ceis

EPS 2013-01

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

Synthèse

Septembre 2014

1. Contexte

Avec le développement du cyberespace, les forces armées doivent développer les compétences leur permettant de mener des opérations militaires dans cet environnement, qu'il s'agisse de sécurité des systèmes d'information, de lutte informatique défensive et offensive ou encore de renseignement. Or le marché de l'emploi cyber est extrêmement tendu, malgré le renforcement de l'offre de formations initiales. La situation ne devrait pas s'améliorer à court et moyen terme car les besoins, soutenus par la transformation numérique de la société, vont continuer à croître.

2. Défis

Le ministère de la Défense doit donc affronter simultanément plusieurs défis : un défi de recrutement, tant quantitatif que qualitatif (comment attirer des profils dans un marché tendu ?), un défi en matière de gestion carrière (comment fidéliser et retenir le personnel ?) et un défi de formation et d'entrainement (comment maintenir le niveau d'expertise dans un environnement à obsolescence technologique rapide ?).

3. Bonnes pratiques

L'analyse des dispositifs RH d'acteurs publics ou privés, français ou étrangers, permet d'identifier différentes pratiques potentiellement intéressantes et couvrant l'ensemble du « pipeline » de la cybersécurité.

Figure 1 : le *pipeline* de la cybersécurité

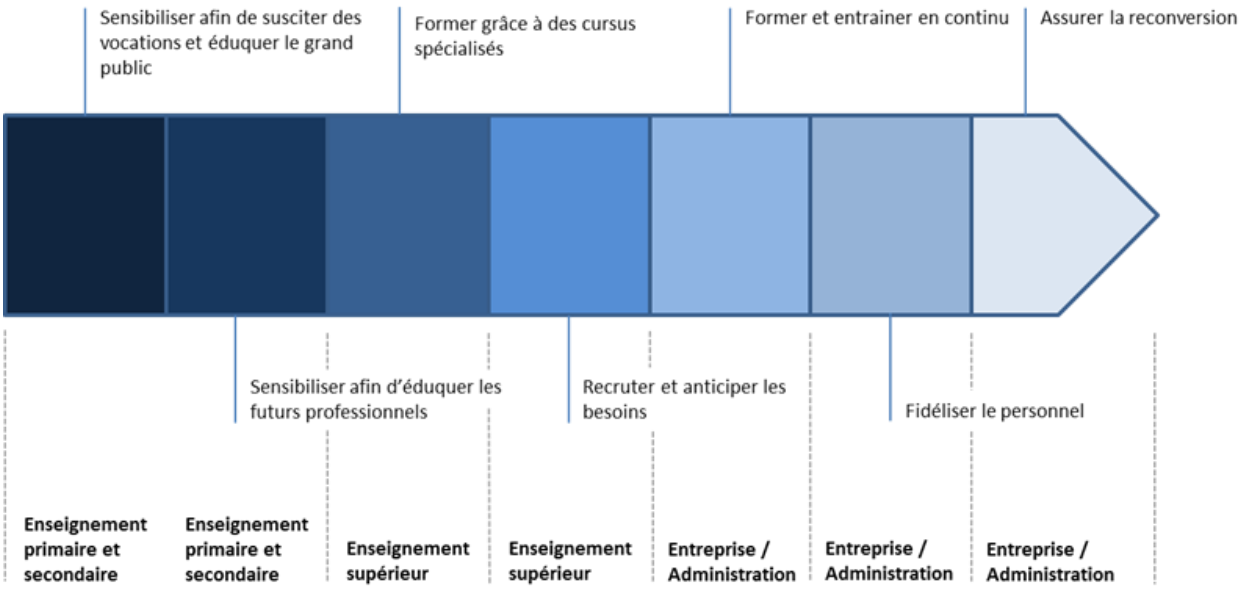

Tableau 1 : liste des bonnes pratiques identifiées

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 exercices d'entrainement
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 entrainement
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'entrainement mutualisé
B32 - Formation et sensibilisation des élites
B33 - Mettre en place un centre de formation continue destinés aux personnels internes et externe

4. Forces et faiblesses de la Défense

Pour faciliter la transposition de ces bonnes pratiques dans le monde de la défense et cibler les recommandations, une analyse SWOT du monde de la Défense par rapport à l'emploi cyber fait ressortir les éléments suivants :

- Forces : excellente image, intérêt des missions, rémunérations compétitives en début de carrière, capacités d'anticipation des besoins, variété des emplois proposés, dispositif de formation performant, infrastructures d'entrainement.
- Faiblesses : processus de recrutement peu adapté, difficulté de proposer un parcours pour les contractuels, pas de référentiel des emplois dédiés, pas de gestionnaire RH spécialisé, rémunérations inférieures après 4 ans d'expérience.
- Opportunités : identification des problématiques par le Pacte Cyberdéfense, réservoir important de personnel qualifié.
- Menaces : concurrence des entreprises, gestion perfectible RH des réserves, pas de cursus LIO contrairement à plusieurs Etats étrangers.

5. Recommandations

Les recommandations portent sur l'ensemble du *pipeline* : très en amont pour susciter des vocations, beaucoup plus en aval pour offrir des parcours attractifs dans la cybersécurité ou comportant des passages par des emplois cyber.

L'emploi cyber est en effet hybride, à mi-chemin entre la sécurité, les technologies de l'information (le cyberespace est un environnement technique) et les métiers de l'organisation considérée. Il ne peut donc être isolé et n'a de sens qu'en prise directe avec les activités opérationnelles de l'organisation.

Tableau 2 : 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 *a minima* 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 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.	Adaptation permanente des ressources humaines aux besoins	Structure permanente en relation avec un référent chez tous les acteurs concernés	2	1
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'entrainement intégré et mutualisé	Ce dispositif serait basé sur un environnement d'entrainement 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'entrainements réalisés	Contenus, environnement d'entrainement 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	Développer d'une vision partagée des métiers, structurer les cursus de formation, faciliter l'orientation	Réunir les acteurs du sujet pour élaborer un référentiel partagé	2	1

		dimension (sécurité, IT, métiers).	des personnes intéressées, faciliter l'émission d'offres d'emploi et donc la recherche de candidats adaptés.			
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 utilisés par l'ensemble des formations proposées par les organisations de la défense.	Homogénéiser les offres de formation	Cadre de cohérence	4	2
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 compétences.	Offrir des parcours de mobilité attractifs	Mise en place d'une plateforme informatique dédiée	3	3
R10	Systématiser les échanges public-privé	Ce programme d'échange permettrait à des personnels du Ministère de la Défense d'être détaché dans des emplois équivalents dans le	Fertilisation croisée des compétences. Création d'une véritable communauté public-	Cadre juridique à adapter	3	3

		secteur privé et réciproquement.	privé en cybersécurité.			
R11	Former les DRH aux enjeux et spécificités du marché de l'emploi cybersécurité	Le but est de proposer aux directions RH des secteurs public et privé des formations spécifiques sur le marché de l'emploi cybersécurité.	Meilleure appréhension du marché de l'emploi cybersécurité par les DRH	Kit de formation RH	4	3
R12	Faciliter l'accès aux ressources en créant une « cyber map » interactive	L'objectif est de recenser et de flécher au niveau national l'ensemble des ressources disponibles	Visibilité accrue des ressources disponibles et des offres d'emplois proposées	Développement de la plateforme et animation quotidienne	3	4
R13	Prévoir des possibilités d'admissibilité directe vers certains corps	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.	Intégration de spécialistes informatiques de haut niveau	Modification des conditions d'accès aux corps de l'armement	4	4

Compagnie Européenne d'Intelligence Stratégique
(CEIS)

Société Anonyme au capital de 150 510 €

SIRET : 414 881 821 00022 – APE : 741 G