"atlantico
UN VENT NOUVEAU SUR L'INFO

Xavier Raufer - janvier 2021

2020 - 2021 : deux articles de prospective géopolitique

2020 et avant : États aveugles, stratégie indirecte et terrorismes sous influence

Vue stratégique et petit-bout-de-la-lorgnette sont incompatibles. Notre rétrospectif regard n'envisagera donc pas quelque épiphénomène de 2020 ; mais, embrassant deux décennies, la sidérante incapacité de la société "de l'information" à percevoir et comprendre ce qui la menace ; qui est l'ennemi. Notamment, dès qu'il s'agit du terrorisme international et de ce qui, à l'arrière-plan, l'anime et le propulse.

Partant de deux cruciaux préalables, nous donnerons ensuite deux exemples de cet aveuglement (volontaire ou non ?), à propos des attentats les plus tragiques du du XXIe siècle débutant ; 11 septembre 2001 (États-Unis) et 13 novembre 2015 (Paris).

FONDAMENTAUX :

1 - JAMAIS, dans l'histoire du terrorisme, un groupe d'action - même suicidaire - n'a opéré sans réseau de soutien ; surtout pour de massives et complexes opérations. La radiographie de dizaines d'attentats complexes ou d'actions de commandos, prouve qu'agir sans logistique est quasi-impossible.

2 - Au Moyen-Orient (matrice des attentats ici rappelés) ; d'abord dans la zone Liban-Syrie-Irak, toute entité émergente, paramilitaire ou terroriste (islamiste ou pas) disparaît vite si elle n'est pas captée par un des États de la région (de la Libye à L'Iran). Ce crucial théorème est valide de 1975, début de la guerre civile du Liban, à nos jours. On lui cherche en vain un contre-exemple.

Nous voici sur un sol ferme : avançons.

ATTENTATS DU 11 SEPTEMBRE 2001, ÉTATS-UNIS - D'abord : ce qui suit n'émane pas d'une officine conspirative mais du cœur de l'État fédéral américain [Congress of the United States... TOP SECRET... *Joint inquiry into intelligence community activities before and after the terrorist attacks of september 2001*" [1]]. Lire ce document déclassifié - à grand peine - sur demande de victimes de ces attentats, répond clairement à la question qui taraude les experts depuis septembre 2001 : JAMAIS l'appareil logistique appuyant les 20 terroristes du 11 septembre n'a été identifié. Nul membre cette cellule logistique qui *forcément* a agi aux États-Unis, n'a jamais été poursuivi, arrêté ou jugé.

Or la réalité, la nature, l'étendue de ce réseau logistique d'al-Qaïda sont connus à Washington depuis 2002, figurant dans les 28 pages les plus secrètes du rapport ici mentionné. Que disent-elles ? Allons vite : ce crucial réseau logistique opérait depuis l'ambassade saoudienne de Washington. Citons le rapport "Aux États-Unis, des pirates de l'air du 11 septembre étaient en contact, et ont reçu aide et

[1] Document récemment déclassifié, à disposition de tout *fact-checker* interessé.

assistance, d'individus liés au gouvernement saoudien... Aux moins deux de ces individus seraient, selon des sources, des officiers de renseignement saoudien... Des associés d'officiels saoudiens aux États-Unis auraient d'autres liens encore avec al-Qaïda".

Suivent 28 pages de noms, dates, actes repérés par le FBI ou la CIA ; de téléphones et adresses. En septembre 2020, une juge de New York donne enfin aux victimes le droit de poursuivre "24 officiels, ou ex-officiels saoudiens" et révéle le nom (caché depuis 2002 !) du chef du réseau de soutien : Mussaed Ahmed al-J... chef de cabinet du prince royal de la famille al-Saoud, alors ambassadeur à Washington.

Ces énormes révélation ont fait peu de bruit aux États-Unis et sont ignorées en Europe. Coïncidence ? Les mutiques médias d'information sont d'usage assujettis à des GAFAM, eux-mêmes couverts d'or par l'Arabie saoudite.

ATTENTATS DU 13 NOVEMBRE 2015 À PARIS - Rappel : lors de la vague d'attentats des années 1980 (bombes à Paris, prise d'otages, etc.), les officiels français découvrent à grand peine, lentement, que ces multiples actes émanent tous d'un unique sommet ; que derrière l'apparent chaos terroriste, existe un bouton marche-arrêt. Quand la France fait certains gestes, les attentats la frappant au Liban, à Paris, s'arrêtent net, au coup de sifflet.

Maintenant : la longue attaque (novembre 2015-printemps 2016) de Paris à Bruxelles mobilise une centaine d'individus de dix pays divers, actifs de la zone Irak-Syrie au cœur de l'Europe ; unis par cellules coordonnées, disposant d'une complexe et solide logistique : lire les actes de justice déja publiés suffit à s'en convaincre.

Cette opération si bien conçue et exécutée a-t-elle germé dans le seul esprit de simplets à la Abdeslam, alcooliques ou toxicomanes, fanatisés à la va-vite et hypnotisés par le constant radotage des rares formules coraniques meublant leurs pauvres têtes ? C'est fort douteux.

On verra dans un prochain article que les États-cibles commencent à entrevoir un piratage d'État, derrière la masse d'intrusion de leurs systèmes numériques les plus secrets ; ces mêmes États ont encore un vaste effort de lucidité à accomplir face au péril qu'ils sous-estiment, voire nient, depuis deux décennies : le terrorisme d'État.

2021 et après : devant un 'Pearl-Harbor' cyber ou militaire, les États occidentaux peuvent-ils encore réagir ?

Partant d'exemples récents, tentons d'envisager ce qui nous attend, plus loin sur la route ; ce qui revient à poser une (grave) question : saurions-nous réagir à temps, face à un violent choc stratégique ? Des cas récents en font douter ; mais avant de les exposer, bref retour sur Pearl Harbor et ses séquelles.

Les rapports suivant l'attaque sont limpides : Pearl Harbor résulte d'une grave incapacité de Washington à croire à l'attaque de Tokyo. Jamais en effet, le Pentagone n'a si bien connu les plans de l'ennemi : codes secrets nippons cassés ; alertes répétées des services spéciaux britanniques ; l'ambassadeur du Pérou à Tokyo prévient : l'attaque japonaise débutera par un raid-surprise sur Pearl-Harbor. En juillet 1941 enfin, le colonel américain William Farthing écrit une note d'alerte que la commission d'enquête qualifie après-coup de "prophétique dans sa précision, voire troublante dans sa prescience des plans ennemis".

Réaction de Washington ? "Ils n'oseront jamais". Résultat : 2 400 morts, 180 avions détruits, 10 navires coulés. Au moins, l'Amérique réagit-elle vite et fort à la provocation : le lendemain, le congrès US déclare la guerre au Japon.

Sans remonter au 11 septembre 2001, avons-nous récemment éprouvé de tels chocs stratégiques ? Oui bien sûr ; et les réactions officielles devant un tel "raidissement singulier de la chose importune, du fortuit", comme dit la philosophie, inquiètent plutôt.

ARABIE SAOUDITE, 14 septembre 2019 à l'aube : parmi les plus grands au monde, les complexes pétrochimiques d'Abqaiq et Khurais sont écrasés par une volée de missiles de croisière ; or dans une péninsule arabe grouillant de radars et de défenses anti-balistiques, nul n'a vu ces missiles s'envoler et filer vers leurs cibles ; n'a donc pu les intercepter. Abasourdis, les experts israéliens bouleversent leurs jugements sur les capacités balistiques iraniennes. Et ce n'est que le 1e décembre 2020 qu'un éditorialiste du *New York Times* fait timidement allusion à un possible "Pearl Harbor" dans la péninsule.

WASHINGTON, le 8 décembre 2020. Une société privée de cyber-sécurité (elle-même piratée) révèle le pire *hacking* jamais commis. Nom de code SUNBURST. Un ami de l'auteur, officiel américain éminent, lui dépeint une *nomenklatura* de Washington "blême, épouvantée", devant le sidérant cyber-braquage, huit mois durant et sans que nul n'ait rien vu, des dispositifs TOP-SECRET du gouvernement et de la défense des États-Unis. Avant d'émerger, gifle suprême, la veille du jour où le Collège électoral déclare Joe Biden formellement élu président.

Department of Homeland Security et sa *Cybersecurity & Infrastructure Security Agency (CISA)... NSA... US Cyber Command... CIA... FBI*..... Aveugles et depuis lors muets, malgré les dizaines de milliards dépensés pour blinder l'informatique officielle américaine. Des intrusions inouïes au Pentagone, dans les ministères régaliens et groupes américains sensibles : défense, finance, etc. Huit mois pour tout y piller, y installer des logiciels malveillants. Les "clouds de défense" et la *Nuclear Security Administration* (qui protège l'arsenal nucléaire US) pourraient avoir été pénétrés. Pour la CISA "un risque grave pour le gouvernement fédéral... les infrastructures essentielles et le secteur privé".

Bien sûr, on apprend ensuite que la société SOLARWINDS ("vents solaires"), dont le logiciel *Orion* fut le cheval de troie des pirates (soi-disant Russes, sans preuve à présent) n'avait pas de directeur de la cyber-sécurité, les codes d'accès de ses cadres circulant sur le Darknet. Son mot de passe pour télécharger ses mises à jour ? solarwinds123.

PARIS, décembre 2020 : *Facebook* et *Instagram* suppriment un dispositif de faux comptes de propagande, favorables à notre présence militaire en Afrique et hostiles aux djihadistes du Sahel. l'interférence politico-diplomatique, dit *Facebook*, émane "d'individus liés à l'armée française". "Interférence étrangère" signifie : fausses pages et comptes créés par des individus X opérant depuis un pays Y, pour y influencer des internautes d'une zone Z : 84 profils, 6 pages et 9 groupes *Facebook*, 14 comptes *Instagram*, plus des comptes *YouTube* et *Twitter*.

En même temps, deux autres systèmes de "guerre de l'information", eux Russes, sont aussi radiés de *Facebook* et d'*Instagram*. Seulement, la Russie possède une myriade de ces "armes informationnelles". Et la France ? Disposons-nous aujourd'hui d'autres cyber-réseaux pour notre guerre d'influence en Afrique ? Espérons-le. ■