ceis

COMMENT DÉVELOPPER LA MAIN D'ŒUVRE SPÉCIALISÉE EN CYBERSÉCURITÉ ?

Décembre 2014

Les notes otratégiques

LES NOTES STRATÉGIQUES

Policy Papers – Research Papers

Cette note stratégique est une synthèse de l'Etude de Prospective Stratégique (EPS) n°2013-01 intitulée « quelles sont les évolutions possibles de la gestion du personnel de défense pour lutter efficacement dans le cyberespace ? » et réalisée par CEIS pour le compte de la Délégation aux Affaires Stratégiques du ministère de la Défense.

TABLE DES MATIÈRES

INTRODUCTION

Les organisations privées et publiques sont aujourd'hui confrontées à plusieurs défis dans leur gestion de la main d'œuvre spécialisée en cybersécurité :

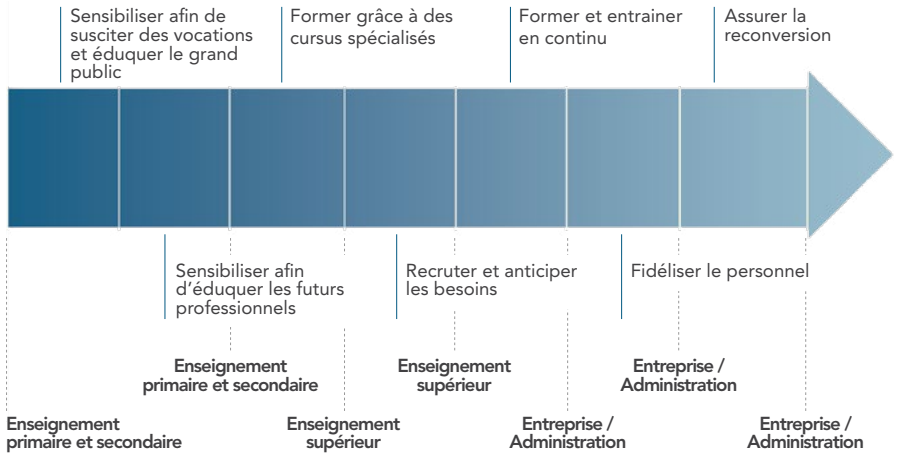
- Un défi de recrutement. Au plan quantitatif, l'offre reste largement insuffisante par rapport à la demande. La 6ème étude GIWS (Global Information Security Workforce study) publiée par Frost & Sullivan et (ISC)[1] sur les professionnels de la sécurité montrait en 2012 que le nombre de postes allait 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 ».

- Un défi lié à la gestion des carrières du personnel spécialisé en cybersécurité. Une fois ces personnes recrutées, 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 de la cybersécurité, la définition d'un référentiel des emplois-types et d'une véritable stratégie RH dans le domaine.

- Un défi lié à la formation et à l'entrainement. L'innovation permanente et extrêmement rapide qui sous-tend le développement du cyberespace constitue un facteur d'attractivité non négligeable pour les personnes intéressées mais implique également l'animation d'un dispositif de formation continue et d'entrainement 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'entrainement, 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



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

1. FONDAMENTAUX DE L'EMPLOI CYBER

1.1. Photographie de la population active « cyber »

1.1.1. Quelques chiffres

Données globales

Au plan international, une étude menée par Frost & Sullivan pour le compte de l'organisation (ISC)[2] 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 2 : 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 2011[3].

[2] *https://www.isc2.org/GISWSRSA2013/*
[3] *http://criminaljusticeschoolinfo.com/legal-justice-news/2013/02/cyber-security-career-paths-6213/*

Etats-Unis

Les Etats-Unis ont adopté une définition extensive de la cybersécurité. 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.

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 état de 40 000 personnes environ pour un chiffre d'affaires de 13 milliards, dont 4,5 en France[4].

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.

1.1.2. 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 universitaire[5]. 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 "H4CKER5 WANTED, an examination of the cybersecurity labor market » publiée en 2014[6], 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.

[4] *http://www.confiance-numerique.fr/wp-content/uploads/2014/05/brochure_observatoire_confiance_numerique_2013.pdf*
[5] *https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf*
[6] *http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf*

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.* » 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 développement 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 employés 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 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 CISSP . Même constat aux Etats-Unis.

[7] *http://etudiant.aujourdhui.fr/etudiant/info/fiche-metier-expert-de-la-cybersecurite-une-filiere-encore-rare.html*

[8] *http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf*

[9] *"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-types 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 précédant. 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 apparait globalement assez faible dans le domaine. Une étude menée par Frost & Sullivan en partenariat avec Booz Allen Hamilton en 2013[10] 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.

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.

[10] *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=AFQjCNEF5GJscvZ11lqHcRzTdZb5_gNhsQ*

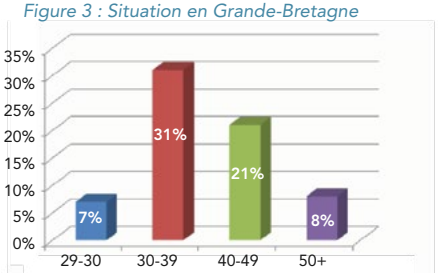
Même constat dans un contexte militaire. L'Air Force américaine a ainsi défini deux types de postes[11] : ceux nécessitant des compétences se rapprochant de spécialités traditionnelles (renseignement, développement, guerre électronique, TIC, etc.) et ceux nécessitant un renforcement des spécialités traditionnelles 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.

Quelles compétences ?

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 active[12]. Même constat aux Etats-Unis : une étude du CIO Council et du DHS publiée en avril 2013[13] indique 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.

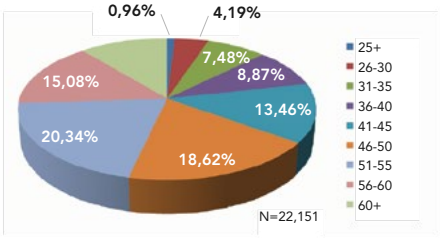
Si la tendance au vieillissement de la population active en cybersécurité devrait s'inverser compte tenu de l'arrivée sur le marché de profils junior -une entreprise de services numériques française interrogée indique ainsi que 60 % de ses embauches dans le domaine concerne des profils juniors (0 à 2 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 3 : Situation en Grande-Bretagne



Source : "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.

Figure 4 : Situation aux Etats-Unis



Source : CIO council et DHS, 2013, https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf

[11] *http://www.rand.org/content/dam/rand/pubs/documented_briefings/2010/RAND_DB579.pdf*
[12] *"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.*
[13] *https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf*

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 concerne spécifiquement la France.

Figure 5 : Niveaux de rémunération constatés en France

Domaine	Estimation production	Début production prévu	Notes
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 -	75-130
	Architecte sécurité/Référent sécurité projet	A partir de 10 années d'expérience	48-60
	Chef de projet (MoE/MoI)	5–10 ans	60-75
Analyse de la menace et investigation numérique	Analyste/chercheur en vulnérabilités	Pas de données pertinentes	Inconnu
	Analyste malware	Pas de données pertinentes	Inconnu
	Analyste forensics et investigations	Pas de données pertinentes	Inconnu
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)	Pas de données pertinentes	Inconnu

1.2. 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.

1.2.1. 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 2017[14] quand le FBI souhaiterait lui embaucher 1 000 agents et 1 000 analystes en 2015[15]. 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)[16]. La demande devrait donc globalement progresser de 13,2 % par an jusqu'en 2017 estime la société de conseil Frost & Sullivan[17].

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 2013[18].

1.2.2. 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.

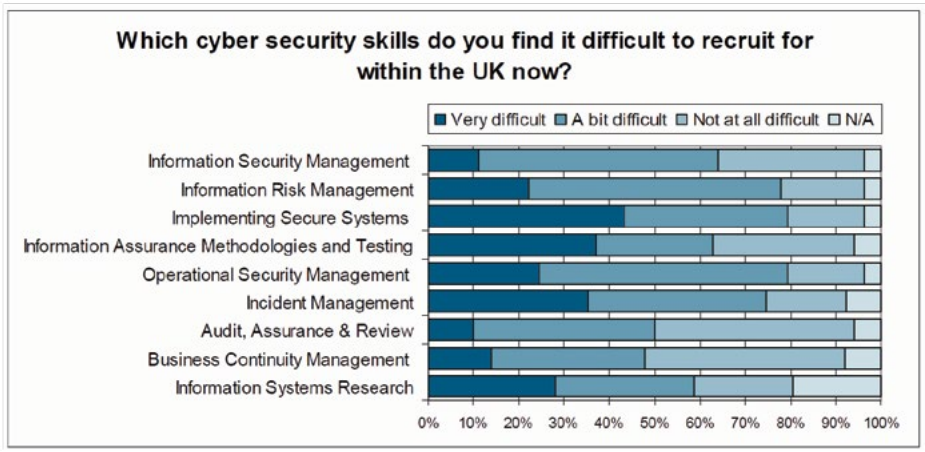
Au plan quantitatif, Laurent Trébulle, directeur des relations entreprises à l'école d'ingénieurs Epita, constate : *« on peut s'attendre à près de 1 000 à 1 200 recrutements en 2014, alors que le nombre de jeunes diplômés se situerait plutôt entre 200 et 300 par an*[19]*»* *« Nous avons 30 postes que nous ne parvenons pas à pourvoir »*, explique de son côté Sébastien Héon d'Airbus Defense & Security[20]. Mêmes échos outre-Atlantique où Diane Miller, directeur du programme CyberPatriot pour Northrop 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 2013[21].

[14] *http://www.defense.gov/news/newsarticle.aspx?id=121670*
[15] *http://www.businessweek.com/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete*
[16] *http://www.iissm.com/newsletter/pdf/NewsletterJune1824.pdf*
[17] *The 2013 (ISC)2 Global Information Security Workforce Study*
[18] *https://www.wantedanalytics.com/analysis/posts/network-security-concerns-drive-hiring-for-cyber-security-professionals-up-by-20*
[19] *http://www.metronews.fr/info/la-cybersecurite-un-eldoradopour-l-emploi/mnbb!6OdEwn5RvpeM/*
[20] *http://www.usinenouvelle.com/article/penurie-de-talents-en-cybersecurite-a-qui-la-faute.N190563*
[21] *http://www.bloomberg.com/news/2013-05-16/cybersecurity-starts-in-high-school-with-tomorrow-s-hires.html*

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 candidats[22]. Le manque serait particulièrement criant pour les 5 % de postes les plus qualifiés, constate la RAND Corporation[23]. 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 manquantes[24].

Figure 6 : Prévisions de croissance annuelle des emplois SSI



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.

[22] *https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf*
[23] *http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf*
[24] *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*

1.2.3. 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 tous 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 secteur[25]».*

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

2. RECOMMANDATIONS

En s'appuyant sur les bonnes pratiques détectées, 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'entrainement.

Notons à ce propos que le DoD américain a publié en décembre 2013 une *Cyberspace Workforce Strategy*[26] 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).

Figure 7 : Les axes de recommandations

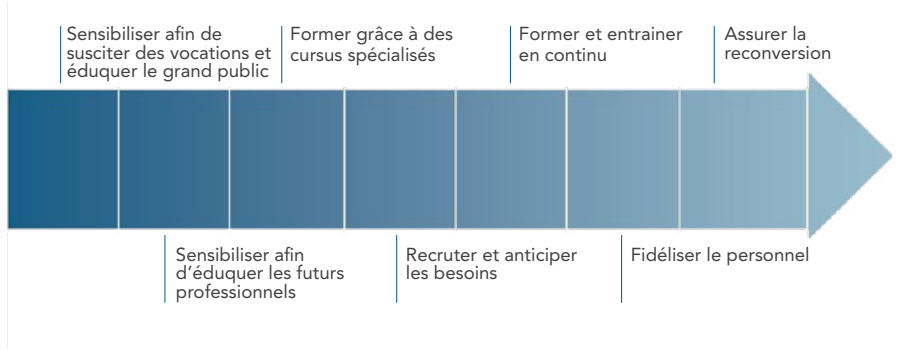


Figure 8. Récapitulatif des recommandations

Recommandation	Couverture
R1 : réaliser une évaluation de la situation existante	
R2 : créer un observatoire des métiers et compétences en cybersécurité	
R3 : organiser un challenge national public-privé	
R4 : construire un centre d'entrainement intégré et mutualisé	
R5 : lancer une campagne de communication	
R6 : créer un référentiel des emplois et compétences partagé	
R7 : proposer une offre de formation variée et cohérente	
R8 : former les formateurs	
R9 : développer les stages, apprentissages et bourse	
R10 : concevoir des parcours et communiquer sur des carrières	
R11 : faciliter la mobilité interne	
R12 : systématiser les échanges public-privé	
R13 : former les DRH aux enjeux et spécificités du marché de l'emploi cybersécurité	
R14 : faciliter l'accès aux ressources	

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

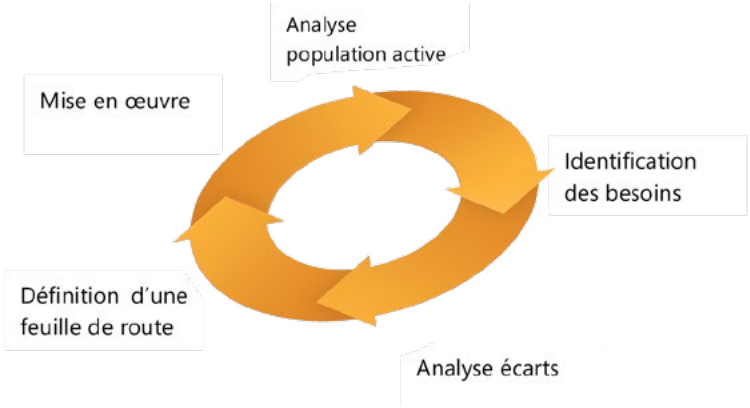
R1 : réaliser une évaluation de la situation existante

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.

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.

Figure 9 : méthodologie d'audit



R2 : créer un observatoire des métiers et compétences en cybersécurité

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 en cybersécurité est recommandée. Cet observatoire, placé au niveau interministériel, 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.

Bonne pratique : le NICE américain

Lancée en 2010 à la suite de la Comprehensive National Cybersecurity Initiative (CNCI), la National Initiative for Cybersecurity Education (NICE)[27], animée par le NIST (National Institute of Standards and Technology)[28], se propose d'établir 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'entrainement 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.

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.

R3 : organiser un challenge national public-privé

A l'image du Cyber Challenge UK, il s'agirait d'organiser une compétition informatique nationale, dans le cadre d'un partenariat public-privé, 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 organisées lors d'un événement international sur 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.

[27] *http://csrc.nist.gov/nice/aboutUs.htm*
[28] *http://www.nist.gov/*

Bonne pratique : Le Cyber Security Challenge UK

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 professionnelle[29]. 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 entrainements 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 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 Summers[30] 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 cybersécurité[31] 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.

[29] *http://cybersecuritychallenge.org.uk/about-us/*
[30] *http://www.itpro.co.uk/631663/postman-crowned-first-uk-cyber-security-champion*
[31] *http://blog.backup-technology.com/13894/cyber-security-challenge-uk-searching-best-hackers-uk/*

Figure 10. Le logo du CSC UK

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 Academy[32]. 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.

R4 : construire un centre d'entrainement 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'entrainement. Or, celle-ci requiert la création d'un centre d'entrainement intégré et mutualisé.

Ce dispositif répondrait aux besoins suivants :

- Couvrir les différents niveaux d'entrainement (élémentaire, supérieur…) ;
- Répondre aux besoins des différents types de population concernés, tant dans le secteur public que privé :
  - spécialistes en systèmes d'information (socle commun) ;
  - généralistes de la chaîne « cyber » ;
  - spécialistes SSI ;
  - 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'entrainement comprendrait :

- Un module « simulation technique », basé sur un environnement de virtualisation permettant la reproduction en miniature de quelques environnements ;
- 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 entrainements ;
- Un module de préparation et de pilotage unifié.

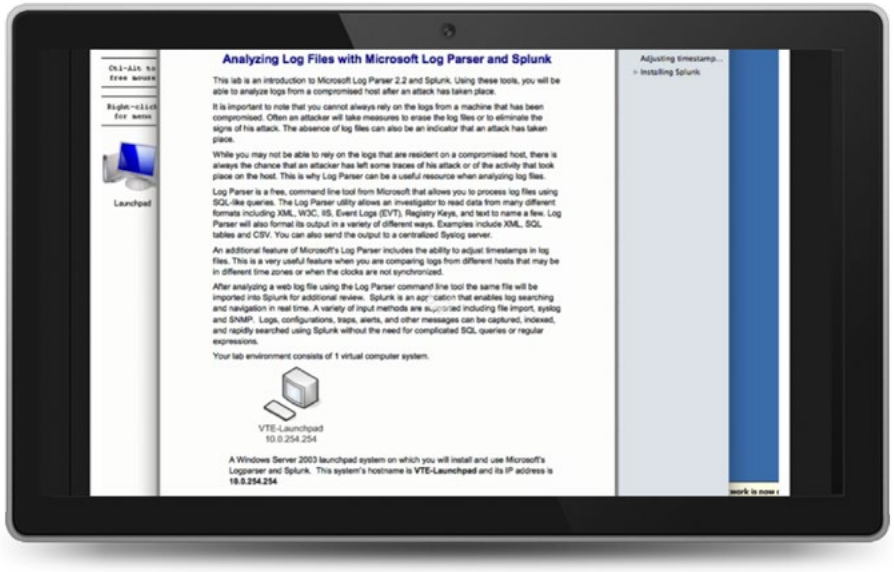
Plusieurs modes d'entrainement seraient proposés : mode présentiel ou mode distanciel, avec un pilotage manuel, semi-automatique ou automatique.

[32] *http://cybersecuritychallenge.org.uk/education/cyber-camps/*

Bonne pratique : Le FedVTE américain

Le National Initiative for Cybersecurity Careers and Studies (NICCS) américain propose un environnement d'entrainement et de formation baptisé « FedVTE » (Federal Virtual Training Environment)[33]. Cette bibliothèque en ligne, qui compte plus de 30 000 utilisateurs inscrits, offre 800 heures de formation[34], 150 démonstrations et un environnement de simulation technique[35]. L'environnement est aujourd'hui utilisé par de très nombreux départements et agences fédéraux, dont le DoD.

Figure 11 : Saisie d'écran de FedVTE : un exemple de « bac à sable »



A noter que les Etats-Unis disposent de plusieurs environnements de simulation et d'entrainement « 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).

[33] *http://niccs.us-cert.gov/training/fedvte*
[34] *http://niccs.us-cert.gov/sites/default/files/documents/files/fedvte-courselist.pdf*
[35] *https://www.fedvte-fsi.gov/Vte.Lms.Web*

R5 : lancer une campagne de communication

Cette campagne de communication aurait pour objectif de communiquer sur les métiers et carrières dans le domaine de la cybersécurité auprès d'un public de scolaires, d'étudiants et de jeunes professionnels.

Elle se traduirait notamment par :

- La présentation des emplois et parcours professionnels à travers des contenus dynamiques (interviews) ;
- La mise à disposition de plusieurs petits jeux en ligne ;
- L'organisation de quelques événements ciblés.

Bonne pratique : Le programme Big Ambition britannique

Big Ambition[36], 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, 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)[37]. 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.

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.

[36] *https://www.bigambition.co.uk/*
[37] *https://www.bigambition.co.uk/BigAmbition/cyber-careers/index.html#/meet*

Secure Future[38] 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*[39], 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 apparait 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 apparait.

Figure 12 : saisie d'écran du jeu «rescue the rockets»

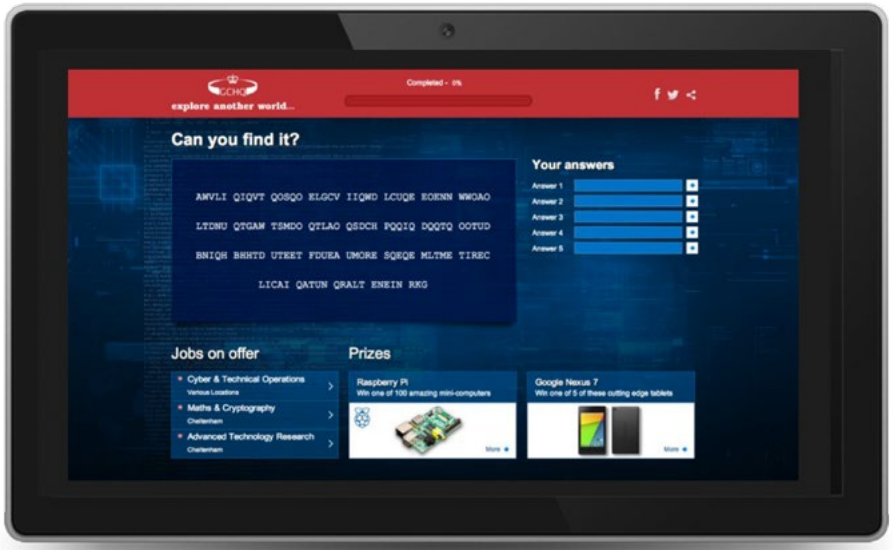
Autre jeu proposé : *Save the Global Games*[40] à travers lequel le joueur doit gérer l'équipe de sécurité d'un évènement à venir : les jeux olympiques qui se déroulent cette année à Cardiff. A travers les boites mails de plusieurs personnages (Katie Data, la directrice de l'IT, Gary Lockitup, le directeur 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 entrainant 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).

[38] *http://www.bigambition.co.uk/secure-futures/*
[39] *http://www.bigambition.co.uk/secure-futures/games/rescue-the-rocket-programme/*
[40] *http://www.bigambition.co.uk/secure-futures/games/save-the-global-games/*

Bonne pratique : La campagne « can you find it ? » du GCHQ

Le GCHQ a lancé une campagne en ligne, « Can you find it? »[41], 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? »[42] : 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 13 : saisie d'écran de la campagne du GCHQ «Can you find it ?»



[41] *http://www.thecodex.com/en/gchq-can-you-find-it-solution*
[42] *http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-code-cracking-challenge-reveals-UK-talent.aspx*

R6 : créer un référentiel des emplois et compétences 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.

Bonne pratique : L'approche intégrée du NIST

Fin 2011, le National Initiative for Cybersecurity Education (NICE) publiait un référentiel des métiers de la cybersécurité[43]. 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 chaine plus globale, permettant une approche 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 cybersécurité[44], partant de l'anticipation en amont de la menace, à la gestion et l'analyse en aval. Il distingue ainsi 7 catégories fonctionnelles, qui se déclinent elles-mêmes en une trentaine de spécialités :

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

R7 : proposer une offre de formation variée et cohérente

Les offres de formation doivent être variées pour répondre à des besoins de nature variée. A l'instar du référentiel des emplois et compétences, il serait intéressant de définir un référentiel des formations disponibles par typologie et niveau.

[43] *http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-Summary-Booklet.pdf*
[44] *http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_interactive_how_to.pdf*

Bonne pratique : Le NICCS américain

Le NICCS (National Initiative for Cybersecurity Careers and Studies)[45] 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 numérique[46]), formation, entrainement 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, découvrir le référentiel des emplois ou se renseigner sur l'éducation de ses enfants).

R8 : former les formateurs

Les offres de formation doivent être variées pour répondre à des besoins de nature variée. A l'instar du référentiel des emplois et compétences, il serait intéressant de définir un référentiel des formations disponibles par typologie et niveau.

Bonne pratique : Le programme britannique Behind the screens

Le programme *Behind the screen* regroupe des projets et des ressources dédiées aux écoles britanniques[47]. 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, Deloitte, 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.

[45] *http://niccs.us-cert.gov*
[46] *Le site relaie enfin une campagne de sensibilisation nationale baptisée Stop Think Connect (http://www.stopthinkconnect.org/)*
[47] *http://www.behindthescreen.org.uk/*

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 débloquer 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 encadrée. Le projet se conclut par la découverte des métiers de la cybersécurité et des opportunités qui s'offrent à eux dans leur orientation scolaire.

R9 : développer les stages, apprentissages et bourses

Les stages, apprentissages et bourses constituent des outils importants pour former des jeunes à l'issue de leur formation. Un programme spécifique pourrait être lancé pour inciter les entreprises à recruter des stagiaires, apprentis ou boursiers dans ce domaine.

Bonne pratique : Le programme d'apprentissage de E-Skills

E-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 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, pen-tester et architecte sécurité[48]. 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.

Ce programme d'apprentissage se déroule sur 2 ans. Les candidats à l'apprentissage bénéficient de l'accès à la base de données du portail Apprenticeships Vacancies[49] afin d'identifier les entreprises pouvant les accueillir. Les apprentissages en cybersécurité sont classés niveaux 4 (higher level)[50] 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 français[51]), ce qui confère à ces offres une forte attractivité. On retrouve cette propension 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 accrédite 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*[52].

[48] *http://www.zdnet.com/uk/ibm-and-bt-to-launch-new-uk-cybersecurity-apprenticeships-7000015417/*
[49] *https://apprenticeshipvacancymatchingservice.lsc.gov.uk/*
[50] *http://www.apprenticeships.org.uk/~/media/Collateral/BrochuresLeaflets/Apps-Framesworks-2014.ashx*
[51] *http://www.lapprenti.com/html/apprenti/salaire.asp*
[52] *http://www.e-skills.com/news-and-events/july-2014/cyber-apprenticeship-gains-tech-industry-gold-accreditation-from-employers/*

A noter enfin, que le GCHQ britannique a proposé pour la première fois un apprentissage[53] : 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 cyberespace. Très bien rémunéré (17 000£ annuelles), 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.

R10 : concevoir des parcours et communiquer sur des carrières

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 ;
- 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 (comprenant notamment quelques jeux interactifs, des fiches de poste, des fiches parcours), réseaux sociaux, publicités dans la presse.

[53] *http://www.notgoingtouni.co.uk/opportunity/technical-apprenticeship-in-it-software-internet-and-telecomms-23716*

R11 : faciliter la mobilité interne

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 ans[54], 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 Canden dans un livre blanc consacré à l'emploi des seniors dans l'IT[55]. D'autre part, parce que la pyramide managériale et la pratique de l'externalisation ont réduit les opportunités dans les entreprises.

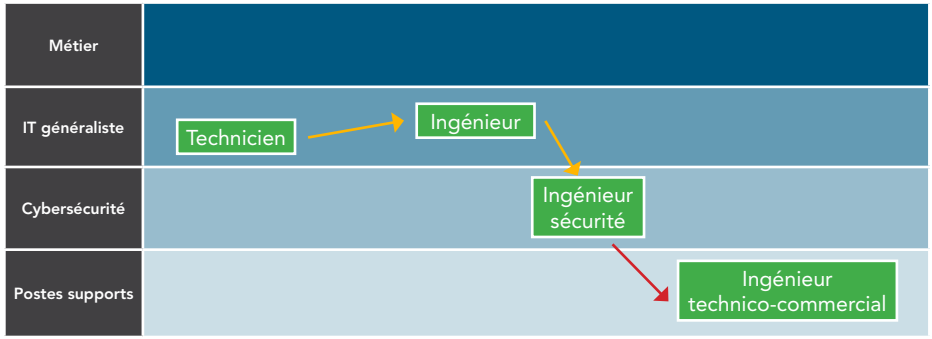
Il faut donc revaloriser les parcours techniques, les carrières de manager n'étant pas la seule voie de valorisation. D'autant que les aspirations des seniors sont souvent relativement différentes. *« Avant la quarantaine, les critères d'une carrière réussie sont objectifs : le salaire, le périmètre 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 Carrière[56].

Un outil favorisant cette mobilité pourrait être développé : une personne qui souhaite évoluer dans sa carrière pourra visualiser les postes qui lui sont proposés, avec ou sans formation supplémentaire, ou identifier les compétences nécessaires pour prétendre au poste visé. Il est possible de flécher la mobilité du personnel, en influençant les choix selon les besoins de l'entreprise : 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.

[54] *http://www.fnmt.fr/fr/communiques-de-presse/emploi-des-seniors-IT-une-fin-carri%C3%A8re-45-ans-nouvelles-voies*
[55] *http://gallery.mailchimp.com/9f370712e6e307699d008e784/files/SeniorIT_LivreBlanc_NvelleCarriere_28jun12.pdf*
[56] *http://gallery.mailchimp.com/9f370712e6e307699d008e784/files/SeniorIT_LivreBlanc_NvelleCarriere_28jun12.pdf*

Figure 14. Exemple de parcours SSI

Figure 15. Exemple de parcours-type



Exemple de parcours type, jalonné de formations, de prise en compte de l'expérience, ou de processus de reconversion/transition

R12 : systématiser les échanges public-privé

La coopération public-privé est fondamentale en matière de cybersécurité. Outre le développement de capacités de réserve permettant notamment de faire face à des situations de crise, il parait intéressant de concevoir un programme d'échange public-privé permettant à des personnels de l'administration 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 de l'administration pendant des périodes de 6 à 12 mois.

Bonne pratique : Les programmes d'échange au DoD américain

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 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). Grâce à ce programme, l'Army a envoyé 4 militaires par an en 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.

R13 : 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
  - Principaux acteurs (écoles, offreurs, utilisateurs finaux, certifications…)
  - La population active cyber
  - Les emplois, compétences et parcours types
  - Perspectives d'évolution
- Evaluer et anticiper vos besoins
  - Analyser l'existant
  - Identifier les besoins
  - Analyser les *gaps*
  - Définir une stratégie
- Recruter grâce à une stratégie multicanal
  - Relations avec les écoles
  - Participation à des événements
  - Communication dans la presse spécialisée
  - Utilisation de *job boards*
- Mettre en place une stratégie de formation continue
  - Tutorat
  - Certifications
  - Formation interne et externe

Ces formations déboucheront sur la remise d'un kit RH sur la cybersécurité.

R14 : faciliter l'accès aux ressources en créant une carte 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.

Bonne pratique : 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 16 : Page d'accueil de la Cyber Maryland Map

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'entrainement. 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 du temps 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 de professionnels en cybersécurité est en effet peu probable. Les besoins vont continuer à croitre, 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.

ceis

Déjà parus :

Cybercriminalité et réseaux sociaux : liaisons dangereuses
Janvier 2015 - english version available

NetMundial, un pas décisif dans l'évolution de
la gouvernance Internet ? Décembre 2014

Cybersécurité des pays émergents Décembre 2013

L'entrainement cyber, un élément clé pour améliorer
la résilience Décembre 2013

Monnaies virtuelles et cybercriminalité
Novembre 2013 – english version available

De l'Union douanière à l'Union eurasiatique, état et perspectives
d'intégration dans l'espace post-soviétique Octobre 2013

PME et marchés de défense – le SIA LAB, une initiative au service
de l'accès des PME aux marchés de défense Août 2013

La coopération technologique et industrielle de défense
et de sécurité du Brésil Mai 2013

Une nouvelle approche du terrorisme. Mieux comprendre le profil
des groupes terroristes et de leurs membres Mai 2013

Le financement de la R&D de défense
par l'Union européenne Avril 2013

Les drones et la puissance aérienne future Février 2013

Compagnie Européenne d'Intelligence Stratégique (CEIS)

Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 – APE : 741 G

280 boulevard Saint Germain – 75007 Paris
Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60

www.ceis.eu