Intervention commune JJQ et JLD

Les grandes désillusions des temps modernes

1) Les téléimprimeurs de l'Ambassade de France à Moscou

Cet épisode de la guerre froide en marge de l'affaire d'espionnage Farewell (surnom de la taupe du KGB qui s'était mise au service de la France) est peu connu. Pourtant il semble avoir eu des conséquences désastreuses sur la suite de celle-ci. C'est le Colonel Cattieuw qui dirigeait à l'époque le Service central du chiffre et de la sécurité des télécommunications(SCCST) (l'ANSSI de l'époque) qui m'en a fait le récit. Il l'a relatée dans un bulletin de l'ARCSI consacré à Myosotis.

Comme beaucoup le savent ici, l'introduction de l'électricité dans les machines de traitement de l'écrit, parmi lesquels figurent les cryptographes, a généré de nouvelles vulnérabilités du fait notamment des parasites émis par ces machines. Ceux-ci peuvent dans certaines circonstances être compromettants. Lorsque ces phénomènes ont été découverts ils ont donné lieu à l'édition par l'OTAN de normes spécifiques hautement classifiées communément appelées normes « TEMPEST ». Mais dans l'affaire qui nous occupe il ne s'agissait pas de signaux parasites fortuits mais provoqués.

A Moscou l'ambassadeur de France particulièrement consciencieux tapait lui-même ses dépêches à l'intérieur d'une cage de Faraday avant qu'elles ne soient chiffrées avec une machine Myosotis puis envoyées au Quai d'Orsay. Tombé en panne, le téléimprimeur qu'il utilisait a été examiné par un technicien local. Celui-ci a découvert que l'un des condensateurs de l'alimentation laissait apparaître trois fils (bleu, blanc, rouge) reliés au secteur. Analysé quelques temps plus tard par le SCCST il a été mis en évidence qu'il s'agissait en fait d'un montage électronique transmettant les caractères des messages avant qu'ils ne soient chiffrés, à une fréquence qui se jouait des filtres mis en place dans la cage de Faraday.

On découvrit rapidement que les autres téléimprimeurs de Moscou et ceux d'autres ambassades avaient subi le même traitement ! D'un point de vue pratique l'opération était réalisée pendant un passage de la frontière russo-polonaise de la valise diplomatique selon une procédure classique, le convoyeur se laissant momentanément distraire par quelque aventure galante.

Compte tenu de la date de la mise en place des téléimprimeurs et de celle de la découverte de ce piège on peut considérer que tout le trafic le plus confidentiel entre Paris et ses ambassades dans le bloc communiste a été lu en temps réel pendant 5 à 6 années… Nos amis américains en furent informés et découvrirent des pièges semblables un peu partout comme du reste nos autres Alliés. Certains parmi vous ont sans doute eu le plaisir de découvrir dans la salle des ambassadeurs de la DGSE un florilège de ce qui se faisait de mieux à l'époque de la guerre froide : les montages électroniques miniatures cachés dans les barres d'espace des machines à écrire ou des micros dans les bois de lit comme dans les cadeaux échangés entre chefs d'Etat sont un délice. Il y a actuellement quelques exemplaires de ces gadgets à l'exposition de la Cité des sciences «L'espion ».

Informé et furieux, le Président de la République qui comprit en particulier qu'une rencontre récente avec Léonid Brejnev avait, selon toute vraisemblance, été biaisée par cette perte de confidentialité

décida l'expulsion de 47 diplomates soviétiques dénoncés comme espions par la taupe du KGB qui nous renseignait. Erreur funeste car la liste de ces espions trahissait celui qui avait pu l'établir et la France perdit sa source d'information la plus précieuse : Farewell fut exécuté.

Notons que la machine Myosotis n'a pas été mise en cause mais elle a été contournée par un défaut de surveillance du périphérique qui lui était associé : le téléimprimeur SAGEM. Or peu avant la mise en place des pièges, bien que s'étant interrogés sur les emplettes que voulaient faire les soviétiques chez SAGEM, les services chargés du contrôle des exportations de matériels sensibles, SGDN et SCCST, avaient donné leur feu vert à une commande de centaines de condensateurs…!

Cette histoire eut pour mérite de faire prendre au sérieux la menace Tempest et dès lors ne furent plus conçues que des machines et des installations respectant cette norme. Du moins en théorie.

C'est ainsi que quelques années plus tard comme officier chiffre de l'EMA je fus chargé de mettre en service la première station de mesure de ces SPC. A titre d'essai je demandai à mon spécialiste d'aller se poster de l'autre côté du Boulevard St Germain en face de l'Etat-major, pour voir ce qu'il recueillerait. Une heure plus tard il revenait me voir en me disant : « Mon colonel vous ne m'aviez

pas dit que vous m'envoyiez en mission dans le sud le mois prochain ! ». A presque 100 mètres de distance, il avait recopié l'écran du bureau des déplacements , un ordinateur GOUPIL G3, (qui allait se révéler être un régal pour les chasseurs de SPC), sur lequel figuraient également les déplacements avec dates, horaires et N° de vol des plus hautes autorités du ministère. Ceci en pleine période d'attentats dont celui du Ténéré. Mais ce type d'ordinateur équipant aussi tous les bureaux les plus sensibles la moisson fut stupéfiante.

Je fis réaliser par la DGA un film de sensibilisation « l'Espion et l'ordinateur »qui, tourné d'emblée en deux langues anglais et français fit un tabac dans les pays de l'OTAN. Malheureusement comme j'ai eu l'occasion de le dire cette menace fut prise en compte à grand frais au moment où une autre plus insidieuse et moins spectaculaire commençait tout juste à être perçue et aurait mérité au moins un traitement de même niveau : celui de la sécurité logique des ordinateurs.

2) L'affaire Humpich

A la fin du siècle dernier la France, incontestablement avait pris le leadership dans l'industrie de la carte à microprocesseur (ou carte à puce) dans le domaine Bancaire notamment. On rappellera que c'est Michel Ugon de BULL (accessoirement membre de l'ARCSI) qui le premier réussit à implanter un microprocesseur sur une carte rendue ainsi capable d'effectuer des calculs permettant d'assurer des contrôles de sécurité dignes de ce nom. Dans cette aventure on ne mésestimera pas le rôle essentiel de deux autres acteurs, Louis Guillou et son complice ici présent Jean-Jacques Quisquater qui réussit à introduire à marche forcée et « au chausse pied » les algorithmes cryptologiques sérieux qu'étaient à l'époque le DES et le RSA.

De mon côté en tant que patron du SCSSI (l'ANSSI de l'époque 95-2000) j'avais depuis longtemps considéré la carte à puce comme l'outil de sécurité ayant le meilleur rapport coût/ efficacité. Et nous en avions fait notre cheval de bataille à tel point que le schéma de certification des produits de sécurité que nous avions bâti d'abord sur les critères européens ITSEC puis ensuite sur les Critères Communs, avait le composant des cartes à puce comme principal objet d'application. Outre la carte bancaire du GIE CB, nous avions réussi à engrangé dans notre démarche de certification la carte Vitale, celle des professionnels de santé (CPS) et convaincu les promoteurs du PME (Porte-Monnaie Electronique) de se plier à cette exigence. Des industriels étrangers, coréens, japonais et même américains tels que MOTOROLA s'en étaient même remis à notre expertise pour l'évaluation de leurs composants ! C'est l'époque où le N°2 de la NSA me présentait à son nouveau patron en disant « le SCSSI est un petit service mais il abat un travail considérable ». Cela se passait à une époque où les cartes américaines fonctionnaient encore quasi exclusivement avec une piste magnétique et où le taux de fraude était plus de 100 fois supérieur à celui observé dans notre pays. Nous tenions là une technologie clef dont nous pouvions mesurer la progression d'année en année à l'occasion du salon parisien « Carte 199x ».

Or c'est en cette fin des années 90 qu'apparurent les premières tentatives de déstabilisation provenant d'outre Atlantique. Des labos sponsorisés se livraient à des attaques contre la technologie européenne et diffusaient les vulnérabilités qu'ils pensaient déceler.

Pourtant ce n'est pas un laboratoire mais un personnage solitaire, self made man, qui en France se passionna pour ces bouts de plastique à puce dorée et fit trembler le tout puissant GIE CB. Serge Humpich en effet étudia et décortiqua pendant quatre années au fond de son garage (comme les fondateurs d'Apple) le mécanisme de la carte bancaire allant jusqu'à acheter dans un vide grenier ou aux puces un terminal de point de vente. Quelques connaissances acquises en cryptologie lui permirent de réaliser des cartes permettant de franchir le premier niveau de contrôle des cartes bancaires, pas très élevé. Celles-ci ne permettaient toutefois pas de retirer de l'argent dans un distributeur ni de faire des achats dépassant un seuil de 300 F.

Soucieux de légalité mais souhaitant tout de même rentabiliser son investissement il chercha par l'intermédiaire d'un avocat à monnayer sa compétence. Le GIE CB fit d'abord mine de jouer le jeu et demanda des preuves. S. H prépara 10 cartes et alla, muni de celles-ci, retirer dans des automates de la RATP des tickets de métro qu'il se garda bien d'utiliser. Hélas ! Le GIE était plutôt enclin à couper les pattes à cet énergumène. C'est alors que ses responsables me contactèrent pour connaître le point de vue du « grand méchant », qualificatif dont d'autres banquiers usaient pour nommer le SCSSI.

J'avais été informé de l'affaire et mes troupes avaient eu le temps de m'instruire sur la légèreté des banques à qui mon service rappelait depuis 14 années que le système devait être renforcé notamment car utilisant des clefs trop courtes. Je surpris mon interlocuteur en disant que j'aimerais bien disposer d'un tel talent dans mon équipe, du coup il me demanda ce qu'en pensait la police. J'avais bien une idée mais par acquis de conscience j'appelai le DGPN avec qui j'avais des rapports courtois. Je lui fis part de l'affaire et lui évoquai mon idée de recruter ce pirate apparemment honnête(on dirait hacker éthique aujourd'hui). Le DGPN me dit qu'il allait consulter ses conseillers et qu'il me rappellerait. Ce qu'il fit quelques instants plus tard. Mais là, l'affaire sembla scellée et je devinai qui il avait consulté dans son entourage : un ancien conseiller juridique du SCSSI qui menaçait les agents du service coupables selon lui de favoriser la prolifération des moyens de chiffrement !

« On le coffre ! » me déclara-t-il en récitant : « il a enfreint la loi Godfrain en s'introduisant dans un système informatique sans autorisation et en s'y maintenant ». Cette loi, pour le malheur de Serge Humpich, n'avait à ma connaissance encore jamais été appliquée et c'était là l'occasion rêvée de l'utiliser. « Quant à votre idée de recruter un pirate dans votre service ajouta-t-il oubliez-là, l'expérience montre qu'un pirate reste un pirate et vous risquez les pires ennuis ». Je m'abstins de lui dire qu'il y avait bien des policiers qui faisaient régulièrement appel à des truands.

Résultat Serge Humpich fut poursuivi et condamné mais durant le procès, l'opinion publique avait dans l'ensemble pris le parti du petit génie contre l'ignoble GIE qui fit la plus grande contre-performance médiatique de son histoire. S.H ne fit pas de prison mais sa menace de révéler la clef qu'il avait trouvée plana pendant plusieurs mois. Le ministère des Finances me demanda même de présider à Bercy une réunion que l'on aurait pu qualifier « de crise » à laquelle furent priés d'assister entre autres le N°2 de la Banque de France, l'état-major du GIE-CB, le Trésor et d'autres acteurs concernés. On en trouva quelques échos dans les médias. La banque de France ayant, semble-t-il, redécouvert qu'elle était responsable des moyens de paiement, s'y montra assez remontée contre le GI E et exigea des actions.

Inauguration du CESTI du LETI

Le Monde

CAHIER SPÉCIAL

D'Amsterdam à Paris, la mode hommes 2000 en capitales

SAMEDI 11 MARS 2000

Alerte à la sécurité des cartes bancaires

● Les cartes à puce ne sont plus inviolables ● Le responsable de la sécurité des systèmes d'information demande aux banques de réagir vite ● La Banque de France s'inquiète du retard pris ● Les transactions via Internet sont à l'origine de la majorité des fraudes

Le secret de Polichinelle

PÈLERINAGE

Paris-La Mecque

Début 2000 je devais aller inaugurer un nouveau laboratoire au LETI de Grenoble fruit d'une opération initiée par le SCSSI suite à la braderie d'une perle de France Telecom par un patron pour le coup peu inspiré. Celui-ci avait en effet décidé de se séparer de deux équipes de Caen et Grenoble (moins de 10 personnes) qui constituaient la force de frappe du SCSSI en matière d'évaluation des composants de carte à puce. Ce sont eux en particulier qui vous trouvaient le mot de passe de votre carte bancaire en moins de 5 minutes. J'avais proposé aux autres acteurs nationaux de la carte de racheter ce joyau mais c'est finalement Bernard Barbier qui au nom du CEA fit la meilleure proposition en créant au sein du LETI, un CESTI. Bernard avait bien fait les choses pour l'inauguration et convoqué le ban et l'arrière ban de tout ce qui comptait dans le secteur mais aussi la presse en abondance. Or la veille, la clef des cartes fut révélée : la menace avait été mise à exécution. Résultat : alors que je venais de terminer mon discours, une journaliste de l'AFP me questionna sur cette information en me demandant ce que nous allions faire. J'étais coincé je ne pouvais me taire et nier qu'une brèche s'était produite. Et j'ai alors exhorté les banques et leur autorité de tutelle à faire le nécessaire pour rétablir rapidement la confiance des populations dans la technologie de la carte à puce. Le lendemain Le Monde titrait en une sur mon intervention déclenchant un cataclysme avec des répercussions jusqu'aux Etats-Unis. Il ne fait pas bon se mettre les banques à dos et ma carrière en souffrit quelque peu.

La perte de confiance dans la carte n'était pas exclue : un rapport secret commandité par une grande banque et une grande compagnie d'assurance aurait conclu que si tous les Français rapportaient leur carte et décidaient de repasser à la monnaie sonnante et trébuchante ou aux chèques il en coûterait 30 milliards de francs. Et encore cela prendrait du temps. En revanche pour remplacer les cartes et les terminaux il en coûterait 500 millions. Evidemment on connait l'éternel principe du capitalisme « nationaliser les pertes et privatiser les profits ». Les banques analysèrent la situation : « 500 millions c'est nous qui allons les payer avec les commerçants, 30 milliards ce sera le contribuable. Hâtons-nous donc lentement de changer les choses ». On continua donc à vivre dangereusement pendant des années jusqu'à l'adoption de la norme EMV.

La leçon : la rapacité de certains avait risqué de mettre en péril un fleuron de l'industrie française car au-delà de la carte bancaire c'était toute l'industrie des cartes, SIM en particulier à l'époque en plein boom, qui risquait d'en pâtir. La technologie des cartes à puce semblait à l'époque hors de portée du banditisme qui se contentait d'utiliser les tickets laissés par les clients et sur lesquels figurait le N° des cartes. Serge Humpich venait de prouver que les choses avaient Changé.

D'ailleurs au même moment circulait déjà sur Internet une liste de toutes les vulnérabilités affectant les cartes…