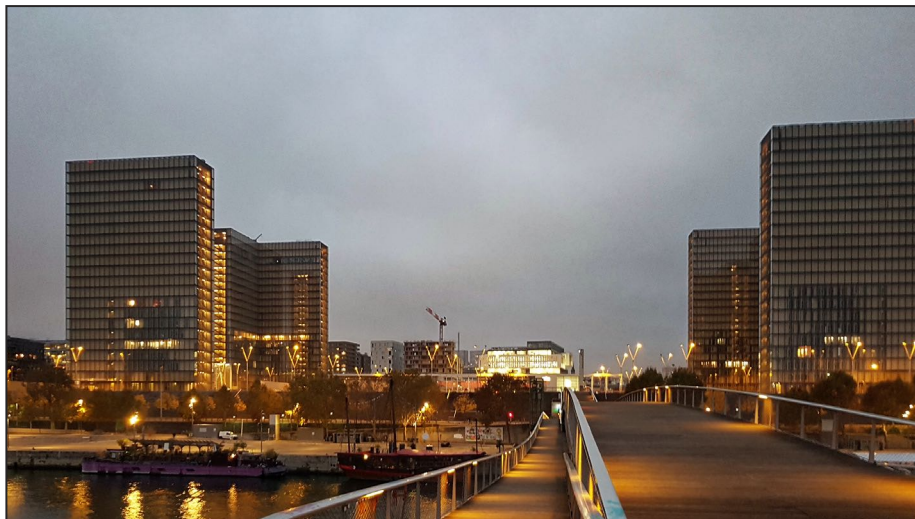


12^{es} Rencontres de l'ARCSI

Allocution d'ouverture

Jean-Louis Desvignes



La Bibliothèque nationale de France

Bonjour à toutes et à tous. Je me réjouis de vous voir aussi nombreux pour participer à ces 12^{es} Rencontres de l'ARCSI qui revêtent comme vous avez pu le voir un caractère doublement solennel et exceptionnel puisque nous célébrons en même temps, pardonnez-moi cette expression jupitérienne, mais qui ici n'oppose pas, au contraire, le centenaire de la victoire de 1918 et les 90 ans de notre association. Il se trouve en effet que ce sont les vainqueurs de la lutte contre le chiffre allemand, dont nous sommes les héritiers qui ont créé une amicale des officiers de réserve servant dans cette spécialité pour que ne soit pas complètement oublié ce que la victoire devait à ces hommes de l'ombre qui ont contribué à faire basculer l'histoire. C'est d'ailleurs pourquoi notre journée comportera une partie historique mais dans laquelle le côté scientifique et technique ne sera pas absent bien au contraire et une partie sans doute plus technique au fur et à mesure que l'on avancera vers notre époque mais qui elle ne sera pas dénuée d'aspects historiques et sociologiques qui font le charme de cette science du secret.

Mais avant toute chose je voudrais m'adresser aux membres de l'ARCSI pour les informer, s'ils n'ont pas regardé leur messagerie depuis hier soir, d'un événement qui nous touche cruellement: notre secrétaire général Jean-Marc Laloy qui était la cheville ouvrière de notre association nous a quittés. Depuis des années il se dépensait sans comp-

ter pour organiser nos manifestations, il n'hésitait pas à relancer les uns et les autres pour les encourager à participer à nos événements. Jean-Marc notre collègue notre ami, notre complice nous a quittés hier matin à l'issue d'une longue maladie. Vous aviez certainement remarqué sa disparition sur le réseau et pour certains un changement physique lors de ses dernières apparitions. Le mal était profond et malgré une résistance hors du commun Jean-Marc a fini par céder. C'est une immense perte pour tous, pour sa famille d'abord, pour ses amis et pour nous tous membres de l'ARCSI. Pour ceux qui le souhaitent il sera possible de le voir une dernière fois demain entre 10 heures et 11 h 30 à la salle funéraire de l'hôpital Charles Foix à Ivry-sur-Seine. Il sera ensuite ramené dans son cher Périgord dans son fief de la Coquille.

Son épouse me disait hier soir qu'il suivrait certainement de là où il sera notre journée pour laquelle il se faisait encore du souci il y a quelques semaines seulement. Je peux témoigner que jusqu'au bout il aura pensé à l'ARCSI qui était sa vie, et à s'intéresser au montage de notre colloque auquel il était frustré de ne pouvoir participer si ce n'est à travers les objets qu'il a bien voulu mettre à notre disposition pour une mini-exposition que vous pourrez voir dans l'espace partenaires. D'ailleurs à présent je sens qu'il s'impacientie et veut voir d'où il est, comment nous nous débrouillons sans lui.

La meilleure façon de lui rendre hommage est de réussir ce colloque.



Le magnifique amphithéâtre de la Bibliothèque nationale de France

En premier lieu puisque nous sommes dans cet amphithéâtre magnifique je voudrais adresser mes très chaleureux remerciements à la Bibliothèque nationale de France en la personne de Madame Isabelle le Masnes de Chermont Directrice du département des manuscrits et représentant Madame Sylviane Tarsot-Gillery Directrice générale de la BNF. Pour célébrer les 90 ans de notre association nous avons en effet pensé à changer de cadre et avons opté pour cet écrin prestigieux. La BNF nous a accordé des conditions avantageuses en montrant de surcroît un intérêt pour nos activités car des travaux de cryptologie ont commencé à la BNF sous la houlette d'Isabelle de Chermont. Il me sem-

ble d'ailleurs que ces travaux pourraient contribuer à exaucer les vœux de l'un de nos membres Daniel Tant ancien archiviste de Reims, qui rêve de pouvoir accéder au contenu de multiples documents dormant au fond d'armoires nationales et régionales faute de pouvoir être mis au clair les codes ayant souvent disparu. Je cède la parole à Isabelle de Chermont.

Sachez que j'ai proposé à votre directrice générale de vous offrir une tribune plus substantielle lors de l'une de nos prochaines manifestations.

Je veux également adresser mes plus vifs remerciements à nos généreux et fidèles partenaires dont vous pouvez apercevoir les Logos sur les planches projetées. THALES, ORANGE, CAPTRONIC, THEGREENBOW, G-ECHO, HS 2, CITALID, QUARKSLAB, et toujours avec le partenariat des Magazines GLOBAL SECURITY MAG et MAGSECURS.

C'est grâce à ces partenaires que nous pouvons vous recevoir dignement et être sûr que vous ne tomberez pas d'inanition. Vous pourrez en effet profiter des pauses pour reprendre quelques forces et pour aller visiter les stands de ces partenaires. Vous pourrez également voir l'exposition de l'ARCSI comprenant la collection de Jean-Marc ainsi que l'atelier de Jon Paul. À l'heure du déjeuner un buffet sera dressé. Comme chaque année nous avons fait appel à l'école de restauration Ecofih. J'espère que vous en serez satisfaits.

À présent venons-en au colloque qui a subi deux ajustements de dernière heure :

Notre premier intervenant le professeur Olivier Forcade a dû s'absenter inopinément pour un grave évènement familial. Cependant quand il m'a appelé hier pour me prévenir celui-ci a immédiatement suggéré pour le remplacer de faire appel à sa brillantissime disciple Agathe Couderc bien connue désormais des membres de l'ARCSI, que je présenterai tout à l'heure, ce que j'ai bien entendu accepté.

Deuxième changement: la table ronde finale ne permettra pas d'entendre le point de vue de l'ANSSI, celle-ci, en raison de sa charge de travail n'a pas été en mesure d'honorer notre rendez-vous traditionnel. À moins que cet organisme de 600 personnes n'ait pas trouvé de candidat pour affronter le redoutable commissaire de la CNIL... Mais nous ne perdons pas au change, loin de là, puisque c'est Jean-Luc Moliner une pointure avérée et déjà entendue dans un précédent colloque qui a accepté de revenir relever le défi alors qu'il nous aura déjà gratifiés d'un exposé très alléchant dans l'après-midi.

Je suis certain que ces deux changements gérés dans l'urgence ne perturberont en rien le bon déroulement ni l'harmonie de notre programme.

Après l'ouverture du feu par Agathe Couderc, c'est Philippe Guillot de Paris 8 qui poursuivra l'évocation historique en nous faisant le point sur l'état de l'art en cryptographie à l'aube du XX^e siècle, tandis que Jean-Jacques Quisquater (professeur émérite de l'université catholique de Louvain) qu'il est inutile de présenter davantage nous réservera quelques-unes de ses dernières trouvailles sur cette période charnière pour la cryptographie. La matinée se terminera par une table ronde introduite par Hervé Lehning désormais auteur à succès après son best-seller « toutes les mathématiques du monde ». Cette table ronde permettra des échanges entre les intervenants précédents et avec la salle.

Après le repas nous reprendrons le cours de l'histoire avec Marie-José Durand-Richard qui nous montrera comment la lutte contre la machine ENIGMA désormais vulgarisée

grâce au film « *Imitation game* » et celle de Lorentz a véritablement industrialisé le travail de cryptanalyse et offert à l'informatique l'occasion de démontrer son efficacité et ouvrir de fantastiques perspectives. Marie-José ne manquera certainement pas l'occasion d'évoquer le pèlerinage de l'ARCSI à Bletchley Parc en juin dernier. Comme elle évoquera aussi les systèmes de cryptophonie de la deuxième guerre mondiale, je vous signale que dans l'« espace partenaires », là où est exposée la collection de Jean-Marc, vous pouvez bénéficier d'explications supplémentaires fournies par notre ami inventeur et collectionneur Jon Paul sur le système SIGSALY dont il a reconstitué le cœur en utilisant des composants d'époque ainsi qu'à des démonstrations de son nouveau simulateur d'ENIGMA dont vous pouvez même passer commande! Entre nous, j'ignore totalement si ce véritable équipement cryptographique qui n'est pas à la portée du premier cryptanalyste venu est considéré comme un objet pédagogique ou une redoutable arme de guerre qui devrait être soumise à autorisation avant d'être mise sur le marché... Profitez donc de l'incertitude actuelle si vous avez quelques secrets à échanger!

Suivra ensuite un morceau de bravoure avec une revue très complète du développement de la cryptologie moderne par Jean-Luc Moliner dont le parcours extrêmement riche et varié tant au service de l'État qu'au service de l'entreprise où il exerce ses talents lui permet d'aborder tous les aspects de celle-ci.

Puis c'est un duo de choc composé de Philippe Duluc au parcours également très riche au sein du ministère de la Défense puis de l'entreprise BULL désormais ATOS, et Jean-Jacques Quisquater qui reviendra sur un sujet que je lui avais demandé d'examiner lors de précédentes rencontres et qu'il a érigé en scénario catastrophe au nom déposé: CATA-CRYPT.

La dernière table ronde sera animée par le professeur Sébastien Yves Laurent de l'université de Bordeaux. Celui-ci s'est beaucoup intéressé aux questions de renseignement et nous avons eu l'occasion de collaborer avec lui alors qu'il était commissaire de l'exposition des Archives nationales sur le Secret de l'État en 2015-2016. Cette exposition a considérablement boosté notre notoriété grâce à notre efficacité dans l'aide au montage de l'exposition et la programmation des conférences largement assurées par des membres de l'ARCSI. Dans cette table ronde nous débattons essentiellement de la liberté de chiffrer, de l'utilisation des back-doors et d'autres façons de contourner légalement ou non les procédés cryptologiques avec le commissaire de la CNIL François Pellegrini, Jean-Luc Moliner déjà présenté et moi-même.

Les questions peuvent être posées à la fin de chaque exposé et lors des tables rondes à l'invitation de l'intervenant ou de l'animateur. Je rappelle comme le fait souvent notre ami Gérard Peliks qu'une question se compose d'une phrase aussi concise que possible suivie d'un point d'interrogation.

J'ajoute que se présenter brièvement avant de poser sa question attire parfois une réponse mieux ciblée.

Je vous souhaite un très agréable et très enrichissant colloque.