La cryptologie en France : forces et faiblesses

Agathe Couderc, Jean-Louis Desvignes, Philippe Guillot, Jean-Jacques Quisquater

Ce texte correspond à l'intervention de l'ARCSI au *18th Cryptologic History Symposium "Icons and Innovation"* organisé conjointement par le *Center for Cryptologic History (CCH)* de la NSA et par la *National Cryptologic Foundation (NCF)* qui s'est tenu virtuellement les 11 et 12 mai 2022. Cette présentation a été effectuée le mercredi 11 mai 2022 au cours de la cinquième session et avait pour titre *Cryptology in France: Strengths & Weaknesses*.

Présentation de l'ARCSI et de ses représentants

Bonjour ! Mesdames et Messieurs. Je suis le Général Jean-Louis Desvignes Président de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI). L'ARCSI a été créée en 1928 par les officiers de réserve des sections de chiffre parmi lesquels figuraient les glorieux acteurs des succès de la cryptologie française pendant la Grande Guerre. Au fil des années, celle-ci s'est progressivement ouverte à de nouvelles populations et à d'autres spécialités. L'évolution des télécommunications et des techniques de chiffrement alliée au développement de l'informatique ont fait entrer dans la grande famille du Chiffre tous ceux exerçant une fonction technique, scientifique ou administrative visant à protéger les informations sensibles. Aujourd'hui, l'ARCSI rassemble des compétences pluridisciplinaires susceptibles d'être mobilisées au service du pays, de sa bonne marche, de sa sécurité et de sa souveraineté.

L'ARCSI est honorée de compter ou d'avoir compté parmi ses membres des figures illustres de la cryptologie comme David Kahn, et de grands experts : Jean-Jacques Quisquater, Michel Ugon, Louis Guillou, mais aussi Nicolas Courtois, David Naccache, Tony Rutkowski, qui apparaîtront dans ce symposium.

Parmi les nombreuses associations françaises traitant de cybersécurité, l'ARCSI, la plus ancienne, est la seule à s'intéresser à la fois à l'histoire de la science du secret et aux enjeux liés à la sécurité de l'information ou INFOSEC.

C'est la première fois que l'ARCSI ose se présenter à ce prestigieux symposium. C'est notre ami américain Tony Rutkowski qui m'a convaincu de tenter l'expérience. Pour la première fois, nous avons pensé vous donner un large aperçu de l'histoire de la cryptologie française avec ses hauts et ses bas. Je remercie le comité de sélection pour sa confiance.

Quatre intervenants suivront :

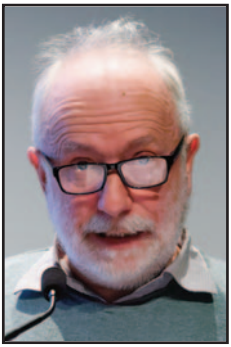
Philippe Guillot, a d'abord exercé ses talents d'ingénieur cryptologue chez THOMSON-CSF, puis dans une seconde vie de chercheur d'histoire en cryptologie à l'université Paris 8. Il vous racontera une période faste qui vit l'efficacité des cabinets noirs du XVIII[e] siècle, puis d'une période plus sombre sanctionnée par la grande défaite de 1870, provoquant heureusement un rebond salutaire.

Agathe Couderc, (doctorante à la Sorbonne), spécialisée en histoire du renseignement et relations internationales. Elle évoquera la période dorée de la Première Guerre mondiale dans laquelle la France est entrée (selon David Kahn lui-même) comme l'État le mieux préparé à utiliser efficacement le renseignement d'origine technique dont la cryptologie.

Je reviendrai alors vous parler d'abord d'une nouvelle période désastreuse, celle qui nous conduira à la défaite de 1940 puis heureusement à un nouveau rebond qui verra la France se placer au premier rang des pays occidentaux. Et offrir au monde une nouvelle technologie révolutionnaire.

Pour plaider l'excellence française à l'aube du nouveau siècle, j'ai fait appel à l'impartialité de notre illustre compagnon belge Jean-Jacques Quisquater, qui a déjà eu l'occasion de s'exprimer dans ce cénacle et qui a plusieurs fois travaillé avec des équipes françaises. Jean-Jacques ne pouvant être avec nous à Paris il interviendra depuis Bruxelles.

Sans plus tarder, je donne la parole à Philippe Guillot.


Philippe Guillot


Agathe Couderc


Jean-Louis Desvignes


Jean-Jacques Quisquater