**Human Resources: The Fundamental Compositional Elements of Cyberdefense.**

**Digital and medical anthropology.**

*Dr. Isabelle Tisserand*

*November 2013 – article n° II.5*

***Abstract*** [1]**.**

*This article is meant to review the management principle axe of management principle of cyberdefense (the fight against cybercriminality and cyberwar) in France. This is a matter of examining the means of designing and developing improved cyberdefense within private and governmental computerized environments. The two ecosystems are henceforth very closely connected, especially when the private environments are Vitally Important Operators (VIO).*[2] *Recruits play a predominant role in cyberdefense success, and require their management to be adapted to their exceptional situation (particularly when it is a matter of cyberwarriors overexposed to computerization, and working within a confined milieu).*

**Reminders: the global cyber-ecosystem**

Since the great wave of computerization of the 80s everywhere on the planet, virtually no social organization has been able to do without computerized equipment, infrastructures and ground, maritime and space networks. This phenomenon clearly marks transition from the Industrial Age to the Digital Age, with the arrival of new populations and new forms of cybercriminality and war.[3] These cultural changes triggered the development of the security culture in France: creation of reflection centers for Security in Computer Systems (SCS), creation of new schools, multiple urgings of sensitivity to security, training and recognition by the community of professionals specialized in SCS[4] inevitable bringing-together of line personnel of the private domain and those of the government, and paramedical and medical evolutions.[5]

Many declared SCS enterprises, particularly because of the interoperability of numerous computer systems, mutualisation of means and programs for the continuation of activity in the case of electrical supply and technical problems[6] (among others, thanks to the use of industrial systems and Data Centers); but also because they have an essential role to play, particularly in the case of a crisis implying private and governmental cooperation for the sake of national security. It is henceforth necessary to implement the *Directives Nationales de Sécurité* (D.N.S.)[7] and follow the Piratnet directives.[8]

---

1 A summary of this article was presented to the members of the workgroups of the Cybersecurity and Cyberdefense Chair on November 22, 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

This is indeed a matter of structuring the devices, whose goal is to reinforce cyberdefense in the full sense of the word.[9] This new field of action consequently implies specific – even exceptional – psycho-social attitudes in human resources dedicated to this kind of mission.

Europe, and France, have considerably reinforced the discussion about the necessity of structuring cyberdefense devices thanks, among other things, to the development of ENISA10 and of the *Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)*[11]. Internationally, numerous powers have provided themselves with cyber-armies, in the context of development strategies of their cyberdefenses, insisting firmly upon the need of offensive forces in the case of attack.[12] The American Department Of Defense (DOD)[13], the leader in this field, the European Union[14] and NATO[15] are organizing themselves, just as are a great many other countries. Analysis of these structures leads to the conclusion that organizational vision is not global, and that the strategies are vulnerable, because of certain managerial axes[16].

In France, private/governmental convergence has been largely promoted by the European Circle of Security and Computer Systems (SSI)[17], which has become the meeting-place for discussions of problems related to the SSI. It encourages solidarity among all the line personnel in the field. Since 2000, it has become an essential source of SSI information and exchange. "Les Assises"[18], a national, annual event, also make it possible to get to know and to encourage the implementation of the measures published in "*Le livre blanc de la sécurité*" by the presidency of the French Republic. Since then, numerous other circles have been created, taking on the totality of the problems no longer essentially functional but rather political, connected to the development of cyberdefense[19]. Recently, the law on military programming emphasized the urgency of implementing it.[20]

All of these actions converge, culturally, to reinforce awareness of private and governmental entities concerning the development of their cyberdefenses, in order to fight against cybercriminality and cyberwar, made possible by the mutual use of vital computer infrastructures. They have also contributed to the massive and rapid increase in computer safety recruitment.[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/

14http://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 », conference on December 9, 2011 at the Conseil Général de l'Armement (CGArm). Paris.

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

18 http://www.lesassisesdelasecurite.com/

19 The term cyberdefense was coined by Daniel Ventre, during works led with the Cyberdefense and cybersecurity Chair.

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

21 In private companies, V.I.O.,but also at the 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

**Communication**

Numerous recruits believe that cyberdefense cannot do without very specific communication, aimed at providing support in the minds of its cyber-teams, its consumers and its competitors. While numerous foreign powers confirm their offensive positions[22], the "Latin" zones – the fact is historically cultural – communicate their essentially defensive postures.[23] The psychological effects of these two positions have radically different emotional effects. While certain international organisations favor attack and offense, others more often evoke "retrenchment" and resistance (a phenomenon largely developed after the 14-18 war[24], and then during the last war[25]). Now, everyone who has studied the different forms of war in the world, and from as far back as history goes, knows that a strike, an attack are much more feared than a shield.[26] Sun Tzu had already written, in 500 B.C., "so the most important thing in war is to attack the enemy's strategy,"… "attack the plans as soon as they come into definition." In pre-Columbian America, there was another expression of dissuasion by the communication of offensive means. They used human heads, shrunk by Indians in the Amazonian region. These trophies, exposed to view, were meant to keep enemies away.[27]

Globally, a hybrid communication, which would simultaneously evoke an organization's defense and its means of responding, would therefore be better adapted to the current international context, as well as to current collective emotional reflexes.[28]

**Selection, recruitment and follow-up of Human Resources in charge of cyberdefense**

Locally, teams in charge of deploying cyberdefense frequently emphasize that human resources management has faults. The current culture of extreme hierarchy, solidly anchored, can interfere with the potential of creativity and initiative, and often slows down the deployment of cyberdefense. Indeed, even if headquarters must absolutely remain hierarchical – military – the human resources in charge of line personnel activities belong, and in the future will belong more and more, to the Digital Natives generation.[29] This situation must lead to a profound knowledge of recruit profiles, and certain managerial openings.[30]

---

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.

The selection of cyberwarriors takes places during military service (among volonteers, since it is not obligatory in France) or in the most prestigious French universities. Attention focuses frequently on engineering schools. But cyberdefense needs multidisciplinary teams. Its agents should therefore come also from the social sciences and the humanities. One cannot effectively control cyber-risks without knowing the cultural milieus from which they originate. No recruitment of personnel specialized in cyberdefense should occur without psychological testing. This testing makes it possible to limit recruitment risks – for the employer and for the employee – and to evaluate:the profile-job coherence, the preferred methods of working and of communication, the development potential, the psychological equilibrium, the stress resistance, the sincerity, integrity, ethics, deontology, etc. In no case should this take place without the full knowledge and consent of the people involved. These tests are also meant to map individual reacions: 1/to negative secondary effects reactions: 1) to secondary effects linked to hyper-computerization (physical, emotional, structural, psycho-social, affective reactions); 2) to positive secondary effects (rapid information recognition, memorization capacity development and constant reorganization of the memorized data, increased capacity for encoding, increased recall strategy for memorized information, representational flexibility, facilitated reactivity and implementation, essentially.

All of this is intended to avoid both the exposure to risks and also the degradation of the professional environment such as: physical or other breakdown, breaking of the rules, accidents, loss and theft of informations, loss of competitive advantages, degradation of image, managerial conflicts, diplomatic and politic incidents.

Here also, and while certain foreign countries have integrated this advantage very well, the “Latin” countries lag behind. Psychology is taboo, due to lack of knowledge. Only the French Navy excels in this field. It has set up a program shared with RETEX[31], in order to improve this strategy. This psychology should be included in cyberdefense cell recruitment programs in general, and those of the O.I.V.s in particular.

Finally, the teams must be regularly tested and evaluated, both individually and collectively, with training meant to increase resistance to stress, and to facilitate systemic and interdisciplinary treatment of problems connected to cyberdefense.

**The Human Dimension of Cyberdefense and Human Resources Management**

The different aspects of human personality follow a continuum. These aspects concern actions, roles, statutes, representations which are carried out in the world (education, work, relationships, etc.). Consequently, the search for coherence and behavioral continuity, during psychological comprehension testing, seeks to provide a maximum guarantee against the possible dangers which could result from a poor recruitment.

Globally, this is a question of detecting means concerning: management of the emotional personality; professional qualities; social intelligence; conflict management capacities; overall social representations. Accreditation ends the recruitment process meant to avoid non-conventional human risks. This undertaking is not systematic and yet it is often the Human Resources about which we are speaking who want it, both for their obligations and for protection.

31 Isabelle Tisserand, « Sécurité alternative ». Collection géostratégie. Ed. L’harmattan, Paris. To be published early 2014.

The manager of cyberdefense teams must understand the profiles of his or her teams, particularly if they are composed of the hyper-computerized younger generation. He or she must not only expect the success of the missions, but also must be available[32], and avoid turnover in human resources by ensuring good work spirit and team solidarity. In the same sense, he or she must ensure negotiation in the case of a dangerous situation, ensure healthful follow-up for personnel and their evolutions, while working in concert with physicians, because of the pathologies linked to the particular professional conditions (secrecy, confinement, man-machine interface, long ergonomic computer positions, irregular hours – particularly when missions involve work overseeing, on-the-spot analysis.

From his or her superior position, the manager must be sure that the new recruit, integrating a hyper-computerized environment, correctly adopts the primordial concept of protection in order to preserve personal integrity, but also the integrity of the organization in which the work takes place. The risks of pathological "slipping" related to the environment itself, as well as the secondary effects called positive (the development of the cognitive capacities in the context of overexposure to computers), must be recognized in order to be adjusted, contained and prevented when they are excessive.[33]

The *Dream Team* concept must be promoted because it is perfectly suited to human resources specialized in cyberdefense. It reinforces organizational "savoir-faire" and leads to dynamic movement. This type of management enhances each person's managerial performance, since the Head of the Project is designated by the group, because she or he has the most knowledge and experience concerning the subject to be treated – while remaining under hierarchical supervision. Finally, equipment and technical means made available to the teams must be recent and first-rate.

**Conclusion**

The specialized press overflows with articles referring to original texts which clearly explain that cyberdefense is being developed in Europe and throughout the world. From a socio-cultural point of view, it must be understood that this new military projection – which is in fact international – signifies the transformation of armies, essentially because of the development of cyberwar, linked to the proliferation of technological infrastructures and of cyber-arms.[34] Logically, these involve a change of exercise milieus, of missions, of recruitment profiles and therefore also a change of the axes of management which can be adapted, as long as on-terrain psycho-social observations are respected. In addition, senior management in charge of new types of personality (Digital Natives in particular) will sooner or later be confronted with legal evolutions[35], as well as new types of Health and Safety regulations on the worksite, implied by the cyber environments with, at stake this time, Defense Security and the safety of the cyber-defenders.

---

32 Maintaining dialogue and trust thanks to debriefings

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 We mean judicial domain in the broad meaning of the term, here.