"atlantico
UN VENT NOUVEAU SUR L'INFO

Xavier Raufer - avril 2021 - I

"PEARL-HARBOR NUMÉRIQUE" : et si c'était fait ?

À Washington, les hauts fonctionnaires et cadre des cabinets ministériels titubent entre accablement et angoisse. Car après enquête et analyses, le "piratage cyber le pire de l'histoire" révélé fin 2020, est bien pire encore qu'annoncé. En décembre 2020, l'entreprise de cyber-sécurité *FireEye* révélait le giga-piratage d'une foule de ministères, administrations et grands groupes - lors duquel *FireEye* s'était d'ailleurs fait voler ses propres cyber-armes offensives, pourtant fort surveillées. L'affaire durait depuis avril 2020 ; depuis, nul système de cyber-sécurité officiel (NSA... CIA... Homeland security) ou des GAFAM (Google, Amazon, Microsoft...) n'y avait rien vu.

La société texane d'informatique *SolarWinds* s'était d'abord fait pirater son logiciel de gestion de réseaux numériques *Orion Networks Management* (ONM, 18 000 clients dans le monde). De là, les pirates - qu'on croit Russes, mais sait-on attribuer sûrement un méfait dans le cybermonde ? - avaient pu arpenter et "faire leurs courses", sept mois durant, dans les serveurs de 250 cibles ultrasensibles : ministère de la Défense (*Pentagone*), Affaires étrangères (*State Department*), Justie, Commerce, etc., y pillant des masses de documents classifiés, de secrets d'État ou des affaires, de cibles d'opérations d'espionnage en cours, d'actes confidentiels de justice, etc. Or depuis, des enquêtes approfondies révèlent une situation bien pire encore :

- Un tiers environ des cibles n'utilisant pas ONM, les enquêtes ont exhumé un autre axe de pénétration : un logiciel (tchèque, celui-là) utilisé par 300 000 clients dans le monde... dont *SolarWinds*. Le gouffre était béant : il devient sans fond.

- D'autres pirates, eux Chinois par hypothèse, auraient participé à une curée lors de laquelle l'énorme "cloud" de Microsoft, se serait carrément fait voler son code-source. Or *Azure* abrite notamment un serveur fédéral nommé "*Azure Government Secrets*" : inutile de traduire. En prime "*Microsoft exchange server*", gérant les courriels de 30 000 entreprises, administrations, etc. aurait aussi été pillé.

Ce, quand les ravages d'une cyber-guerre sont désormais clairs : bien conduit, un piratage stratégique peut saboter des réseaux et centrales électriques, barrages et pipelines ; effacer des données cruciales ; faire exploser des usines pétrochimiques en y manipulant les pressions et températures ; empoisonner de loin des réseaux d'eau en y injectant des doses mortelles de désinfectants, etc.

Devant ce désastre, le président Biden a promis de "faire de la cyber-sécurité une absolue priorité à tous les niveaux du gouvernement".

Plus vite dit que fait, pour plusieurs raisons fondamentales :

- Cyber égale Internet + *World Wide Web*, architecture numérique passée de 1993 (1e navigateur à interface graphique), à fin 2020, de 15 millions à presque 5 milliards d'usagers, dans l'anarchie totale.

- Anarchie permise par des GAFAM, *Microsoft* en tête, ayant assuré leur domination mondiale en vendant au public, entreprises et administrations, des logiciels bon marché donc plein de "trous", tout pirate pouvant y piller leurs milliards de clients et usagers. Dans ce domaine, les premières enquêtes remontent à 2013 : déjà, ce pillage rapportait aux pirates (d'abord, sur le *DarkNet*) quelque 5 milliards de dollars par an.

- Selon le (tardivement lucide) laboratoire sécurité de *Google*, même si tout internaute réalisait sur le champ 100% des mises à jour censées éviter les piratages, 75% des failles resteraient accessibles, de par l'inextricable infinité des réseaux et systèmes.

- En cause, l'"Internet des objets". 30 milliards d'objets sont déjà connectés ; en 2021 - silencieux *tsunami* - le rythme est de **7 500 connexions nouvelles par *minute***.

- Nommées *Zero-Day-Exploits*, les failles dénichées (et vendues...) par les pirates restent en moyenne ouvertes dix-huit mois. Une éternité pour voler, piller, espionner... Imaginons une banque ou une bijouterie, aux coffres béants un an et demi de rang...

En 1996 et (bien sûr..) au Forum de Davos, John Perry Barlow, lyrique chantre de l'Internet, clamait sa *Déclaration d'indépendance du cyberespace* : "Un continent si vaste qu'il pourrait être illimité... Un monde nouveau que toute notre avidité n'épuisera sans doute jamais ; offrant plus d'opportunités qu'il n'y aura jamais d'entrepreneurs pour les exploiter ; un lieu où les malfaiteurs ne laissent nulles traces ; où, mille fois volés, les biens appartiennent toujours à leurs légitimes propriétaires... Où seuls les enfants se sentent vraiment chez eux..."

Un quart de siècle est passé.

Infini protoplasme à l'obésité galopante, métastasant à la vitesse de la lumière, le cybermonde est-il encore contrôlable et sécurisable ?

À Washington, les stratèges et experts commencent à en douter. ■