Introduction aux 13es rencontres de l'ARCSI le 26 novembre 2019 à la BNF

Général Jean-Louis Desvignes Président de l'ARCSI

Bonjour à toutes et à tous. Je me réjouis de vous voir aussi nombreux pour assister à ces 13es rencontres de l'association des réservistes du chiffre et de la sécurité de l'information et suis heureux de vous accueillir dans ce somptueux amphithéâtre que la Bibliothèque Nationale de France a mis à notre disposition pour la deuxième année consécutive. Les fidèles de nos évènements se souviennent que l'an dernier c'est la directrice des manuscrits, **Isabelle le Masne de Chermont**, qui nous avait accueilli et que, quelques temps plus tard, nous avions eu la chance de la recevoir en retour lors de notre dîner annuel à l'Ecole militaire . Nous avions également eu le bonheur d'écouter Madame **Camille Désenclos** de l'Université de Haute Alsace sur un sujet directement en rapport avec nos activités. Cette année c'est encore grâce à la bienveillance de Monsieur **Denis Bruckmann** à présent directeur général de la BNF que nous devons d'être dans ce cadre magnifique et à qui sans attendre je cède la parole.

***

Monsieur le directeur général, je sais que vos occupations ne vous permettront pas d'assister à notre colloque aussi je voudrais dès à présent vous exprimer au nom de tous les membres de l'ARCSI mes plus chaleureux remerciements pour votre accueil et à travers vous remercier toutes vos équipes et particulièrement tous vos collaborateurs qui ont répondu avec célérité et beaucoup de gentillesse à nos différentes demandes.

En remerciement de votre action à notre égard, je vous prie d'accepter ce modeste présent : la médaille des 90 ans de notre association ainsi que ce catalogue très recherché qui a accompagné l'exposition des Archives nationales en 2015 « Le secret de l'Etat ». Exposition à la réussite de laquelle l'ARCSI avait largement contribué notamment en mettant à la disposition des AN des objets de notre collection et en organisant les conférences d'accompagnement.

***

Poursuivant mes remerciements je voudrais me tourner vers nos partenaires fidèles qui nous permettent de vous recevoir dignement **: le Groupe Orange** dont nous avons plusieurs représentants et dont nous accueillerons cet après-midi le directeur de la sécurité, **THALES** qui nous accompagne depuis toujours, The Greenbow dont j'ai vu qu'elle avait reçu le label « fournisseur de la Défense », **Hervé Schauer 2 (HS2)** toujours présent à nos rendez-vous**,** tout comme **Citalid, Captronic, Quakslab** et bien **entendu MAGSECUR** et **Global Security Mag**. J'anticipe également mes remerciements en direction de la société nourricière **ECOFIH** pour le lunch de 13h.

***

Comme vous le savez ces rencontres ont repris le thème déjà évoqué dans le passé de la confiance et plus précisément, pour ce qui nous concerne, celui de la confiance dans les outils imaginés pour remédier aux vulnérabilités des moyens de communication et principalement de l'Internet même si le besoin de sécurité concerne aussi le stockage des données , leur archivage ou l'accès aux services etc.

Protéger et percer les protections a toujours été une activité réjouissante pour les plus habiles.

Cela était vrai du temps des Grecs comme au moyen âge, durant la Renaissance comme sous les deux Empires, durant les grands conflits du 20 ème siècle comme, j'allais dire de nos jours mais hélas non : de nos jours bien des choses ont changé, la situation pour les moins avertis est encore pire !

D'abord parce que l'information aujourd'hui malgré son abondance incommensurable a une valeur croissante, ensuite parce que les moyens de la transmettre ou de la traiter offrent à ceux qui les maîtrisent une opportunité absolument inégalée d'assoir leur puissance et leur pouvoir sur l'humanité.

De tout temps des hommes clairvoyants, conscients de ce pouvoir ont mis leur talent au service de la maîtrise de l'information soit en la protégeant tâche généralement confiée aux chiffreurs soit en déjouant les protections mises en œuvre par leur adversaire tâche dévolue aux cryptanalystes compétences souvent réunies en une seule. Et la guerre entre la cuirasse et l'épée s'est perpétuée durant les siècles avec de temps en temps un avantage à l'une ou l'autre des branches en fonction de l'évolution des techniques mais aussi parfois en fonction de considérations sociologiques, psychologiques voire morales. Ainsi observe-t-on notamment à la fin du 18ème siècle une perte de compétences l'argent permettant sans doute d'acheter les codes plutôt que de se fatiguer les méninges à décrypter les dépêches. De manière surprenante les Révolutionnaires qui ne dédaignaient pas l'inquisition décrétèrent le secret des correspondances. Cela ne les empêcha pas d'exploiter la faiblesse du chiffre de Marie-Antoinette pour la raccourcir. De même après la 1ère guerre mondiale quand, bien qu'ayant fort appris des Français en matière de cryptologie (voir la lettre de remerciements du LCL Yardley au capitaine Painvin pour ses cours de cryptographie) le président des Etats-Unis considéra qu'il était immoral de lire la correspondance de ses amis…Toutefois ce noble sentiment ne tarda pas à évoluer et la Black Chamber de Yardley donnera quelques années plus tard Christal Palace c'est-à-dire la NSA.

Par conséquent, le principal moyen de protéger sa correspondance a été longtemps le recours à la cryptographie et nous allons voir ce matin avec Hervé Lehning et Philippe Guillot en particulier comment la confiance dans cet art avant qu'elle ne devienne une science a connu des hauts et des bas.

Mais la technologie évoluant d'autres composantes de la confiance sont venus s'ajouter et bien vite on a compris qu'un bon procédé cryptologique sur le plan théorique, voire réputé inviolable, mais mal implanté dans une machine pouvait s'avérer catastrophique. L'arrivée de l'informatique, « boostée » rappelons-le en partie par le besoin de casser le chiffre du Reich a notablement étendu le champ des possibilités des attaquants par rapport aux défenseurs.

-Comme dit précédemment l'ordinateur a permis de réaliser de manière industrielle des attaques notamment par force brute inimaginables manuellement.

- L'introduction de l'informatique dans les moyens de communication et de traitement des données a offert de multiples et nouvelles opportunités de fuites et de canaux cachés.

- Aux failles logicielles et matérielles imputables aux concepteurs et manufacturiers se sont ajoutées les failles intentionnellement laissées à la disposition de certains Etats.

C'est ce que nous verrons notamment avec l'exposé de JJQ sur les désillusions des temps modernes.

Les défenseurs tels que **Joël Hosatte** ont donc eu bien du mérite pour bâtir malgré tous ces pièges des protections efficaces.

Mais force est de constater que bien souvent c'est à des négligences humaines que l'on doit les plus grandes désillusions.

Pourtant certaines innovations semblent parfois apporter la solution ce fut le cas avec les systèmes à clefs publiques, la cryptographie quantique et maintenant les blockchains. Là encore, comme toujours nous verrons que chaque nouvelle technologique a ses deux faces et voit souvent et de plus en plus tôt l'avantage qu'elle apporte détourné à des fins a minima délictuelles**. Jean-Paul Delahaye** suivi de **Jean-Luc Moliner** vont essayer de nous éclaircir sur le pouvoir de quelques-unes de ces nouvelles technologies révolutionnaires.

Toute solution sécuritaire proposée nécessite d'être évaluée. C'est à l'ANSSI que revient ce rôle en s'appuyant sur un schéma de certification appelé prochainement à évoluer en s'européanisant. C'est **Franck Sadmi** qui nous expliquera cette évolution qui devrait faciliter la tâche de certains parmi vous. Enfin il n'est pas de rencontre de l'ARCSI sans qu'on n'y parle de droit. C'est fondamental surtout quand il s'agit de confiance et ce sera **Bertrand Warusfel** qui s'en chargera.

Chaque demi-journée se terminera par une table ronde si possible conclusive et ouverte aux questions de la salle l'une sera animée par **Thierry Buffenoir** et la dernière par notre sage de service **Laurent Bloch**.

N'oubliez pas que certains de nos partenaires disposent d'un stand que vous pouvez aller visiter à tout moment mais surtout pendant les pauses. Je vous signale également la tenue du stand de l'ARCSI où vous pourrez assister à des démonstrations de notre ami **Jon Paul** qui vous présentera : le simulateur ENIGMA qu'il a développé pour notre association et la reconstruction à l'identique (comme la Flèche de Notre Dame !) du premier convertisseur analogique digital de l'Histoire utilisé dans le système SIGSALY. Il vous parlera aussi de notre projet de **Musée du Secret** pour lequel nous sommes à la recherche de partenaires. Un premier argumentaire est disponible et nous en parlerons aux membres de l'ARCSI lors de notre prochaine assemblée générale. Sachez simplement que les principaux pays EU, GB, ALL, Pol possèdent de tels musées et qu'ils sont très prisés. Nous sommes persuadés qu'une telle réalisation rencontrerait le succès. Tous ceux qui veulent nous aider d'une manière ou d'une autre sont les bienvenus.

Mesdames, Mesdemoiselles, Messieurs chers amis, je vous souhaite une très agréable et très enrichissante journée.