ANTIRESSE
N° 221 | 23.2.2020

Crypto saga

Que reste-t-il de la neutralité suisse?

Devenez stupide avec Powerpoint (2)

Observe • Analyse • Intervient

LE BRUIT DU TEMPS par Slobodan Despot

Cryptocratie: la grande épopée d'espionnage qu'on n'a pas encore écrite

La société Crypto AG à Zoug, label suisse au-dessus de tout soupçon, avait donc fabriqué le cheval de Troie universel, multicoups, multiusages. Plus futé que celui des Grecs anciens, il n'était même pas offert à l'adversaire: bien mieux, les clients payaient pour se faire espionner! Avant que l'establishment ne recouvre une fois de plus ce scandale colossal d'un voile de pudeur, essayons de comprendre tout ce qu'il nous révèle sur ce pays, sur le monde et l'époque où nous vivons.

LES DOUBLES TORPILLES

Le 2 mai 1982, un sous-marin d'attaque de la marine britannique coulait de deux torpilles le croiseur *General Belgrano*, pièce maîtresse de la force argentine détachée à la (re)conquête des îles Malouines. Les 325 marins qui périrent au cours de l'opération forment plus de la moitié des pertes humaines de l'Argentine au cours de cette étrange guerre livrée pour trois rochers perdus dans l'Atlantique Sud. Au moment de sa destruction, le *General Belgrano* se trouvait hors de la zone d'exclusion de 200 milles nautiques autour des îles instaurée par le Royaume-Uni. Selon l'histoire officielle, les renseignements britanniques avaient intercepté un ordre de mouvement perçu comme hostile et le Cabinet de guerre décida de frapper sans prévenir, dans une aire de navigation libre(1). Selon la version rectifiée, la position du Belgrano avait été détectée sans peine par les Américains et les Allemands (alliés des Britanniques) grâce à la machine de chiffrement piégée que la société suisse Crypto SA avait vendue aux Argentins(2). L'ironie de l'histoire est qu'au même moment, l'ambassade de Suisse à Buenos Aires — selon une coutume bien établie — servait d'intermédiaire entre les deux gouvernements en conflit. Les deux torpilles, sans doute, ne savaient rien l'une de l'autre.

OPÉRATION RUBICON: LA RÉALITÉ DU MONDE FRAPPE À LA PORTE DE LA SUISSE

Comme tant d'autres pays, l'Argentine s'était fiée à la marque Crypto SA pour éviter de devoir développer à grands frais ses propres systèmes de cryptage — ou les acheter auprès d'une grande puissance potentiellement intrusive. Quel meilleur argument marketing pour vendre de la technologie de sécurité que d'y apposer le label suisse? La Suisse neutre et sa tradition de bons offices. La Suisse candide, pacifique et honnête. Sans ce mythe, les îles Malouines auraient peut-être changé de main... Ce n'est que l'une des tragédies — peut-être la plus spectaculaire, mais qu'en sait-on? — dues au système de trahison organisé par la CIA et le BND allemand autour d'une entreprise dirigée par un génie, Boris Hagelin — génie des affaires (et des «affaires») plus encore que de la cryptographie, matière où il excellait bien avant de mettre le pied en Suisse. C'est une histoire si riche, si complexe et si révélatrice à la fois qu'on aurait envie de la lire au coin du feu, avec un bon cognac. Elle fournirait la matière d'au moins trois grands romans d'espionnage. L'ironie mélancolique d'un John le Carré lui donnerait la patine idéale, celle des armes anciennes qui nous paraissent aujourd'hui dérisoires, mais qui ont fait couler plus de sang et suscité davantage de terreur que nos gadgets ultramodernes. L'histoire des machines piégées de Boris Hagelin incarne l'espionnage dans son essence même, avec mille portes dérobées, mille escaliers donnant sur nulle part, mille évidences si convaincantes qu'on peut être sûr qu'elles ne sont que des mirages. Toute l'histoire de la Guerre froide — et au-delà: du XXe siècle des massacres et des révolutions — est *chiffrée* dans ses développements. Rayonnant à partir de la Suisse, elle touche 130 pays, dont une immense majorité de victimes et de dupes et deux ou trois tireurs de ficelles. En apparence du moins, car nous n'en savons toujours pas le fin mot, et nous ne le saurons probablement jamais. Elle multiplie les coups bas, les alliances ambiguës, les morts suspectes. Elle remet en question toute la fable du non-engagement helvétique de ces 70 dernières années. Au contraire, elle fait entrer ce pays de plain pied dans le bain de «sang, de sueur et de larmes» que fut le XXe siècle. Elle risquerait même de le libérer du syndrome de la pendule à coucou que lui a méchamment collé Orson Welles, de cette aversion séculaire pour toute prise de position nette et affirmée, cette peur de toute grandeur et de tout tragique qui se réconforte dans la microgestion perfectionniste du quotidien.

C'est bien pour ça que la Suisse officielle, après une vague d'agitation, ne veut déjà plus en entendre parler! Ce n'est même plus une question d'intérêts: c'est une affaire de conditionnement mental.

«MEURTRE SOUS LES GÉRANIUMS»

Tel est le titre de la chronique consacrée par le grand écrivain Georges Haldas aux années de guerre telles qu'il les a vécues depuis sa ville de Genève, cernée à l'époque par «l'empire du meurtre» hitlérien. Haldas, à l'époque,

travaillait dans un *Journal* (de Genève) qui incarnait, tant bien que mal, une certaine liberté d'expression au milieu de la censure nazie. Las! Qu'y apprenons-nous? Que ces messieurs de la rédaction — d'éminentes figures du journalisme «neutre» —, balançaient chaque jour par téléphone le contenu de leurs propres articles à la Kommandantur parisienne, pour ne pas risquer une interdiction du journal sur le territoire voisin, en France occupée. *«Imaginer ainsi le Journal de Genève, "seul quotidien suisse d'audience internationale", littéralement aux ordres des censeurs allemands donne une idée exacte (et terrifiante) de l'indépendance d'esprit qui régnait à l'époque dans ses murs»,* conclut Jean-Michel Olivier. Le «guichet de courtoisie» offert à la Gestapo par le Journal de Genève dans l'Europe hitlérienne annonce les portes dérobées de Crypto SA offertes à la CIA dans l'Europe américaine. Les occupations se suivent, une idéologie chasse l'autre, une seule chose reste immuable: la posture sainte-nitouche de l'establishment helvétique. Comme pour le Journal de Genève, personne à aucun niveau ne savait rien au sujet de Crypto SA. Ainsi que l'a résumé avec une drôlerie féroce l'humoriste Benjamin Décosterd, à la lumière de l'affaire «Rubicon», l'«entretien d'embauche pour bosser à la Confédération» pourrait à peu près se passer ainsi: > «Alors, Monsieur, citez-nous trois de vos défauts? > — Ben, je suis incompétent, j'ai pas de mémoire et je suis bordélique. > — Non, les qualités c'est après…

Certes, il n'y a rien d'helvétique dans cette entreprise fondée par un «Suédois» quelconque, sinon la domiciliation, les employés et les impôts… En quoi cela peut-il bien concerner la Suisse? Avec une indignation qui est plutôt rare dans le paysage médiatique, Jacques Pilet démonte le processus d'*«enfumage»* par lequel le *«système»* essaie d'éteindre l'incendie. Loin d'être une vieille anecdote de la Guerre froide, rappelle-t-il, la «saga» n'est pas si ancienne puisqu'en 2016 encore, le chef des renseignements — et aujourd'hui bras droit du conseiller fédéral Cassis —, *«vantait les mérites de Crypto AG devant les officiers suisses»* en y voyant *«un bon exemple de la façon dont on peut générer de la sécurité sur sol neutre»*. Le patron du renseignement était évidemment payé pour ne rien savoir des activités de renseignement de Crypto AG! Les officiels suisses regardent de tous côtés sauf du bon, comme des dindes dans la basse-cour pendant que le renard s'occupe du poulailler.

L'ENVIE DE NE RIEN SAVOIR

Car c'est la troisième fois, au moins, que le scandale Crypto tente de s'immiscer dans la conscience publique des Suisses. En 1992, un ingénieur suisse de Crypto était détenu et malmené en Iran avant d'être libéré contre une caution rondelette. Le pauvre Hans Bühler, qui semble-t-il ne savait rien des manœuvres de sa propre boîte, a vu sa vie brisée et a entamé contre le système du mensonge une croisade qui fut poliment étouffée. La Police fédérale, à l'époque, n'avait pas jugé utile d'enquêter. Un signal parmi d'autres, mais dont l'accumulation devrait au

moins fournir matière à réflexion et à scoops à un journalisme helvétique désespérément en quête de public. Or que voit-on, à de rares exceptions près? Un manque de curiosité devenu une seconde nature. Pour que personne (à l'exception de l'Antipresse) n'aille dérouler la biographie de Boris Hagelin, il fallait vraiment que les rédactions soient occupées ailleurs. En voici le résumé remarquablement insignifiant dans le quotidien *24 Heures*:

> «À son retour des États-Unis, l'ingénieur suédois Boris Hagelin fonde à Zoug une entreprise de dispositifs de chiffrement. Il choisit la Suisse parce qu'elle est non alignée et qu'elle a une pratique d'exportation plus libérale que la Suède.»

Hagelin était peut-être suédois d'origine. Il était surtout russe depuis trois générations, et une émigré de la révolution bolchévique. Au moment de son installation en Suisse, en 1948, il est déjà un industriel fortuné de la cryptographie qui avait déjà produit 140'000 machines pour l'armée américaine (la M-209). Il n'est pas concevable que les services et l'administration suisses n'aient pas eu au moins un entretien d'information avec lui. Revenons à nos jours: la presse nous apprend tout de même que le Conseil fédéral, tout en ne sachant rien, «*se prépare depuis des semaines à ces révélations — avec un document interne intitulé "Sprachregelung Crypto AG"*». On sait que les ministres suisses ne prononcent pas «bonjour» sans l'avis de leurs *Spin Doctors*. Un «règlement de parole» (*talksheet*, dans le langage branché) vise le plus souvent à «reformuler» des choses qui ne doivent pas être dites telles quelles. Quelles choses? Qui a élaboré ce document? Que contient-il? Mystère...

Passons sur les journalistes: ils n'ont jamais de temps ni de moyens pour enquêter. Mais pour que personne dans le milieu universitaire, ce dernier demi-siècle, ne se soit intéressé à cet épisode clef de la guerre froide(3), il fallait là aussi une dose d'incuriosité pour ainsi dire institutionnelle. Les prétextes à enquêter sur les liens entre la Suisse, les services «alliés» et l'OTAN n'ont pourtant pas manqué, à commencer par le «faux scandale» de l'organisation P26.

La décrédibilisation peut-être définitive de la «neutralité» suisse par cette affaire — avec toutes ses conséquences diplomatiques et commerciales — poussera-t-elle l'establishment à une prise de conscience, pour ne pas parler de remise en question? On peut aimablement sourire. En définitive, bien des «angles morts» de l'histoire si lisse de ce pays n'ont été explorés que par la littérature — les Frisch, Dürrenmatt, Chessex. Peut-être en sera-t-il de même pour la *Crypto saga*. Asseyons-nous donc quand même dans notre vieux fauteuil au coin de la cheminée et versons-nous un grand verre de cognac XO...

NOTES

1. Voir «ARA General Belgrano», wikia.org.
2. «La Suisse au cœur de l'opération "Rubicon"», *Le Temps*, 12.2.2020.
3. A l'exception notable de la thèse de doctorat de l'historien Daniele Ganser, *Les Armées secrètes de l'OTAN* (trad. française aux éd. Demi-Lune). Mais Ganser a été écarté du milieu académique pour «parti pris».

CANNIBALE LECTEUR de Pascal Vandenberghe

Devenez_stupide_en_dix_slides.ppt (2)

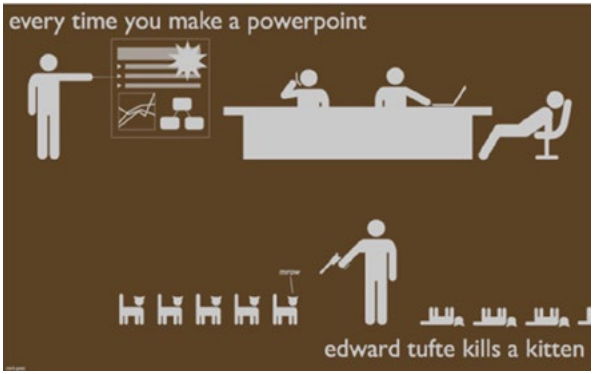
Créés d'abord pour répondre aux besoins de l'armée américaine, les systèmes de présentation investiront ensuite massivement le monde de l'entreprise, avant de revenir en force par un usage immodéré dans le monde militaire et de se déployer dans tous les autres champs de la société: institutions publiques, universités, écoles. En quoi et comment PowerPoint contribue-t-il à la fabrication d'une pensée unique et favorise-t-il la réduction de la pensée? Poursuite de l'exploration de l'enquête de Franck Frommer, *La pensée PowerPoint*(1).

5 février 2003. Devant l'assemblée de l'ONU, Colin Powell, secrétaire d'État à la Défense, lance une présentation PowerPoint qui deviendra célèbre. Utilisant toutes les fonctionnalités du logiciel, il va persuader l'assistance de l'existence d'armes de destruction massive en Irak. Quelques heures plus tard, la présentation est mise en ligne sur le site de la Maison-Blanche et apparaît sur Internet: il faut aussi convaincre le peuple américain de la nécessité de déclencher une guerre «préventive» contre l'Irak. Le 8 septembre 2005, lors d'un entretien sur la chaîne ABC, Powell reconnaîtra avoir menti.

C'est encore PowerPoint qui remplace le traditionnel plan d'attaque lors de l'offensive et servira à «expliquer», par un graphique, l'organisation de l'Irak à la suite de l'opération militaire. À la lecture de cette *slide*, on comprend que les affaires intérieures de l'Irak seront réglées en une quarantaine de mois avec 5000 soldats américains. On sait ce qu'il en est advenu dans la réalité… Quelques *slides* ne peuvent rendre compte de la complexité d'une situation, comme le déclara le général McMaster dans le *New York Times*: « *PowerPoint est dangereux car il peut créer l'illusion de la compréhension et l'illusion de contrôle. Certains problèmes du monde ne sont pas bullet-isables.*» Cette invasion de Powerpoint fera dire plus tard au général Tommy Franks, présent en Irak au début de l'offensive: «*Aujourd'hui les commandants en opération informent Washington, l'OSD*(2) *et le secrétaire à la Défense de leur action grâce à PowerPoint… Au lieu d'un ordre ou d'un plan, vous recevez en retour un lot de diapositives PowerPoint… C'est frustrant, parce que personne n'a de plan d'attaque contre PowerPoint!* »

Mais ce sont les entreprises qui ont d'abord subi les dégâts causés par l'usage inapproprié ou l'abus de PowerPoint(3). La nécessité de communiquer, consécutive à la mise en place d'un nouveau paradigme (gestion par projet, transver-

salité, passage de l'ère du «savoir-faire» à celle du «savoir-être», etc.) va trouver une réponse avec PowerPoint. Alors que la réflexion et l'argumentation doivent précéder la fabrication d'une présentation, qui ne devrait être destinée qu'à les soutenir ou les illustrer, les managers vont se prendre au jeu de l'animation et passer plus de temps à créer une présentation «qui en jette» qu'à la réflexion. Ainsi la forme prend le pas sur le fond. Au fil du temps, la fabrication de la présentation viendra précéder la réflexion qui devra se plier aux règles de la *Bullet list*. Fâcheux pour la pensée: car aligner des points successifs, ce n'est pas développer un raisonnement.



PowerPoint, c'est le royaume du «copier-coller»: on modélise, et les cabinets d'audit utilisent les mêmes matrices d'une problématique à une autre, d'une entreprise à une autre. L'une des plus célèbres est le SWOT, de l'anglais *Strenghts* (forces), *Weaknesses* (faiblesses), *Opportunities* (opportunités) et *Threats* (menaces). Le langage utilisé dans PowerPoint, passant de la phrase verbale à la phrase nominale, crée une nouvelle grammaire, par laquelle une langue vivante devient insignifiante. La phrase nominale induit — faussement — une impression d'objectivité, d'impartialité. L'usage de formules toutes faites et de mots vides fabrique un discours désincarné qui n'est qu'une suite de lieux communs de la novlangue médiatico-économique. Réduit à quelques dizaines de mots, le vocabulaire est d'une pauvreté affligeante et l'emploi du lexique militaire est quasi obsessionnel («cible», «feuille de route», «mobilisation», «tactique», «impact», «conquête», etc.). Dans la présentation d'un graphique, en tassant ou, à l'inverse, en accentuant les courbes, on peut à loisir faire passer un message ou son contraire. Qualifiées par une étude américaine de «somnifère des organisations», les présentations PowerPoint doivent être menées par un orateur capable d'assurer le spectacle. Il s'agit de donner à voir, plus que de donner à savoir, un art dans lequel Steve Jobs fut indéniablement grand maître.

Médium de l'instantanéité, PowerPoint ne permet pas les associations d'idées permanentes qu'offre une lecture linéaire. Culture du zapping (on passe rapidement d'une idée à l'autre, sans lien ni construction logique), PowerPoint est aussi culture du slogan de type publici-

taire, dans lequel le raccourci et la synthèse sont agrémentés de force euphémismes destinés à masquer ou atténuer des vérités difficiles à dire face à un public. C'est ainsi qu'au milieu des années 1990, France Telecom, devenu privatisé, va imposer à ses 4000 «managers» 6 modules de Powerpoint répartis sur 10 jours étalés sur 9 mois. La nouvelle politique «conquérante», qui prévoit des dizaines de milliers de suppressions d'emploi et de «mobilité» (et va se solder par une mémorable vague de suicides), s'appuie notamment sur une série de *slides* destinées à réagir devant les «postures de résistance(4) » qui laissent pantois.

Dans cet univers d'immédiateté et de contrôle qu'est devenue l'entreprise «moderne», l'individu doit se soumettre ou se démettre. Il doit répondre à des injonctions paradoxales («soyez créatifs!»), « muscler ses compétences», être «innovant», «performant», «à l'écoute», et surtout «capable de s'adapter». Comme l'écrit Franck Frommer dans sa conclusion: «*Profondément narcissique, ce modèle d'individu est focalisé sur la seule satisfaction de ses désirs et n'envisage sa vie qu'à l'aune de ses propres droits et de son intérêt. Mais il souhaite s'intégrer dans des cadres normatifs dans la mesure où il estime qu'ils sont conformes au modèle dominant et qu'ils lui permettent de réussir. Il est toujours présent mais irresponsable, toujours connecté mais jamais impliqué. Ses seules valeurs sont celles qui lui permettent de "se réaliser", de "se développer personnellement", sans projet à long terme. Il doit pouvoir se comparer, s'évaluer, afin de répondre à une situation de compétition permanente… En un mot, totalement pris en charge par le monde technico-économique, il a l'illusion de l'autonomie tout en ayant perdu toute initiative.*»

Et si PowerPoint ne rend pas forcément «stupide», il n'en demeure pas moins que «*PowerPoint participe, sans nul doute, comme de nombreux autres médias, à l'"analphabétisation du monde", à l'abandon du sens critique, à l'adhésion aveugle à une nouvelle forme de "servitude volontaire".*» Moi qui ai passé des décennies dans des grandes entreprises et ai vécu cette période qui va de l'apparition de PowerPoint à son indiscutable hégémonie, je ne peux que confirmer ces propos: oui, la «powerpointisation» des esprits contribue bien au formatage des cerveaux. Il les rend dociles et soumis.

NOTES

1. Franck Frommer, *La pensée PowerPoint. Enquête sur ce logiciel qui rend stupide.* (La Découverte, 2010).
2. *Office of the Secretary of Defense.*
3. Faute de place, nous n'aborderons pas ici les autres secteurs touchés: administrations publiques, universités, écoles. Pour se faire une idée précise de l'ampleur des dégâts, je renvoie le lecteur au livre de Franck Frommer.
4. Une dizaine de slides tirées des modules de France Telecom sont reproduites dans le livre de Franck Frommer. Leur lecture est sidérante et atterrante!

La destruction du «General Belgrano»

FUTURISK par Sébastien Fanti

Crypto AG. La ligne rouge

Je lis tout ce qui est publié, respectivement diffusé sur cette affaire. Tout. Et je souris. Souvent.

Le nombre d'experts qui se targuent de tout connaître de ce dossier ne cesse de m'étonner.

Tout comme de ceux qui déclarent ne rien en savoir.

Pour ma part, je réserve mes mots aux deux instances saisies de ce dossier: un ancien juge fédéral et la Délégation des Commissions de gestion. Mon rôle importe peu. Il est, à ce stade, infinitésimal.

La seule question qui m'importe est celle de la ligne rouge.

Celle qui, si elle a été franchie, devra inexorablement conduire à des actes forts. Nonobstant toutes les tentatives actuelles de minimiser les conséquences de ce qu'il faut bien appeler le CryptoGate tant en termes de neutralité que de démocratie.

Quelle est-elle? Celle des enfers. Du schéol.

Concrètement, cela signifie que si quiconque a été torturé, emprisonné, assassiné en raison de la découverte du subterfuge, il faudra alors avoir le courage de sanctionner, de manière inclémente, tous ceux qui ont concouru ou su ce qu'il advenait. Et n'ont rien fait.

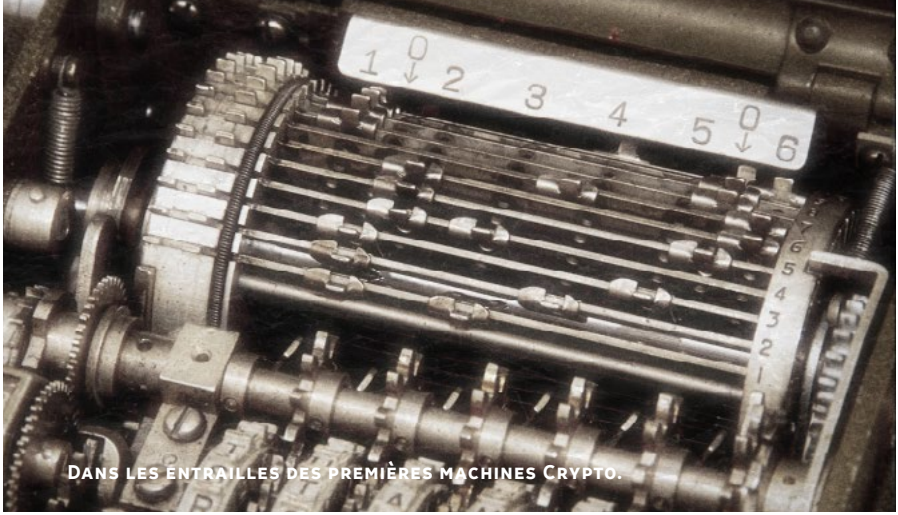
La démocratie helvétique se targue d'être la plus vieille démocratie du monde. Cela ne restera que des mots si elle est incapable de vouer aux gémonies ceux qui en ont fait l'obéissant valet d'un service de renseignement étranger.

La ligne rouge a-t-elle été franchie?

Vous en saurez beaucoup plus dans un prochain article-

Le magazine de l'Antipresse est une publication de l 'Association L'Antipresse. Conception, design et réalisation technique: INAT Sàrl, CP 429, Sion, Suisse. Directeur-rédacteur en chef: Slobodan Despot.
Abonnement: via le site ANTIPRESSE.NET ou nous écrire: antipresse@antipresse.net
N. B. — Les hyperliens sont actifs dans le document PDF.

It's not a balloon, it's an airship! (Monty Python)



Dans les entrailles des premières machines Crypto.

ANGLE MORT par Arnaud Dotézac

Crypto saga, épisode 1: qui était Boris Hagelin?

L'affaire Cryptoleaks, qui ébranle actuellement les institutions helvétiques, mérite une attention particulière, même au-delà des frontières suisses. En réalité, elle concerne le monde entier dans la mesure où la plupart des pays y sont impliqués, soit comme épieurs, soit comme épiés.

Le rôle principal dans cette magistrale entourloupe est tenu par Crypto AG, une entreprise fondée à Zoug en 1952, produisant des machines de chiffrement militaire, réputées «propres». Or, une longue série de révélations démontre que les algorithmes de ces machines étaient truqués au bénéfice de la NSA, de la CIA, du BND allemand et sans doute également des services britanniques. Ce petit monde pouvait espionner à sa guise les heureux propriétaires desdites machines alors qu'ils se croyaient protégés par la «security made in Switzerland». Entre 120 et 130 gouvernements se seraient ainsi fait berner.

Cette affaire soulève plusieurs questions politiques en Suisse.

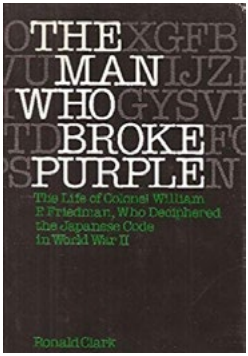
En premier lieu, les autorités fédérales, le Service de Renseignement de la Confédération (SRC) et le Conseil fédéral (gouvernement), nient contre toute vraisemblance en savoir quoi que ce soit. Ce mensonge flagrant ne tiendra pas longtemps. En fin de compte, les autorités seront bien obligées de s'expliquer sur cette grave entorse au droit de neutralité suisse. La Confédération aura en effet autorisé, en connaissance de cause, la vente de ces machines piratables à des pays en guerre avec les Américains.

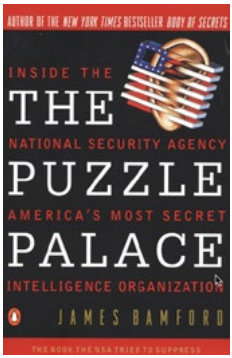
Se pose également la question du

degré de mensonge d'État admissible dans une démocratie comme la Suisse. Peut-être faudrait-il envisager une sorte d'échelle de Richter du mensonge politique afin de confiner un tant soit peu l'omnipotence des autorités en ce domaine?

Cette affaire pourrait aussi nuire gravement à la santé diplomatique helvétique, fondée sur sa politique des bons offices en tant que tiers neutre et de confiance.

Pour finir, elle dévoile un fort degré d'inertie au sein du peuple souverain, qui semble s'être habitué à ne plus réagir qu'aux stimuli de ses smartphones. Il n'y a encore pas si longtemps, une divulgation de bien moindre ampleur aurait suffi à mobiliser les consciences. Rappelons-nous l'affaire des Fiches ou les réseaux *stay-behind* (P26). Rien de tel aujourd'hui et c'est d'autant plus étonnant que cette affaire resurgit, à intervalles réguliers, depuis plus de quarante ans!





ALERTES PRÉCOCES

La première évocation d'une collaboration entre le fondateur de Crypto et la NSA figure dans l'ouvrage de **Ronald Blake** *The man who broke purple* publié à Londres chez Little Brown en 1977 et que la NSA a tenté de faire interdire. Ce livre est en réalité une biographie d'un des plus éminents hauts fonctionnaires de la NSA, **William Friedman**, qui deviendra l'un des officiers traitants de **Boris Hagelin**, en 1957.

Puis c'est au tour de **V. James Bamford**, dans *The Puzzle Palace*, paru en 1982 chez Houghton Mifflin Co. (Boston), de révéler noir sur blanc l'enrôlement de Crypto AG pour la NSA. L'auteur avait réussi à se procurer des documents encore non classifiés par simple oubli des services, ainsi que des documents judiciaires publics. Immédiatement après cela, le président **Reagan** ordonna leur mise au secret mais le mal était fait et, déjà, largement commenté par la presse, notamment le New York Times du 19 septembre 1982.

Difficile pour les autorités suisses d'affirmer, en 2020, qu'elles ne savaient rien. D'autant que dans son édition du 17 avril 1986, le *Financial Times* en remit une couche en mentionnant Crypto AG comme maillon explicite du système d'écoute américain!

Puis vint, en 1992, l'arrestation de **Hans Buehler**, cadre commercial sans histoire de Crypto en visite de routine chez ses clients iraniens. Quoique motivés sans doute par d'autres raisons, les Iraniens prirent publiquement prétexte de la trahi-

How US broke Libyan codes

BY PETER MARSH IN LONDON

THE US Government should release more details of the radio messages it has intercepted that provide evidence of links between the Libyan regime and terrorist activities in Europe, according to Professor Ray Cline, a former deputy director of the US Central Intelligence Agency (CIA).

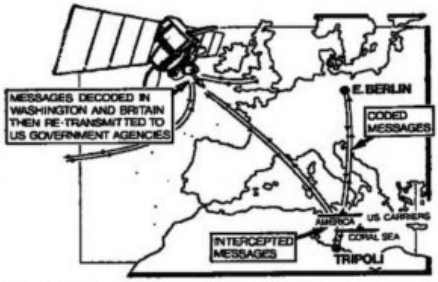
Prof Cline, of the Centre for Strategic and International Studies at Georgetown University in Washington, said yesterday that "it would be helpful" if President Ronald Reagan authorised disclosure of some of the language used by Libyan officials and terrorists in messages said to have been passed between Tripoli and European capitals.

Prof Cline, who was at the CIA from 1963 to 1966 and from 1969 to 1973 was director of intelligence at the State Department, was speaking after US officials had already lifted some of the normal veils of secrecy over such interception of radio messages.

The body primarily responsible for these activities is the National Security Agency, based in Washington, which works closely with Britain's Government Communications Headquarters (GCHQ) in Cheltenham.

An essential part of the work of both these orgainsations is the breaking of codes used routinely by governments to encrypt their radio messages.

For enciphering, Libya uses sophisticated equipment made by Crypto of Switzerland, said by intelligence sources yesterday to be one of the world's leading companies in this technology.



Other companies in the forefront of encoding technology include Racal and Plessey of Britain, and Harris, ITT, Litton and the Collins division of Rockwell in the US.

Such equipment translates ordinary written sentences into a stream of seemingly meaningless symbols which can be interpreted only by a decoding mechanism at the the point of reception. The symbols are transmitted as radio signals.

US government officials have cited radio messages between Tripoli and the nation's embassy in East Berlin as providing evidence of Libya's involvement in terrorist activities. A bomb explosion in a West Berlin discotheque, on April 5, assumed to be the work of Libyan terrorists, killed two people and injured about 200.

Despite the high-quality equipment available to Tripoli, it appears that breaking the Libyan code was not too difficult for US intelligence workers. According to one British intelligence expert, it is unlikely that the Soviet Union, itself highly skilled in encoding, would have helped Col Muammer Gadaffi by passing on details of its own top radio coding techniques.

The pattern of events seems to have been as follows:

In recent weeks, US ships from the 6th Fleet have been taking up position off Libya, ostensibly for practice manoeuvres but more realistically to gather radio signals flowing to and from Tripoli.

Navy ships routinely carry sophisticated computer equipment used to pick up signals intended for them, to interfere with enemy transmissions by techniques such as jamming and also to decipher enemy radio traffic. The aircraft carriers America and Coral Sea, the fleet's main battleships, can be assumed to carry the bulk of the 6th Fleet's interception hardware.

Once picked up by aerials on the US ships, the Libyan signals have to be decoded. This is done by transmitting the messages – still in their meaningless, garbled state – by communications satellite, either to the NSA in Washington or GCHQ in Britain. The satellites would probably be members of the Defence Satellite Communications System (DSCS) series, of which more than a dozen have been launched.

The US and UK security agencies work in close conjunction under a series of agreements not made public. Some NSA staff are housed in the GCHQ's main building in Cheltenham.

At either the US or UK centres, computers would go to work "unscrambling" the messages using complex code-breaking programs. The first such programs were those used by British intelligence experts during the Second World War to break the Enigma code in which German messages were encrypted.

According to intelligence experts, with modern techniques it probably takes no more than a few seconds for the computers to translate the coded Libyan messages to comprehensible sentences. The messages, in their uncoded state, would then be flashed back by satellite to the US fleet or to other US government agencies.

Signals picked up in this way by ships would be supplemented by radio transmissions intercepted by electronic signal-gathering satellites, called "ferrets", of which the US has several in orbit at any one time.

son des Suisses. Ils ne relâcheront Buehler qu'après 9 mois d'interrogatoires serrés et de détention sous régime sévère, outre le versement d'une rançon d'un million de dollars. C'est à ce moment que les informations relatives aux «*back doors*» des machines Crypto se mirent à déferler. L'actionnariat réel de Crypto commençait même à intriguer du monde, comme en atteste une enquête du *Spiegel* parue en 1996. On pouvait y lire que plusieurs membres du conseil d'administration de Crypto AG agissaient en fait pour le compte d'intérêts allemands, suggérant déjà clairement le rôle actif du BND dans la direction de l'entreprise. On y apprenait aussi que certains ingénieurs allaient chercher leurs directives au siège du Bureau central du chiffrement à Bad Godersberg, dans la proche banlieue de Bonn. Quand ce n'était pas des membres connus de la NSA, qui venaient, jusqu'à Zoug, donner les leurs et s'assurer de leur mise en œuvre.

Mais voici qu'une troisième salve fut tirée en 2014, plus puissante encore que les précédentes. Les autorités américaines levèrent fina-

LE NOUVEAU QUOTIDIEN 5. Juli 1994

Hans Bühler soupçonne la Crypto AG d'espionnage

L'ingénieur, emprisonné en Iran, puis libéré et licencié, réitère ses accusations. L'entreprise a porté plainte. Procès aujourd'hui

A 53 ans, Hans Bühler est un homme brisé. Il a passé neuf mois et demi dans les prisons iraniennes en 1992, accusé notamment d'espionnage, de contacts non autorisés avec des militaires et de consommation d'alcool. L'ingénieur et homme d'affaires travaillait pour l'entreprise zougoise Crypto AG, spécialisée dans la fabrication d'appareils pour la transmission de messages codés. Ses employeurs ont payé la caution d'un million de dollars. Mais, peu après son retour en Suisse début 93, Hans Bühler a été licencié. Depuis, le Zurichois cherche à comprendre ce qui lui est arrivé et dirige ses soupçons vers ses anciens employeurs.

Nerveux, la voix parfois cassée par un sanglot, Hans Bühler a donné une conférence de presse hier à Zurich. Ce pourrait être la dernière: ce matin débute le procès intenté par Crypto AG contre lui et la maison d'édition Ringier. La *Schweizer Illustrierte* avait publié en mai l'affirmation de Hans Bühler qui accusait la Crypto AG d'activités dans les services de renseignement. L'entreprise zougoise souhaite interdire à son ancien vendeur de haut vol de continuer à semer le doute sur ses activités.

En compagnie de sa famille et d'un collègue iranien lui aussi emprisonné et licencié, l'homme d'affaires a, hier, répété ses dires: des appareils de codage auraient été manipulés par les services secrets allemands et américains, selon lui, pour permettre à ces mêmes services de décoder les informations échangées dans un pays tiers. Hans Bühler se demande s'il n'a pas été abusé et si son arrestation ne découle pas des activités de la Crypto. Ces soupçons, ces accusations sont graves. Mais l'homme d'affaires n'a pas de preuves pour les étayer. Il affirme cependant que des témoins seront cités au procès.

Parmi les ingénieurs liés à la Crypto dont les récits fondent les attaques de Hans Bühler se trouve un Zurichois qui avait témoigné sous anonymat lors de l'émission Rundschau du 23 mars. Il avait été le premier à évoquer la manipulation d'appareils. Hier, Hans Bühler a dévoilé son identité mais sans avoir obtenu son accord préalable... Les déclarations de cet homme, dont le nom est connu à Berne, avaient suscité le lancement de recherches préliminaires par le ministère public afin de savoir s'il fallait ouvrir une procédure pénale contre la Crypto AG. Peter Lehmann, porte-parole du ministère public, confirme la poursuite des recherches préliminaires mais refuse de commenter l'avancement des travaux, tout comme il ne souhaite pas s'exprimer sur d'«hypothétiques éventualités» telles que celles soulevées par Hans Bühler.

Dans cette affaire particulièrement absconse, la Crypto ne «veut émettre aucun commentaire avant le procès». L'entreprise avait démenti les affirmations diffusées lors de l'émission Rundschau, selon lesquelles ses appareils auraient été trafiqués.

SONIA ZORAN
ZURICH

lement le secret-défense protégeant les archives de **William Friedman**, celles-là mêmes qui furent bloquées par Reagan. Or, ces archives regorgent de rapports probants et de correspondances édifiantes sur les mouchardages de Crypto AG en faveur de la triade NSA, CIA et BND. Les documents principaux sont aisément consultables sur le site de cryptomuseum, qui les a indexés (en bas de page).

RAVALEMENT DE FAÇADE

Beaucoup d'encre se mit encore à couler. Mais à Berne, en haut lieu, on passa encore l'éponge cependant qu'on organisait, très discrètement, la restructuration du groupe Crypto de manière à lui refaire, en 2018, une virginité via deux entités toutes neuves. A l'époque, personne n'y prit garde, des opérations de ce type étant courantes. C'est seulement le 11 février 2020 qu'on en saisira la vraie portée: il s'agissait en fait de sortir la CIA du capital de Crypto AG, qu'elle détenait à 100 %! On apprenait maintenant que la CIA et le BND avaient été depuis 1970 les réels propriétaires de Crypto AG, à parts égales, avant que la CIA ne rachète toutes les actions du BND en 1993, devenant ainsi jusqu'en 2018 son propriétaire unique.

C'est d'ailleurs le seul scoop de cette «enquête» conjointe du *Washington Post* (organe américain) et de la ZDF (organe allemand), avec accessoirement l'implication de la SRF (télévision suisse alémanique) et de la chaîne radio hollandaise Argos conjointement au site, également hollandais, cryptomuseum.com.

Le montage CIA-BND était évidemment fort bien camouflé derrière des entités écran du Liechtenstein, des cabinets d'audit de paille, quoique fort renommés en Allemagne, et des comptes bancaires autrichiens. Ces derniers virent sortir beaucoup d'argent liquide, déversant leurs flux dans les caisses noires de la CIA et du BND.

ÉVIDENCES ET FAUX-SEMBLANTS

Mais se pose-t-on pour autant les bonnes questions? S'agit-il uniquement d'un problème de crédibilité diplomatique et de neutralité de façade pour la Suisse? Peut-on réduire toute cette affaire à une énième pratique occulte des services secrets, que viendra toujours blanchir la raison d'État? Ne doit-on pas aussi, et surtout, se pencher sur la première des qualités des communautés du renseignement, qui est justement de *savoir encoder les évidences*? N'est-ce pas là le cœur de métier du cryptage, que de rendre inintelligible aux tiers, au grand public notamment, le véritable sens des signes?

En fait, dans un tel univers, le meilleur réflexe est à coup sûr de ne jamais prendre ce type d'informations pour argent comptant, surtout quand la source n'est autre que la CIA elle-même. Quel est son intérêt de faire fuiter cela précisément aujourd'hui? Ne maquille-t-on pas autre chose? Par quels procédés? Etc. C'est en se posant ce type de questions que l'on peut espérer appréhender certains aspects du jeu en cours. Certains seulement, et en toute modestie. Ce ne sont pas en effet les fantômes du bienheureux Boris Hagelin et consorts, aussi géniaux entrepreneurs soient-ils, que l'on s'apprête à rencontrer, mais bel et bien les plus puissants prédateurs de l'intoxication, du leurre et bien sûr du fichage industriel, que l'histoire ait jamais produits.

LA TRAME D'UNE AUTOBIOGRAPHIE IDYLLIQUE

En guise d'échauffement, nous commencerons par survoler les premières lignes de l'autobiographie officielle du fondateur de Crypto AG, le mystérieux Boris Hagelin.

L'une des premières leçons données aux jeunes recrues de la NSA est de ne pas croire aux coïncidences. On leur apprend notamment à calculer le seuil au-delà duquel une coïncidence ne peut plus en être une. Cet «indice de coïncidence», comme on le nomme dans le jargon, est généralement très bas. Il est par exemple de 2 % pour des récurrences de signes dans un texte ordinaire rédigé en français, superposé à un autre du même ordre. Au-delà, le texte devient suspect. Or, l'autobiographie de Boris Hagelin est littéralement truffée de coïncidences: à près de 90 %. Mais on le comprend beaucoup mieux lorsqu'on découvre que ce n'est pas lui qui l'a rédigée, mais la NSA! Non pas que les faits relatés soient faux, car tout y semble plus vrai que vrai, mais c'est plutôt dans la manière dont on y organise la trame, les processus narratifs, les séquences d'omissions et d'émotions, etc. qu'on enfume le lecteur.

Le bon codage peut être très mélodieux, comme en l'espèce. Les escapades touristiques d'Hagelin et de son épouse aux Caraïbes, au Mexique ou en mille autres lieux bucoliques, illustrées de photos de famille, impriment l'image d'une vie détendue, dégagée des soucis matériels et bien rangée à la fois.

Les photos sont authentiques, les lieux ont bien été visités, de sorte que c'est cette empreinte émotionnelle qui marquera la cible: l'image d'un homme placide et inoffensif.

Jamais, en revanche, on ne le verra négocier avec ses donneurs d'ordre en uniforme, ces hauts, parfois très hauts gradés américains des trois Armes, ou bien leurs homologues de l'OTAN mais aussi du bloc soviétique, des dictatures sud-américaines ou du Moyen-Orient. Jamais on ne le verra davantage, et pour cause, discuter avec ses interlocuteurs et amis intimes des «Services» (sauf Friedman mais en situation bien inoffensive), là encore américains, mais aussi français, britanniques ou allemands. Ces derniers seront d'ailleurs très souvent issus des **réseaux Gehlen**, la crème des anciens espions du IIIe Reich, recyclés à grande échelle par les Américains dès 1944.

UNE ALLEMAGNE RUSSE

Le questionnement s'impose à l'égard des moindres détails, même si au final cela ne donne rien. C'est le principe même de la prise en compte des signaux faibles. Prenons l'exemple très anodin du lieu de naissance d'Hagelin. Il se dit né en 1892 à **Adschikent**, aujourd'hui en Azerbaïdjan. Une ville pourtant bien difficile à retrouver sur les cartes. En fait quasiment impossible à repérer sous cette orthographe rare. Pourquoi l'avoir choisie? Pour faire exotique? Pourquoi pas.

Correctement orthographié «Hajikand» (Hacıkənd), ce n'est qu'un minuscule hameau, perdu au milieu de nulle part sur les contreforts du Haut-Karabagh. Mais pourquoi diable sa mère aurait-elle accouché dans un tel endroit? Sans doute parce que 1892 fut la grande année du choléra à Bakou, où travaillait le père de Boris. On pourrait donc en déduire qu'elle regagnait la capitale impériale, où les Hagelin disposaient d'un beau logement familial, pour fuir l'épidémie et qu'elle fut stoppée en chemin par les premières douleurs.

Or ce hameau n'est pas sur l'itinéraire de Saint-Pétersbourg. Creusons donc encore un peu. Hajikand se trouve dans le prolongement immédiat de **Goygol**, une vraie ville cette fois. Mais cette ville fondée en 1819, le fut sous un autre nom, un nom allemand: **Helenendorf**. Il s'agissait d'une colonie de vignerons souabes, établie là sur ordre du Tsar **Alexandre Ier**, au sein d'un dispositif plus vaste destiné à contrer les velléités arméniennes de récupérer cette terre, qu'ils considèrent toujours comme la leur, comme on le sait.

Boris Hagelin est donc certes d'origine et de nationalité suédoise. Mais il est aussi un Russe de troisième génération et de nationalité. Il est bien né sur le territoire de la Sainte Russie de l'époque, mais il se trouve que c'était aussi une zone allemande luthérienne. Pourquoi le cacher ainsi? Aurait-il voulu refouler l'indice trop marqué de ses affinités allemandes? On n'en saura rien dans l'immédiat mais on aura pointé un signal faible qui pourra s'avérer utile pour la suite de notre analyse.

TURBULENCES

GRANDE-BRETAGNE · Les patients non-conformes seront privés de soins!

Jusqu'ici, le personnel des hôpitaux publics britanniques avait le droit de refuser de traiter les patients agressifs — physiquement ou verbalement —, si ceux-ci n'étaient pas dans un état critique.

Mais voici que la liberté de laisser crever va bientôt s'étendre à toute forme de harcèlement, d'intimidation ou de discrimination, en particulier les remarques homophobes, sexistes ou racistes.

Le Secrétaire britannique à la santé a adressé une circulaire au personnel soignant pour préciser qu'«aucun acte de violence n'est mineur» et que «se faire agresser ou insulter ne fait pas partie du cahier des charges».

On s'imagine bien qu'être ambulancier ou urgentiste n'est pas une sinécure: un sur sept s'est fait agresser au Royaume-Uni l'an dernier. Mais sont-ils vraiment aptes à juger si la mauvaise humeur d'un patient est raciste ou homophobe, en particulier parmi les personnes âgées qui n'ont pas encore eu le temps d'assimiler le lexique du politiquement correct? Et comment détermine-t-on si l'état du patient est critique? En vérifiant au bout de six heures s'il gigote encore?

Même dans le féroce système du crédit social chinois, on n'a pas encore inclus le refus de soins aux individus mal notés.

PAYS-BAS · Cacophonie autour du vol MH-17

Une nouvelle dissonance vient s'ajouter à la cacophonie qui a entouré l'enquête internationale sur le crash du Boeing malais dans le Donbass en juillet 2014, faisant 298 victimes. Elle vient des Néerlandais eux-mêmes, qui ont pris l'initiative de l'enquête internationale sur les causes de la catastrophe. Selon un document confidentiel émanant du Service de renseignement militaire des Pays-Bas, le Boeing se trouvait hors de portée des missiles sol-air qui ont été repérés et clairement identifiés sur des prises de vue aériennes faites le jour du drame. Grâce à une fuite, le document a fait surface à quelques semaines du procès qui va s'ouvrir le 9 mars. Or, l'acte d'accusation au centre du procès identifie précisément un missile sol-air Buk de fabrication russe à l'origine de la destruction du Boeing. Il met en cause trois ressortissants russes et un rebelle ukrainien soupçonnés d'avoir acheminé la plate-forme de tir du missile depuis le territoire russe. L'an passé déjà, l'objectivité de l'instruction menée par les enquêteurs internationaux sous l'égide des Pays-Bas a été sérieusement remise en question par le premier ministre malais Mahathir qui a réagi à la mise en accusation des 4 suspects:

> «Depuis le début, ils [les enquêteurs internationaux] n'ont jamais autorisé notre implication. C'est injuste et inhabituel. Nous pouvons donc voir qu'ils ne se penchent pas vraiment sur les causes de l'accident et qui en était responsable. Mais ils avaient déjà décidé que ce devait être la Russie. Donc nous ne pouvons pas accepter ce genre d'attitude. Nous sommes intéressés par l'état de droit, la justice pour tous, et peu importe qui est impliqué. Nous devons savoir qui a réellement tiré le missile, et c'est seulement à ce moment-là que nous pourrons accepter le rapport en tant que vérité complète».

J.-M. Bovy/21.02.2020

- Voir aussi: «La Malaisie révèle que des données de l'enquête sur le vol MH17 ont été falsifiées»

CLIMAT · Le coronavirus, une solution?

Selon le site spécialisé (britannique) CarbonBrief, l'épidémie de Coronavirus aurait temporairement réduit les émissions chinoises de CO2 d'un quart!

> Au total, les mesures prises pour contenir le coronavirus ont permis de réduire de 15 à 40 % la production dans les principaux secteurs industriels. Il est probable que ces mesures ont permis d'éliminer un quart ou plus des émissions de CO2 du pays au cours des deux dernières semaines, période où l'activité aurait normalement repris après les vacances du nouvel an chinois.
>
> Sur la même période en 2019, la Chine a rejeté environ 400 millions de tonnes de CO2 (MtCO2), ce qui signifie que le virus pourrait avoir réduit les émissions mondiales de 100 MtCO2 à ce jour. La question clé est de savoir si les impacts sont durables, ou s'ils seront compensés — voire inversés — par la réaction du gouvernement à cette crise.
>
> Une première analyse de l'Agence internationale de l'énergie (AIE) et de l'Organisation des pays exportateurs de pétrole (OPEP) suggère que les répercussions de l'épidémie pourraient réduire jusqu'à un demi pour cent de la demande mondiale de pétrole en janvier-septembre de cette année.

Greta Thunberg et les greta-groupies devraient étudier de près cette bonne nouvelle! Un bon virus global, et le problème climatique serait définitivement réglé. Ouf!

Pain de méninges

ESPIONNAGE ET LITTÉRATURE

L'espionnage et la littérature marchent de pair. Tous deux exigent un œil prompt à repérer le potentiel transgressif des hommes et les multiples routes menant à la trahison. Ceux d'entre nous qui ont été intronisés dans le monde secret ne le quittent jamais vraiment. Si nous n'en partagions pas déjà les mœurs avant d'y entrer, nous les adoptons pour toujours.

— John le Carré, *Le tunnel aux pigeons, histoires de ma vie*.