Interview de Xavier Raufer

Criminologue

♦ **SDBR : Vous venez de publier un livre passionnant intitulé « Cyber-criminologie »*. On ne vous attendait pas sur ce terrain. Qu'est-ce qui vous a motivé ?**

XR : La criminologie, c'est facile à comprendre, consiste à s'occuper des méchants et à se demander : que font les criminels ? Où sont-ils ? Pourquoi le font-ils ? Comment le font-ils ? Les criminels peuvent aujourd'hui exercer leurs talents à la fois dans le monde physique et dans le monde numérique, or nous observons un déficit énorme d'information sur ce qui se passe dans le monde cybernétique. Ce livre correspond à ma crainte grandissante de voir que nous sommes de plus en plus menacés et, les mêmes causes produisant les mêmes effets, que nous sommes là encore enfermés dans une ligne Maginot : la catastrophe cybernétique de TV5 Monde vient de le démontrer !

♦ **Que vient faire la ligne Maginot dans le risque Cyber ?**

Je vais rapidement vous rappeler l'histoire de ce fleuron français de la Défense. Il y a eu deux lignes de défense parallèles en 1939, entre la France et l'Allemagne : la ligne Siegfried (dont les premiers éléments remontent à 1916) et la ligne Maginot (construites dans les années 30). Un saut technologique était intervenu, depuis la première guerre mondiale, relatif à l'aviation de chasse et aux groupes de bombardement d'assaut, ce qui impliquait que les canons ne pouvaient plus être laissés en permanence sur les casemates fortifiées, sauf à devenir des cibles de choix pour l'aviation. Sur la base des recherches des ingénieurs, il fut décidé alors d'enterrer les canons à 30 mètres de profondeur et de leur adjoindre un système de vérins hydrauliques, pour pouvoir les ramener en surface, en position de tir, très rapidement et à la demande. Les ingénieurs français ont donc réalisé un système hydraulique, unique pour l'époque, bien supérieur à celui de la ligne Siegfried. Un jour, le général Von Rundstedt (futur maréchal) qui faisait une promenade exploratoire vers la ligne Maginot, constate l'avancée technologique française et décide de contourner la ligne Maginot en cas d'attaque des lignes françaises. C'est ce qui s'est passé en 1940, avec pour conséquence la déroute de l'armée française en 48 heures ! La suffisance de nos militaires d'alors était telle qu'ils nieront l'évidence, même quand des gardes forestiers signaleront l'avancée des blindés allemands à travers les Ardennes !

♦ **Donc vous dites, si je comprends bien, que nous somnolons derrière notre cyber-ligne Maginot…**

Je constate simplement que toute la réflexion en France, sur cyberdéfense et cybersécurité, se fait à partir de considérations bureaucratiques et technologiques. A chaque réunion sur ces sujets - et il y en a souvent en France ; à chaque interview de responsables de la cybersécurité, c'est toujours la technique, en l'occurrence l'informatique, qui est discutée et jamais n'est tenu compte de la nature et des évolutions de l'ennemi ! Qui sont les cybercriminels ? Que font-ils ? Comment le font-ils ? Dans SDBR, je lis de fréquentes interviews sur ces sujets, or jamais vos interlocuteurs n'abordent l'évolution de la cybercriminalité. C'est désolant et scandaleux, et je comparerais volontiers cela à la médecine de Molière ! La médecine moderne pose d'abord un diagnostic, ensuite diverses explorations et délivre seulement enfin un traitement. Or nos spécialistes actuels du cyber dédaignent souverainement la partie connaissance et identification d'un ennemi, qu'ils semblent ignorer !

♦ **Mais, à la décharge des spécialistes, l'ennemi n'est pas facile à identifier…**

Il est vrai que l'ennemi bouge sans arrêt, qu'il évolue, qu'il s'adapte et cherche sans cesse des voies et des issues pour entrer dans les systèmes informatiques, et y dérober de l'argent ou des informations. Mais ces évolutions rapides, la plupart des "cyber-experts" les ignorent… Souvenons-nous qu'il y a deux façons d'ignorer : la première est de savoir qu'on ignore et de le reconnaître, la deuxième, plus insidieuse et dangereuse, est d'ignorer qu'on ignore ! Le danger est de croire qu'on maitrise une science sûre, alors qu'on ne sait rien ! Le meilleure exemple de ce que j'avance est l'affaire TV5 Monde, où un système informatique et toutes ses annexes (Facebook, Twitter) ont été piratés et mis à terre pendant 2 jours entiers. Comme vous l'avez constaté, il y a eu lors de cette catastrophe majeure un grand silence de la part des "cyber-experts" : ni explications convaincante sur ce qui s'est passé, ni excuses de ne pas savoir…

Suite de l'interview page 3

** Cyber-criminologie de Xavier Raufer, CNRS Editions*

Interview de Xavier Raufer
Criminologue

♦ Vous savez bien que l'habitude est de garder secrètes les conclusions de l'analyse et de l'enquête sur les piratages d'OIV…

Balivernes ! Dans le domaine médical, on garde secret le dossier du patient, mais on révèle les causes de la maladie pour protéger la population : voyez par exemple le sida. L'information permet la prévention. Quand on lit un rapport, français ou européen, sur le sujet Cyber, on y trouve surtout des généralités : niveau de connaissances des méthodes de lutte contre la cybercriminalité, prise de conscience du danger de la cybercriminalité, attitudes face à la cybersécurité, types d'attaques, etc. Rien sur les cybercriminels ! En Grande-Bretagne, où on redoute le risque cyber, une étude de début 2015 a montré que 80% des attaques informatiques étudiées provenaient du crime organisé… Le cyber-crime est devenu une activité criminelle à part entière, massivement de la part d'individus qui ont déplacé leurs activités du monde physique vers le numérique, en hybridant leurs spécialités. Or, dans tous les articles et ouvrages écrits sur ce sujet, rien n'est écrit sur : qui sont les criminels ? Où sont-ils ? Que font-ils ? Quelles sont les évolutions du cybercrime ? Donc, le livre* que je viens de publier essaie de combler ce vide et de sortir de l'entre-soi des habituels colloques.

♦ Que faudrait-il faire pour faire évoluer l'approche du sujet ?

En France, nous peinons parfois à nommer la menace, mais s'ajoute à cette habitude deux autres défauts : d'une part l'entre-soi de techniciens, qui pensent que les phénomènes techniques relèvent uniquement de la technique (or l'histoire montre que la logique du blindage et du canon ne résout jamais rien) ; d'autre part l'absence de volonté politique de faire progresser le débat. Or la décision politique à prendre serait simple : il suffirait que les responsables politique de la cybersécurité et de la cyberdéfense cessent de financer tout rapport, conférence ou support d'information ne comportant pas, au moins, une moitié d'information sur le thème "qui sont les criminels et que font-ils" ? Ce n'est pas nouveau, car dès l'antiquité, Sun Tsu enseignait la maxime « connais ton ennemi » ! Nous ne connaissons pas nos cyber-ennemis ! Ce qui est en revanche rassurant, si je peux dire, c'est que la criminalité numérique n'est à présent que la traduction d'actes criminels existant depuis l'antiquité : vol d'argent ou de secrets, rançon, prostitution, trafics illicites, trafic d'êtres humains, etc.

♦ Que révèle, selon vous l'affaire du piratage de TV5 Monde ?

Cette affaire est un choc stratégique pour la France. Nos Livres Blancs de la Défense et toute l'activité du ministère de la Défense nous exposent la hantise des Etats modernes, ou coalitions d'Etats (UE), celle du "choc stratégique" : sous-entendu «plus jamais un 11 septembre » ! Les Etats-Unis ont été assommés pour 10 ans par le choc stratégique du 09/11. Coup sur coup début 2015, la France a subi deux chocs stratégiques : Charlie Hebdo et l'Hyper Cachère dans le monde physique, et TV5 Monde, tout aussi grave dans le monde numérique. Un outil d'information internationale, qui porte la voix de la France, a été mis KO durant deux jours : l'appareil, mais aussi ses dirigeants. Où étaient alors les cyber-experts ? Pourquoi cette imprévision? Pourquoi ce choc soudain ? C'est un échec grave !

♦ Que recommandez-vous ?

D'abord, ce préalable. L'espèce humaine peut subir trois chocs : le connu-connu (ex : il y a des braquages et cela peut arriver), le connu-inconnu (il y a des formes d'agression connues mais on n'imagine pas qu'elles puissent nous frapper : exemple le 11/09) ; enfin il y a l'inconnu-inconnu (ce qu'on ne peut anticiper car on l'ignore totalement : l'épidémie de sida). Dans le connu-inconnu et dans l'inconnu-inconnu, l'informatique ne peut rien prédire. L'incertitude ne peut pas être plus modélisée aujourd'hui qu'au temps d'Aristote. Le passé n'est pas prédictif de l'avenir. La meilleure preuve n'est-elle pas la difficulté des super-ordinateurs des météorologues à prédire le temps ? Maintenant, une première suggestion : une veille criminologique, de ce qui est publié sur le Net, dans les vingt principaux forums anglo-saxons, nous donnerait la synthèse régulière des incidents et attaques criminels, narrés par des experts (des vrais) exposant leurs expériences. Avec cette veille criminologique, nous aurions 90% de la connaissance nécessaire pour se protéger.

Interview réalisée par Alain Establier