cyber-sécurité : Hisser les acteurs français au niveau de la compétition mondiale*, Association Française des Editeurs de Logiciels et Solutions Internet, Paris, 2014, 36 pages.
- AKIN Jeff, RYA Roseann, VASQUEZ Eric, *Acquiring the Right talent for the Cyber Age – The Need for a Candidate Development Plan*, Booz Allen Hamilton, Mclean VA, 2010, 12 pages.
- BOOZ ALLEN HAMILTON, *Cyber In-Security – Strengthening The Federal Cybersecurity Workforce*, Mclean VA, 2009, 36 pages.
- BOOZ ALLEN HAMILTON, *Cyber Workforce Analysis*, Mclean VA, 2 pages.
- BOOZ ALLEN HAMILTON, *Reading the next Generation Cyber Workforce – Acquiring, Developing, and Retaining Cyber professionals*, Mclean VA, 2010, 16 pages.
- CYBER TECHNOLOGY & INNOVATION CENTER (CTIC), *Cyber Security Jobs Report*, The Abell Foundation & CyberPoint International, 2013, 51 pages.
- CIGREF, *Les nouveaux rôles de la Fonction SI – Missions, compétences et marketing de la fonction*, Paris, 2014, 56 pages.
- E-SKILL, *Career Analysis into Cyber Security: New & Evolving Occupations*, e-skills UK publication, Londres, 2013, 44 pages.
- HAYS, *Etude de Rémunération Nationale 2014*, Londres, 2014, 104 pages.
- INDUSTRY AND PARLIAMENT TRUST, *Cyber Security 2.0 – Reflections on UK*, IPT Cyber Security Commission, United Kingdom, 2014, 42 pages.
- HAMMERSTEIN Josh, MAY Christopher, *The CERT Approach to Cybersecurity Workforce Development*, Software Engineering Institute – Department of Defense, Carnegie Mellon University, 2010, 19 pages.
- LIBICKI Martin C, POLLAK Julia, SENTRY David, *HACKER5 WANTED - An Examination of the Cybersecurity Labor Market*, RAND, Santa Monica CA, 2014, 110 pages.
- MERCER, *Blending employee goals with organizational talent needs through proactive career management*, Marsh & McLennan Companies, USA, 2011, 2 pages.

- MCDUFFIE Ernest L, *Shaping the Future of Cybersecurity Education*, NICE, 2011, 15 pages.
- NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION, *Cybersecurity Framework*, NIST, Washington DC, 2011, 22 pages.
- NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION, *How to use the National Cybersecurity Workforce Framework*, NIST, Washington DC, 2013, 25 pages.
- NATIONAL SCIENCE FOUNDATION ADVISORY COMMITTEE FOR CYBERINFRASTRUCTURE, *Task Force on Cyberlearning and Workforce Development*, NSF, 2011, 85 pages.
- PDRI, *NICE Defines Cybersecurity Workforce*, pdri a CEB Company, Washington, 2 pages.
- SUBY Michael, *The 2013 (ISC)² Global Information Security Workforce Study*, Frost & Sullivan, Californie 2013, 28 pages.
- The Cybersecurity Forum Initiative, *Senior Cyber Leadership: Why a Technically Competent Cyber Workforce Is Not Enough*, CSFI, Omaha NE, 2013, 27 pages.

Ouvrages spécialisés:

- APEC, *LES MÉTIERS DES SYSTÈMES D'INFORMATION*, Publication de l'APEC, Paris, 2014, 163 pages.
- LIBICKI Martin C, POLLAK Julia, SENTRY David, *HACKER5 WANTED - An Examination of the Cybersecurity Labor Market*, RAND, Santa Monica CA, 2014, 110 pages.

Articles:

- CHOO King-Kwang Raymond, MARTINI Ben, « Building the next generation of cybersecurity professionals », *Twenty Second European Conference of Information Systems*, Tel Aviv 2014, 13 pages.
- KAY David J, PUDAS Terry J, YOUNG Brett, « Preparing the Pipeline: The US Cyber Workforce for The Future », *Defense Horizons – National Defense University*, INSS, Tel Aviv, 2012, 17 pages.
- CORPEL Alain, LALLEMENT Patrick, MALNOURY Germain, « Les besoins de formation en cyber sécurité - Enquête auprès des entreprises », *Institut Charles Delaunay*, Troyes, 2014, 8 pages.

Revue spécialisée:

- IANewsletter, *A New Layer of Security*, IATAC, volume 13, n°3, 2010, 44 pages.

10. Table des illustrations

Figure 1 : le <i>pipeline cybersécurité</i>	7
Figure 2 : les composantes de la GPEC	8
Figure 3 : les phases de l'étude	9
Figure 4 : les opérations dans le cyberspace.....	9
Figure 5 : Prévisions de croissance annuelle des emplois SSI.....	10
Figure 6 : Répartition de la « cyber operations workforce » fédérale américaine (2009)	11
Figure 7 : Certifications sécurité les plus répandues en Grande-Bretagne.....	13
Figure 8 : répartition de la population active "cyber" par âge.....	15
Figure 9 : Niveaux de rémunération constatés en France	17
Figure 10 : Grille des salaires « cybersécurité » du DoD (2012)	19
Figure 11 : quelles sont les capacités cyber difficiles à trouver sur le marché ?.....	21
Figure 12 : exemple de fiche « emploi type » NICCS.....	29
Figure 13 : saisie d'écran programme "Behind the screens"	32
Figure 14 : les critères de certification d'une formation cybersécurité par le GCHQ.....	35
Figure 15 : saisie d'écran de la campagne du GCHQ "Can you find it ?"	38
Figure 16 : fiche de poste de RSSI sur le site Big Ambition	40
Figure 17 : saisie d'écran du jeu "rescue the rockets"	41
Figure 18 : saisie d'écran du jeu « save the global games ».....	43
Figure 19 : les étapes de la planification des effectifs « cyber » proposée par le NICE.....	48
Figure 20 : le modèle de maturité proposé par le NICE.....	51
Figure 21 : Publicité du DSD australien : do you want to play the game no one else can ?	53
Figure 22 : interview d'une cyber analyste (DSD australien).....	54
Figure 23 : exemple d'annonce pour un apprentissage (Grande-Bretagne).....	55
Figure 24 : exemple d'offre de stage cybersécurité sur le site e-Skills UK.....	57
Figure 25 : répartition des étudiants bénéficiant du programme SFS par organisme	60
Figure 26 : le challenge FIC	65
Figure 27 : stands de la NSA à la RSA 2014 et à la Defcon 2012.....	69
Figure 28. Les niveaux d'assimilation des compétences selon EBK	78
Figure 29. Exemple de fiche compétence selon EBK	79
Figure 30. Exemple de fiche métier selon EBK	80
Figure 31. Parcours carrières et compétences, CSIS	81
Figure 32. Exemple de fiche « emploi type », CSIS.....	82
Figure 33. Fiche « emploi type » décrivant les compétences requises selon le critère « performance level », CSIS.....	82
Figure 34. Fiche « emploi type » décrivant les certifications et formations recommandées, CSIS.....	83
Figure 35. Extrait du "IISP Skills Framework"	86
Figure 36 : Le processus de management des talents « cybersécurité » de Steria	87
Figure 37. Capture de l'outil d'évaluation des compétences du SANS Institute	91
Figure 38. Fiche d'évaluation du RSSI, By Mark Edward Stirling Bernard, CyberSecurity /Information Security Program Expert at Independent CCSO or CISO as a Service	93
Figure 39. Schéma illustrant la complémentarité des 4 types de postes au sein de l'USAF.....	95

Figure 40. « Career Field Pyramid », USAF	96
Figure 41. Plans de carrière, USAF.....	98
Figure 42. Exemple de certification niveau "débutant", par CompTIA	100
Figure 43. Rally point, le LinkedIn de l'armée américaine	105
Figure 44. Exemple de conversation sur RallyPoint.....	106
Figure 45. Article sur la semaine du volontariat de Symantec.....	108
Figure 46 : Saisie d'écran de FedVTE : un exemple de quizz	113
Figure 47 : Saisie d'écran de FedVTE : un exemple de « bac à sable »	113
Figure 48 : Liste des cours proposés par la DISA dans FedVTE (par durée décroissante)	114
Figure 49. Cyber Academy Training Framework.....	121
Figure 50. Illustration : La Marine recrute dans un monde virtuel	127
Figure 51 : méthodologie d'audit.....	137
Figure 52 : exemple de baromètre de l'emploi cyber (Wanted Analytics)	140
Figure 53. Schéma récapitulatif : exemples de grandes fonctions de la cybersécurité.....	146
Figure 54. Extrait du référentiel des emplois types sur les fonctions « sécurité en amont » et « protection du SI ».....	147
Figure 55. Extraits de matrice de compétences générales	150
Figure 56. Extrait du référentiel d'emplois, avec indications de densités.....	151
Figure 57. Récapitulatif des métiers selon leur densité	152
Figure 58. Exemple de parcours SSI	160
Figure 59. Exemple de parcours type 1	160
Figure 60. Exemple de parcours type 2.....	160
Figure 61. Illustration d'une aire de compétence entre le poste de départ et le poste désiré.....	163
Figure 62 : Page d'accueil de la Cyber Maryland Map.....	171

11. Annexes

11.1. Annexe 1 – Proposition d'un référentiel des métiers

Fonction	Détail	N°	Emplois types	Indicateurs - densité		
				IT	Sécurité	Métier
1. Sécurité en amont	a) R&D	E1	Ingénieur R&D	■	■	
	b) Assurances, audit et compliance	E2	Assureur qualité	■	■	■
		E3	Auditeur organisationnel	■	■	■
		E4	Auditeur conformité	■	■	■
		E5	Professionnel qualité	■	■	■
		E6	Auditeur technique	■	■	
		c) Anticipation du risque	E7	Consultant/expert gestion du risque	■	■
	E8		Gestionnaire de Risques	■	■	■
	E9		Consultant gestion de crise	■	■	■
	d) Architecture des infrastructures et systèmes d'information	E10	Architecte système	■	■	
		E11	Architecte réseau	■	■	
		E12	Architecte application	■	■	
		E13	Développeur	■	■	
		E14	Architecte sécurité		■	
		E15	Référent sécurité projet	■	■	
		E16	Chef de projet (MoE/MoI)	■	■	■
		E17	Cryptologue	■	■	■
	e) Intégration	E18	Développeur / concepteur	■	■	■
		E19	Chef de projet	■	■	■
		E20	Intégrateur	■	■	■
	f) Déploiement	E21	Technicien réseau-télécoms	■	■	
		E22	Intégrateur d'exploitation	■	■	

2. Analyse des menaces	a) Veille technologique et menaces	E23	Consultant cybersécurité			
	b) Veille stratégique	E24	Veilleur cybersécurité			
	c) Recherche en vulnérabilités					
	d) Analyse de malware et modes opératoires	E25	Analyste cybersécurité			
		E26	Chercheur			
3. Administration et gouvernance du SI	a) Maintenance applicative	E27	Responsable maintenance applicative			
	b) Gouvernance IT	E28	Administrateur système			
		E29	Administrateur réseau			
		E30	Responsable d'exploitation			
		E31	Responsable PCA/PRA			
	c) Support utilisateurs	E32	Administrateur <i>data</i>			
		E33	Assistant fonctionnel			
		E34	Technicien IT			
4. Protection du SI	a) Gouvernance et exploitation SSI	E35	Ingénieur sécurité			
		E36	RSSI			
		E37	Administrateur sécurité			
		E38	Technicien sécurité			
		E39	Télé-assistant			
		E40	Expert produit/technologie (IAM, MDM, IDS, IPS, etc.)			
	b) Mise à l'épreuve	E41	Pentesteur			
	c) Collecte et détection	E42	Ingénieur spécialiste collecte et analyse de logs			
		E43	Ingénieur chargé d'analyse en détection d'intrusions			
d) Réponse à incident	E44	Ingénieur en charge de la réponse aux incidents				

5. Cyberopérations						
6. Investigations	a) Inforensique	E45	Expert forensic			
		E46	Expert recovery			
	b) Analyse de malware et modes opératoires	E47	Ingénieur reverse			
		E48	Ingénieur analyste en vulnérabilités et codes malveillants			
	c) Acteurs judiciaires	E49	Police judiciaire			
		E50	Magistrature			
		E51	Conseil juridique			
d) Privés	E52	Investigateurs de droit privé				
Appui juridique	a) Protection des données à caractère personnel	E53	Correspondant informatique et libertés			
		E54	Avocat			
	b) Conseil juridique NTIC	E55	Juriste d'entreprise			
		E56	Juriste cyberdéfense			
Marketing et communication		E57	Responsable Marketing et communication			
Commercial	Avant-vente	E58	Ingénieur technico-commercial			
	Vente	E59	Responsable commercial			
Formation et entrainement		E60	Formateur			

11.2. **Annexe 2 – Synthèse des bonnes pratiques**

#	Intitulé	Descriptif	Contraintes associées	
Gouvernance globale				
B1	Mise en place d'une structure de gouvernance unifiée	Le NICE comprend plusieurs volets : sensibilisation, développement du « pipeline », développement des pratiques opérationnelles.	Il faut une structure d'animation permanente.	Le N... cybe... l'ens... form... aille...
B2	Mise en place d'un « guichet unique » en matière de carrières et de formation	Le NICCS (National Initiative for Cybersecurity Careers and Studies) est un site-guichet unique pour la sensibilisation, la formation, l'entraînement et la découverte des carrières en cybersécurité.	Une animation permanente du site est nécessaire.	Inté... carr...
Alimentation du pipeline				
B3	Diffusion de kits de formation pour enseignants	Le programme <i>Behind the screen</i> fournit des ressources de formation et de sensibilisation aux enseignants britanniques. L'un des projets concerne spécifiquement la cybersécurité.	Suppose la mise en ligne de nombreux contenus.	Acti... sens... voca...
B4	Labéliser et certifier des formations	Le GCHQ britannique a engagé un programme de labélisation et de certification de formations supérieures en cybersécurité.	Il faut établir un référentiel très précis en amont.	Perr... de g... entr...
B5	Revalorisation des filières scientifiques et techniques auprès des scolaires	Le programme a pour objectif de communiquer massivement sur les filières techniques et scientifiques auprès des étudiants du primaire pour revaloriser ces parcours.	Structure d'animation	La v... est t...
B6	Lancement de « serious game » sur la cybersécurité	Le GCHQ a lancé une campagne en ligne, « Can you find it? », proposant des défis avec des codes complexes à trouver en ligne et à résoudre.	Conception et développement informatique	Acti... 15 a...
B7-1	Animation d'une campagne de promotion des métiers de la cybersécurité	Le programme britannique « Big Ambition » a lancé plusieurs campagnes pour faire connaître les métiers de l'IT, et notamment les métiers de la cybersécurité.	Développement informatique	App...
B7-2	Lancement d'une campagne ponctuelle de promotion des métiers cyber	Le DHS organise chaque année le National Cyber Security Awareness Month (NCSAM). Les événements organisés dans le cadre de ce mois de la cybersécurité ont pour objectifs non seulement de sensibiliser le grand public mais aussi de communiquer sur les carrières et emplois cyber.	Aucune	Perr... exist...

Gestion des carrières

B22	Créer un référentiel des métiers et des compétences	Référencer selon ses besoins les métiers et compétences nécessaires.	Le préalable de toute démarche de recrutement et d'entraînement reste la cartographie et l'audit de ses propres besoins.	Un n requ recr
B23	Mise en place d'un processus normalisé de gestion des compétences	Steria a mis en place pour son activité sécurité un cycle comprenant entretien individuel, « people review » et comité d'évaluation. Pratique habituelle en RH mais déclinée ici dans le domaine de la cybersécurité.	Aucune	Faci
B24	Se doter d'outils d'évaluation des compétences	Se doter d'un outil d'évaluation des compétences plus ou moins interactif.	Former les responsables des ressources humaines. Adapter l'outil à ses spécificités. Choisir un outil externe a un coût non-négligeable.	S'as capa con com éval
B25	Organiser la mobilité des profils			
B25-1	Créer une véritable filière de mobilité interne	L'US Air Force propose une seule et unique filière cybersécurité.	Veiller à ne pas noyer les véritables postes « cybersécurité » dans les problématiques IT et télécommunications.	Sim mut form
B25-2	Proposer des plans de carrière	L'US Air Force communique sur des plans de carrière.	Aucune.	App inte
B25-3	Développement des échanges entre public et privé	Le DoD américain met en place un programme pilote autorisant les échanges temporaires entre public et privé.	Bonne coordination avec les entreprises privées. Cadre juridique nécessaire.	App inte
B25-4	Accompagner la transition professionnelle des militaires	CompTIA, une organisation destinée à développer l'activité IT, a lancé « Armed for IT Careers » qui propose un cursus de transition pour le personnel militaire.	Coûts.	Valo Fair pub

B26	Valoriser par le salaire	Ces programmes autorisent une augmentation de salaires pour la rétention des « compétences critiques »	Coûts. Risques d'abus : certains profils n'auraient pas eu besoin de cette prime pour rester en poste. Fiabilité des données.	Con sect Séd Favo prix
B27	Créer une communauté	Ces différentes initiatives tendent à rassembler les professionnels de la cybersécurité grâce à des rencontres virtuelles ou des évènements réels	Fiabilité des profils. Risques d'image en raison du manque de contrôle des contenus. Quelques animateurs relativement disponibles sont nécessaires.	Féd Favo
Formation continue et entraînement				
B28	Favoriser les labs et l'auto-formation afin de stimuler l'innovation	Steria propose à ses salariés des espaces de réflexion, véritables « laboratoires », où les salariés y sont libres d'innover	Coûts. Gestion du temps.	Favo
B29	Le tutorat entre collègues	Les collectivités organisent des bourses internes à la mobilité et des stages d'immersion professionnelle à destination des agents déjà en poste.	Gestion du temps.	Valo form
B30	Faire de la formation continue une récompense et un moteur de mobilité interne	Symantec propose un système de formation relativement complet, continu, jalon accessible à chaque étape de la carrière.	Rétention des talents en interne.	Favo inte
B31	Création d'un centre de formation et d'entraînement mutualisé	FedVTE est un centre d'entraînement et de formation en ligne proposant des formations sous forme de cours en ligne ou de quizz mais aussi des environnements de simulation technique.	Disposer d'un environnement de simulation et concevoir des contenus adaptés.	Perr de t
B32	Formation et sensibilisation des élites	Le National Defense University a mis en place deux programmes de formation en cybersécurité ciblant un public de décideurs publics et privés.	Corps enseignant et contenus.	Perr add tran Faci

B33

Mettre en place un centre de formation continue destinés aux personnels internes et externes

Dispense de cours pour les personnels internes à l'entreprise et externes à celles-ci pour tout niveau, de débutant à expert

Difficulté de maintenir à niveau l'ensemble des personnels compte tenu de la rapidité de l'évolution technologique

Perr
ses

11.3. Annexe 3 – Synthèse des recommandations

#	Intitulé	Descriptif	Résultats escomptés	Ressources nécessaires	Coût prévisionnel ¹	Niveau de priorité ²
R1	Réaliser une évaluation de la situation existante	L'évaluation comprendrait différentes phases : analyse de la population active, identification des besoins, gap analysis, définition d'une feuille de route et mise en œuvre. Cette analyse serait réalisée <i>a minima</i> au niveau des personnels de la Défense et idéalement au niveau interministériel.	Meilleure évaluation et anticipation des besoins	Méthodologie d'évaluation, panel d'organisations et de personnes à cibler.	3	1
R2	Créer un observatoire des métiers et compétences cyber interministériel	L'Observatoire des métiers et compétences cybersécurité permettra de s'assurer d'une continuité entre la stratégie globale, les besoins et le recrutement. Il permettra de développer un	Adaptation permanente des ressources humaines aux besoins	Structure permanente en relation avec un référent chez tous les acteurs concernés	2	1

		référentiel des métiers en adéquation avec les besoins de chacun des acteurs et les formations existantes. Cette recommandation s'inscrit dans l'action n°30 du pacte Défense Cyber.				
R3	Organiser un challenge national public-privé	Cette compétition permanente serait organisée en différentes étapes (4 séries d'épreuve) réparties dans toute la France pour s'appuyer sur les différentes initiatives régionales qui voient le jour dans le domaine	Forte médiatisation des emplois sécurité. Détection de nouveaux talents.	Contenus techniques. Organisation.	1	1
R4	Construire un centre d'entraînement intégré et mutualisé	Ce dispositif serait basé sur un environnement d'entraînement comprenant une partie simulation technique et une partie jeu de rôle. Il proposerait des contenus clés en mains variés.	Démultiplier le nombre de formations et d'entraînements réalisés	Contenus, environnement d'entraînement et équipes de formation	1	1

R5	Créer un référentiel des emplois et compétence partagé	Le référentiel détaille les emplois-type par famille puis liste les compétences nécessaires. Des indicateurs de densité permettent de déterminer le niveau de profondeur demandé pour chaque dimension (sécurité, IT, métiers).	Développer d'une vision partagée des métiers, structurer les cursus de formation, faciliter l'orientation des personnes intéressées, faciliter l'émission d'offres d'emploi et donc la recherche de candidats adaptés.	Réunir les acteurs du sujet pour élaborer un référentiel partagé	2	1
R6	Favoriser le recrutement de hauts potentiels	Il s'agit de proposer des spécialisations cyber dès la sortie de l'école de formation (Air, Terre et Mer) afin de se doter de personnels réalisant des carrières courtes et susceptibles de se reconvertir aisément dans le privé au bout de 10-15 ans de carrière.	Attirer des profils techniques de haut niveau	Modification des cursus de formation initiale	3	2
R7	Proposer une offre de formation variée et cohérente	L'objectif est de définir un cadre de référence composé de plusieurs niveaux de formation qui seront ensuite	Homogénéiser les offres de formation	Cadre de cohérence	4	2

		utilisés par l'ensemble des formations proposées par les organisations de la défense.				
R8	Concevoir des parcours et communiquer sur les carrières, pas uniquement sur les emplois	L'objectif est de constituer, sur la base d'un référentiel des emplois et compétences, des parcours type proposant des passerelles entre métiers et cybersécurité, IT et cybersécurité.	Meilleure information des juniors et seniors sur les parcours proposés	Définition des parcours-type grâce à un groupe de travail, campagne de communication	3	2
R9	Faciliter la mobilité interne	Le but est d'anticiper les désirs d'évolution et de changement des personnels et de mieux organiser la mobilité. Cette mobilité serait facilitée par une plateforme permettant aux personnels de se voir proposer des évolutions de carrières et de rechercher des postes en fonction de leurs	Offrir des parcours de mobilité attractifs	Mise en place d'une plateforme informatique dédiée	3	3

		compétences.				
R10	<p>Systematiser les échanges public-privé</p>	<p>Ce programme d'échange permettrait à des personnels du Ministère de la Défense d'être détaché dans des emplois équivalents dans le secteur privé et réciproquement.</p>	<p>Fertilisation croisée des compétences. Création d'une véritable communauté public-privé en cybersécurité.</p>	<p>Cadre juridique à adapter</p>	3	3
R11	<p>Former les DRH aux enjeux et spécificités du marché de l'emploi cybersécurité</p>	<p>Le but est de proposer aux directions RH des secteurs public et privé des formations spécifiques sur le marché de l'emploi cybersécurité.</p>	<p>Meilleure appréhension du marché de l'emploi cybersécurité par les DRH</p>	<p>Kit de formation RH</p>	4	3
R12	<p>Faciliter l'accès aux ressources en créant une « cyber map » interactive</p>	<p>L'objectif est de recenser et de flécher au niveau national l'ensemble des ressources disponibles</p>	<p>Visibilité accrue des ressources disponibles et des offres d'emplois proposées</p>	<p>Développement de la plateforme et animation quotidienne</p>	3	4
R13	<p>Prévoir des possibilités d'admissibilité directe vers certains corps</p>	<p>L'objectif est d'offrir aux étudiants la possibilité d'intégrer directement les corps techniques de la Direction Générale de</p>	<p>Intégration de spécialistes informatiques de haut niveau</p>	<p>Modification des conditions d'accès aux corps de l'armement</p>	4	4

	<p>l'Armement après l'obtention de leurs diplômes d'ingénieur.</p>
--	--

¹ de 1 : très coûteux à 4 : moins coûteux

² (de 1 : très prioritaire à 4 : moins prioritaire)

