Les ressources humaines : éléments constitutifs fondamentaux de la cyberdéfence. Anthropologie numérique et médicale.

Dr. Isabelle Tisserand.

Novembre 2013 – article n°II.5

Résumé[1].

Cet article a pour objectif de passer en revue les principaux axes managériaux de la cyberdéfense (la lutte contre la cybercriminalité et la cyberguerre), en France. Il s'agit d'examiner les moyens de concevoir et de développer une cyberdéfense améliorée, dans les environnements informatisés privés et d'État. Les deux écosystèmes sont désormais intimement liés, notamment lorsque les environnements privés sont des Opérateurs d'Importance Vitale (O.I.V.)[2]. Les recrues jouent un rôle prédominant dans la réussite de la cyberdéfense et réclament une gestion adaptée à leur situation exceptionnelle (notamment lorsqu'il s'agit de cyberguerriers surexposés à l'informatique et travaillant en milieu confiné).

Cyber-écosystème global, rappels

Depuis la vague d'informatisation des années 80 qui a déferlé sur la planète terre, plus ou presque plus aucune organisation sociale ne peut se passer d'équipements informatiques, d'infrastructures et de réseaux terriens, maritimes et spatiaux.

Ce phénomène marque clairement le passage de l'ère industrielle à l'ère du numérique, avec l'apparition de nouvelles populations et de nouvelles formes de cybercriminalité et de guerre[3]. Ces changements culturels ont été des tremplins pour le développement de la culture sécurité en France : création de centres de réflexion orientés sur la sécurité des systèmes d'information (SSI), création de nouvelles écoles, sensibilisations à la sécurité pléthoriques, formation et reconnaissance de la communauté des professionnels se dédiant à la SSI[4], rapprochement inéluctable entre les opérationnels du privé et de l'État, évolutions paramédicales et médicales[5].
De nombreuses entreprises déclarées O.I.V., notamment du fait de l'interopérabilité de nombreux systèmes informatiques, de la mutualisation des moyens et des programmes de continuité d'activité en cas de sinistres énergétique et technologique[6] (entre-autres grâce à l'utilisation de systèmes industriels et de *Data Centers)* ; mais aussi parce qu'elles ont un rôle essentiels à jouer, notamment en situation

[1] Une synthèse de cet article a été présentée aux membres des goupes de travail de la Chaire de cybersécurité et de cyberdéfense le 22 novembre 2013.
[2] http://www.sgdsn.gouv.fr/site_rubrique70.html
[3] Isabelle Tisserand, « hacking à cœur, les enfants du numérique », Ed. E/Dite, Paris 2002. Première ethnographie sur les Hackers.
[4] http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/
[5] En lien avec les pathologies liées à la surexposition aux environnements informatiques ainsi qu'au confinement dans l'interface homme-machine.
[6] http://www.ssi.gouv.fr/IMG/pdf/Guide_securite_industrielle_Version_finale-2.pdf

de crise impliquant une coopération privé/État pour la sécurité du pays, doivent désormais mettre en œuvre des Directives Nationales de Sécurité (D.N.S.)[7] et respecter les plans PIRANET[8].

Il s'agit bien là de structurer des dispositifs, dont le but est de renforcer la cyberdéfense au sens large[9]. Ce nouveau champ d'action implique, par voie de conséquence, des dispositions psycho-sociales particulières - voire singulières - chez les ressources humaines dédiées à ce type de missions.

L'Europe et l'État français ont considérablement renforcé le discours sur la nécessité de structurer des dispositifs de cyberdéfense grâce, entre-autres, au développement de l'ENISA[10] et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[11]. A l'international, de nombreuses puissances se sont dotées de cyber-armées dans le cadre des stratégies de développement de leurs cyberdéfenses, affichant avec fermeté l'existence de forces offensives en cas d'attaque[12]. Le *Deparment Of Defense* (DOD) américain[13], leader en la matière, l'Union Européenne[14] et l'Otan[15] s'organisent tout comme un grand nombre d'autres pays. L'analyse de ces structures permet de déduire que la vision organisationnelle n'est pas globale et que les stratégies sont faillibles du fait de l'omission de certains axes managériaux[16].

En France, la convergence Privé/État a largement été promue par le cercle Européen de la Sécurité et des systèmes d'information (SSI)[17] qui est devenu un centre de rassemblement des problématiques liées à la SSI. Il favorise la solidarité de tous les opérationnels du domaine. Il est devenu un lieu incontournable de renseignements et d'échanges sur la SSI depuis l'an 2000. Les « Assises de la sécurité »[18], événement national et annuel, permet en outre de faire connaître et d'inciter à mettre en oeuvre les mesures publiées dans « Le livre blanc de la sécurité » de la présidence de la république française. Depuis, de nombreux autres cercles ont vu le jour, drainant l'ensemble des problématiques non plus essentiellement fonctionnelles mais politiques, liées au développement de la cyberdéfense[19]. Récemment, la loi de programmation militaire a insisté sur l'urgence de la déployer[20].

Tous ces actes concourent, culturellement, à renforcer la prise de conscience des privés et des étatiques en matière de développement de leurs cyberdéfenses, pour lutter contre la cybercriminalité et contre la cyberguerre, envisageables du fait de l'utilisation mutualisée d'infrastructures vitales informatisées. Ils ont également participé à l'accroissement massif et rapide de recrutements en sécurité informatique[21].

---

[7] http://www.sgdsn.gouv.fr/site_rubrique70.html

[8] http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/cyber-attaques-l-exercice-piranet-2012-met-l-etat-a-l-epreuve-d-une-crise.html

[9] http://www.gouvernement.fr/gouvernement/livre-blanc-2013-de-la-defense-et-de-la-securite-nationale

[10] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

[11] http://www.ssi.gouv.fr/

[12] http://www.foxnews.com/world/2013/09/28/britain-military-recruiting-cyber-warriors/

[13] http://www.defense.gov/home/features/2013/0713_cyberdomain/

[14] http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle/international/voir-les-articles/union-europeenne-la-lente-mise-en-place-d-une-cyberdefense-commune

[15] http://www.nato.int/cps/fr/natolive/topics_78170.htm

[16] Isabelle Tisserand, « cybercontexte, libertés et interdépendances », conférence du 9 décembre 2011 au Conseil Général de l'Armement (CGArm). Paris.

[17] http://www.lecercle.biz/Default.aspx

[18] http://www.lesassisesdelasecurite.com/

[19] Le terme de cyberdéfense a été défini par Daniel Ventre, lors de travaux menés dans le cadre de la Chaire de cybersécurité et de cyberdéfense.

[20] Loi de programmation militaire 2014-2019. http://www.senat.fr/dossier-legislatif/pjl12-822.html

[21] Dans les entreprises privées, les O.I.V., mais également à l'ANSSI : « Le 7 juillet 2009, le Gouvernement, pour se doter de véritables capacités en matière de sécurité des systèmes d'information, décide la création de l'ANSSI, rattachée au SGDSN. En Février 2011, l'ANSSI se voit confier une mission supplémentaire de cyberdéfense et devient alors l'Autorité nationale en matière de sécurité des systèmes d'information. Suite à

La communication

De nombreuses recrues considèrent que la cyberdéfense ne peut faire l'économie d'une communication très spécifique, destinée à la soutenir dans les esprits de ses cybers-équipes, de ses consommateurs, de ses compétiteurs et de ses concurrents. Tandis que de nombreuses puissances étrangères affirment leurs positions offensives[22], les zones latines et le fait est historiquement culturel, communiquent essentiellement sur leurs postures défensives[23]. Les effets psychologiques de ces deux positions ont des effets émotionnels radicalement différents. Tandis que certaines organisations internationales s'inscrivent dans l'attaque et l'offensive, les seconds évoquent plus fréquemment le retranchement et la résistance (phénomène largement développé depuis la guerre de 14-18[24], puis lors de la dernière guerre[25]). Or, tous ceux qui ont étudiées les différentes formes de guerre dans le monde et depuis les périodes historiques les plus anciennes, savent que l'on craint beaucoup plus une force de frappe, une attaque, qu'un bouclier[26]. Sun Tzu écrivait déjà, 500 ans avant Jésus-Christ : « *ce qui donc est de la plus haute importance dans la guerre, c'est de s'attaquer à la stratégie de l'ennemi* », « *attaquez-vous aux plans dès leur principe* ». En Amérique précolombienne, il existait une autre expression de la dissuasion par la communication des moyens offensifs. Il s'agit des têtes humaines réduites par les indiens de la région amazonienne. Ces trophées, exposés, avaient pour but de tenir l'ennemi à distance[27].

Globalement, une communication hybride, qui évoquerait simultanément les défenses et les moyens de riposte d'une organisation, serait donc mieux adaptée au contexte international, ainsi qu'au réflexe émotionnel collectif actuels[28].

Sélection, recrutement et suivi des ressources humaines en charge de la cyberdéfense

Localement, les équipes en charge de déployer la cyberdéfense, soulignent fréquemment que la gestion des ressources humaines comporte des failles. La culture ultra-hiérarchisée actuelle et fortement ancrée qui peut avoir pour effet d'entraver les rythmes de créativité et l'initiative, est souvent un frein au déploiement de la cyberdéfense. En effet et même si le commandement doit absolument rester hiérarchique - militaire -, les ressources humaines dévolues aux activités opérationnelles appartiennent, et appartiendront de plus en plus, à la génération des *Digital Natives*[29]. Cet état de fait doit induire une bonne connaissance des profils des recrues et certaines ouvertures managériales[30].

---

cette forte montée en puissance, l'ANSSI recrute une centaine de spécialistes en cybersécurité et cyberdéfense juniors et expérimentés aux profils très variés ». Source : http://www.ssi.gouv.fr/fr/anssi/emploi/

[22] http://obsession.nouvelobs.com/high-tech/20131031.OBS3607/israel-terre-promise-de-la-cyber-guerre.html?xtor=RSS-12

[23] http://obsession.nouvelobs.com/hacker-ouvert/20131030.OBS3274/cyberdefense-les-programmes-secrets-de-la-france.html?xtor=RSS-12

[24] 4 août 1914. Message du président de la république Raymond Poincarré aux assemblées, à propos de « L'Union sacrée » en France : « *Dans la guerre qui s'engage, la France aura pour elle le droit, dont les peuples, non plus que les individus, ne sauraient impunément méconnaître l'éternelle puissance morale. Elle sera héroïquement défendue par tous ses fils, dont rien ne brisera devant l'ennemi l'union sacrée et qui sont aujourd'hui fraternellement assemblés dans une même indignation contre l'agresseur et dans une même foi patriotique* ».

[25] Période de développement de la résistance.

[26] Sun Tzu, la stratégie offensive, In « L'art de la guerre », Ed. Flammarion, 1972.

[27] Isabelle Tisserand, l'Amazonie et les pampas-terre de feu, In « A la rencontre des Amériques », Musée de l'Homme, Ministère de l'éducation nationale et de la culture, Paris, 1992.

[28] Notamment en rapport avec l'augmentation du besoin de sécurité des populations, qui savent que leur (sur)vie est plus que jamais dépendante de la protection des réseaux informatiques et des infrastructures vitales.

[29] La génération née dans des sphères privée et éducative informatisées.

[30] Jean-Luc Delcroix, « le management stratégique, d'abord humain », collection intelligence et géostratégie, L'Harmattan, avril 2013.

La sélection des cyber-défenseurs a lieu lors du service militaire (lorsqu'il a lieu car il n'est plus obligatoire en France) ou dans les écoles françaises les plus réputées. L'attention focalise fréquemment sur les écoles d'ingénieurs. Mais la cyberdéfense a besoin d'équipes pluridisciplinaires. Aussi, ses agents devraient également provenir des sciences sociales et humaines. On ne peut efficacement se prémunir de cyber-risques sans connaître les milieux culturels dont ils proviennent.
Aucun recrutement de personnel dédié à la cyberdéfense ne devrait avoir lieu sans tests psychologiques. Ils permettent de limiter le risque en termes de recrutement - pour l'employeur et pour l'employé - et d'évaluer l'adéquation profil/poste, modes de travail et modes de communication préférentiels, potentiel de développement, équilibre psychologique, résistance au stress, authenticité, intégrité, éthique, déontologie, etc. En aucun cas ils ne se déroulent sans le consentement éclairé des personnes. Les tests ont également pour but de cartographier les réactions des individus 1/ aux effets secondaires négatifs liés à l'hyper-informatisation (réactions physiques, émotionnelles, structurelles, psycho-sociales, affectives) ; 2/ aux effets secondaires positifs (rapidité de repérage de l'information, développement de l'empan mnésique et réorganisation constante des données mémorisées, amplification des capacités de codage, stratégie de recherche de l'information en mémoire accrue, malléabilité des représentations, réactivité et mise en acte facilitées, pour l'essentiel).

Tout cela a pour objectif de prévenir les risques susceptibles, aussi, de dégrader l'environnement professionnel : décompensations, infractions, accidents, perte et vols d'informations, pertes d'avantages concurrentiels, dégradation de l'image de marque, conflits managériaux, incidents diplomatiques et politiques.

Ici encore et tandis que certains pays étrangers ont bien intégré cet avantage, les pays latins sont en reste. La psychologie est taboue par manque de connaissance. Seule la Marine française, « La royale », excelle dans ce domaine. Elle a déployé un programme de partage de RETEX[31] afin de promouvoir cette stratégie. Celle-ci devrait être intégrée dans les programmes de recrutement des cellules de cyberdéfense en général et des O.I.V. en particulier.

Enfin, les équipes doivent être régulièrement éprouvées et évaluées, tant sur le plan individuel que collectif, grâce à des stages d'augmentation de la résistance aux stress, de traitement systémique et interdisciplinaire de problématiques liées à la cyberdéfense.

La dimension humaine de la cyberdéfense et la gestion des ressources humaines

Les diverses facettes qui composent la personnalité humaine suivent un continuum. Ces facettes sont relatives à des actions, des rôles, des statuts, des représentations qu'ils se font du monde (éducation, travail, relation, etc.). En conséquence, la recherche de cohérence et de continuité comportementale, lors du passage des tests de compréhension psychologique, à pour intérêt d'évaluer ce continuum, afin d'assurer une garantie maximale contre les éventuels dangers que peut entraîner une mauvaise recrue.

Il s'agit, globalement, de détecter une moyenne concernant : la gestion de la personnalité émotionnelle, les qualités professionnelles, l'intelligence sociale, le degré de rétro contrôle, les réactions face au management et les capacités relationnelles, la capacité à gérer les conflits, les représentations sociales globales.

L'habilitation vient clôturer le processus de recrutement préventif de risques humains non conventionnels. Cette disposition n'est pas systématique, alors que ce sont souvent les ressources humaines dont nous parlons qui la réclament, tant pour leurs obligations que pour leurs protections.
Le manager d'équipes en charge de cyberdéfense doit avoir bien compris les profils qui constituent ses équipes, notamment s'ils proviennent de la jeune génération hyper informatisée. Il ne doit pas

[31] Isabelle Tisserand, « Sécurité alternative ». Collection géostratégie. Ed. L'harmattan, Paris. A paraître début 2014.

seulement veiller à la bonne réussite des missions, il doit être disponible[32] et éviter le turn-over des ressources humaines, en s'attachant à entretenir le bien-être au travail et à souder le corps collectif. De la même manière, il devra assurer la négociation en cas de situation à risques, le suivi prophylactique des personnels pour leurs évolutions, tout en travaillant de manière concertée avec la médecine du travail, du fait de pathologies liées à des conditions professionnelles particulières (secret, confinement, interface homme-machine, positions ergonomiques informatiques de longues durées, horaires décalées notamment lorsque les missions induisent un travail de veille, d'analyse de terrain).

En amont, il doit faire en sorte que la recrue qui intègre un environnement hyper informatisé adopte correctement le concept primordial de protection afin de préserver sa propre intégrité, mais aussi celle de l'organisation dans laquelle il travaille. Les risques de glissement pathologique induits par l'environnement lui-même, ainsi que les effets secondaires dits positifs (développement des capacités cognitives en situation de surexposition à l'informatique), doivent être repérés afin de pouvoir être modérés, contenus et prévenus lorsqu'ils sont vécus de manière exacerbée[33].

Le concept de *Dream Team* doit être promu, car il sied parfaitement aux ressources humaines qui se dédient à la cyberdéfense. Ceci renforce le savoir-faire organisationnel et induit un mouvement dynamique grâce à des équipes projets éphémères. Ce type de management augmente la performance managériale de chacun, du fait que le chef de projet est désigné par le groupe, parce qu'il détient le plus de connaissance et d'expérience sur le sujet à traiter - tout en restant sous supervision hiérarchique -. Enfin, les équipements et les moyens techniques mis à la disposition des équipes doivent être à la pointe.

Conclusion

La presse spécialisée regorge d'articles évoquant les textes fondateurs qui expliquent clairement que la cyberdéfense se développe en Europe et dans le monde. Du point de vue socio-culturel, on doit comprendre que cette nouvelle projection militaire - au demeurant internationale -, signifie la transformation des armées du fait, essentiellement, du développement de la cyberguerre liée à la prolifération des infrastructures technologiques et des cybers-armes[34]. Celle-ci induit, en toute logique, un changement des milieux d'exercice, des missions, des profils recrutés et donc également des axes de management qui peuvent être adaptés, à condition de s'appuyer sur des observations psycho-sociales de terrain. En outre, les directions des ressources humaines en charge de nouveaux types de personnalités (*Digital Natives* notamment) seront tôt ou tard confrontées à des évolutions du Droit[35], ainsi qu'aux nouveaux problèmes de gestion de santé et de sécurité au travail induits par les environnements cybers avec, pour enjeu et cette fois-ci, la sécurité de la défense et de ses cyber-défenseurs.

[32] Entretenir le dialogue et la confiance grâce aux débriefings.
[33] Dr. Isabelle Tisserand, Analyse anthropologique et médicale des environnements de hautes technologies. Nouvelles populations, nouveaux risques d'addictions, In « Annales de médecine interne ». Ed. Masson, Paris. 2000.
[34] Le commencement des cyber-armes- Ecole de Saint-Cyr Coëtquidan. *www.st-cyr.terre.defense.gouv.fr/.../Article%20n°11%20-%20Chaire%20...* 1. Le commencement des *cyber-armes*. Djamel Metmati. Juillet 2013 – Article n°11.
[35] Nous pensons ici au domaine juridique au sens large.