"atlantico
UN VENT NOUVEAU SUR L'INFO

ENJEU SÉCURITÉ 2017

*XAVIER RAUFER - mai 2017*

# CYBER-DÉSASTRE : Une nouvelle 'ligne Maginot' ?

Des ordinateurs bloqués par centaines de milliers - dont ceux d'administrations ou de sociétés mondiales (Renault en France). "La pire attaque informatique de l'histoire"... Plus de cent pays sont touchés... Voici donc le planétaire piratage opéré par le virus *WannaCry* - un fort offensif "bébé" (parmi tant d'autres...) de la NSA, le service de renseignement américain, subtilisé à son apprenti-sorcier de maître et récupéré puis utilisé... tiens, mais par qui au fait ?

Là, comme d'usage, nul expert en sécurité informatique, officiel ou privé, ne sait rien du coupable. Et comme toujours, nul de ces experts - si prodigues pourtant en "solutions" - n'a prévu cette attaque dont l'ampleur planétaire même, établit qu'elle ne peut relever de la cyber-génération-spontanée.

Autre incohérence ressentie au vu des premières réactions. Sempiternellement et mécaniquement, le banc-de-poissons médiatique attribue tout acte international de piratage informatique à la Russie et aux cyber-sbires de Poutine - or là, la banque centrale de Russie est fortement affectée par WannaCry. Fourberie moscovite ? Ou pratique habituelle du bobard par des médias hypnotisés par la *Silicon Valley* ? Dans l'intérêt de sa sécurité, l'opinion française aurait intérêt à savoir ça.

La vérité, la voici - l'auteur alerte sur ce point crucial dès 2015 dans son traité de "cyber-criminologie" (CNRS-Editions) : la jungle du cybermonde est absolument dérégulée - c'est la Banque de France sans les coffres forts ; la circulation automobile sans code de la route. En exergue de ce livre, l'auteur exposait ce qu'il estime être les quatre thèses fondatrices de la cyber-criminologie :

*Diagnostic 1* - dans l'ensemble "cyber-crime", crime domine. Scruter le monde cybercriminel révèle que celui-ci n'a rien inventé d'original. Dans leur "monde ambiant" et jusqu'à présent, les cybercriminels se bornent à reproduire les variantes de la criminalité physique.

*Diagnostic 2* - La cybercriminalité ne régressera pas, grâce à plus encore de haute-technologie, mais par volonté politique. Une simple fuite en avant type blindage-et-canon provoquerait, dans ce domaine, un désastre analogue à celui de l'inepte guerre *high-tech* d'Irak.

*Traitement, 1* - Il faut au cybermonde un *code de la route* ; comme en son temps, la société de l'automobile suscita le sien. Ce code devra être conçu et imposé par une

coalition de nations puissantes, dans l'espoir raisonnable qu'il s'imposera mondialement. Autre image possible pour l'indispensable superstructure normative : celle de la tour de contrôle.

*Traitement, 2* - Le code de la route vaut pour tout véhicule, luxueux ou modeste : de même, seul un code du cybermonde sanctionnera-t-il efficacement les prédateurs, financiers maraudeurs, géants du net, etc. qui, aujourd'hui, le pillent impunément ou exploitent ses usagers.

Au-delà du monde éthéré des principes, en matière de cyber-sécurité, les sombres présages s'amassent depuis des mois sans que le concert des nations (G7 et autre) dépasse le stade des communiqués affligés ou inquiets :

- La banque centrale du Bangladesh subit un "cyber-braquage" de 81 millions de dollars (coupable avéré inconnu à ce jour).

- Toujours plus sophistiqués et vicieux, les cyber-pirates ciblent les distributeurs de billets, les entreprises et même - vive l'"internet des objets" - les ours en peluche de nos bambins.

- En 2016, le Japon subit 128 *milliards* de cyber-attaques petites ou grandes - 350 millions par jour, 14,6 millions par heure !

- En 2016 toujours, des logiciels pirates type *WannaCry* ont fait en France 250 000 victimes. Logiciels "toujours plus agressifs, destructifs et imprévisibles" (*Dark Reading*, 13/02/2017)

- En Grande-Bretagne, la fraude informatique est devenue l'infraction la plus courante ; un britannique sur 10 en subit une en 2016 (plus de 6 millions de victimes).

Dans les motifs du drame, la culture d'ingénieurs des responsables de la cyber-sécurité. Savants et bons techniciens, Ils ignorent le monde du crime. Or c'est de criminalité dont il s'agit - même, de criminalité grave, des experts (*Dark Reading*, 13/03/17) estimant que certaines entités cybercriminelles accèdent désormais à la puissance d'Etats-nations ; voir notamment la préoccupante "mutation" du milieu cybercriminel du Nigeria.

Second souci en matière de cyber-protection et de *high-tech* : confier les affaires de sécurité à des ingénieurs a ses limites. L'histoire de la fameuse "Ligne Maginot" le prouve. Souvenons-nous : le nez sur leur règle à calcul, de brillants ingénieurs français décidèrent alors que le problème fondamental relevait de hydraulique (du fait de l'aviation en piqué, il fallait permettre la sortie et le repli rapide des canons, depuis les blockhaus) ; ils dotèrent donc de pompes et vérins d'avant-garde une ligne Maginot bien plus *high-tech* que sa germanique contrepartie, la Ligne Siefgried.

Cette technologique excellence impressionna fort le (futur) maréchal von Rundstedt : plutôt que d'y sacrifier ses troupes, il décida sagement de contourner le chef-d'œuvre... Or les cyber-pirates font-ils autre chose aujourd'hui ? ■