

Partenaires de l'ARCSI

{BnF



THALES

THEGREENBOW



Citalid

quarkslab  
SECURING EVERY BIT OF YOUR DATA



MAG SECURS  
INFORMATIQUE ■ RÉSEAUX ■ TÉLÉCOM ■ INTERNET



13<sup>es</sup> Rencontres de l'ARCSI

*La confiance dans notre monde numérique peut-elle renaître ?*

Mardi 26 novembre 2019

BNF - Avenue de France - 75013 Paris

ARCSI

Association régie par la loi de 1901, reconnue d'intérêt général

SIRET : 511 069 569 00016  
<https://www.arcsi.fr>

Secrétariat de l'ARCSI  
[secretariat@arcsi.fr](mailto:secretariat@arcsi.fr)

Association  
des  
Réservistes du Chiffre  
et de la  
Sécurité de l'Information

## Mardi 26 novembre 2019

Le thème de la confiance dans les technologies du numérique a été régulièrement abordé lors de nos précédentes *Rencontres*. Pour cette 13<sup>e</sup> édition, nous nous proposons de réexaminer les raisons de la défiance qui s'est installée, sans hésiter à en rechercher des racines dans le passé, puis d'imaginer comment rebâtir la confiance au besoin en changeant radicalement les manières de l'instaurer.

Le passé nous révèle de grandes désillusions nées soit d'une méconnaissance des procédés de protection ou de la faiblesse de ceux-ci souvent jumelée à une sous-estimation de l'adversaire, soit de trahisons humaines imputables à une confiance accordée sur des bases difficilement opposables à la raison.

Les différents progrès enregistrés en cryptologie manuelle ou mécanique ont longtemps été handicapés par la nécessité de recourir à des assistants ayant accès aux éléments secrets du canal protégé (les clefs). Ces clerks (de confiance) pouvaient soit trahir comme Hans Thilo Schmidt, soit détourner à leur profit le moyen de communication protégé comme dans le cas du télégraphe de Chappe. L'avènement de moyens limitant la manipulation des clefs a repoussé les possibilités de compromission à un niveau plus élevé de la conception ou de l'utilisation des procédés. L'invention de la cryptologie à clef publique a semblé résoudre le problème en supprimant la nécessité d'un partage préalable de secrets.

Pourtant au fur et à mesure que de nouvelles technologies furent introduites dans la chaîne de confiance, apparurent de nouvelles vulnérabilités : ainsi l'électricité permit l'exploitation des parasites qu'elle engendrait, et l'informatique offrit un boulevard à la corruption tellement aisée des logiciels.

L'arrivée d'Internet aggrava les choses dans des proportions inimaginables. Livré au public sans le moindre souci de sécurité, il a vite montré ses faiblesses mais pas assez vite pour qu'on songe à ne pas le déployer. Pour faire face à ses lacunes furent développées des protections telles que les chiffreurs IP et les pare-feu tandis que toute l'informatique entraînait dans l'ère des rustines qui s'empilent. Aujourd'hui en raison d'une part de ces tares congénitales aggravées par la mise sur le marché trop rapide de produits informatiques inachevés mais aussi de failles supplémentaires introduites par certaines agences étatiques le monde est entré en cyber insécurité. Insensiblement, on s'est résigné à un état de fait qui aurait été jugé impardonnable et sanctionné pour tout autre secteur d'activité.

Certains responsables de la sécurité ont pris goût à cette lutte et oubliant parfois leur mission première - veiller à rendre difficile le contournement des protections - ils ont privilégié ce qui semblait donner un aspect opérationnel attrayant à leur métier en privilégiant le volet réactif (les cyber pompiers) à la prévention (la réalisation « *d'outils bien nés* »). Une course à l'échalote sans fin entre pirates et cyber SAMU toujours à la traîne s'est dès lors engagée.

Y a-t-il des raisons d'espérer ? Oui sans doute, en agissant dans plusieurs directions et dont certaines seront sans doute jugées utopiques. C'est tout le débat de ces 13<sup>es</sup> *Rencontres* auxquelles vous êtes très cordialement conviés.

Jean-Louis Desvignes

Participation gratuite (*dans la mesure des places disponibles*)

Inscription obligatoire sur le site de l'ARCSI : <https://www.arcsi.fr>

## La confiance dans notre monde numérique peut-elle renaître ?

- 8 h 30 *Accueil*
- 9 h 00 Général (2s) Jean-Louis Desvignes <sup>A</sup> (*Président de l'ARCSI*)  
M. Denis Bruckmann (*Directeur général de la BNF*)  
• *Allocutions d'ouverture*
- 9 h 20 M. Hervé Lehning <sup>A</sup> (*Professeur de mathématiques, écrivain et journaliste scientifique*)  
• *L'incroyable confiance des origines ou les grandes déconvenues du passé*
- 9 h 45 M. Philippe Guillot <sup>A</sup> (*Université Paris 8 Vincennes Saint-Denis*)  
• *Quelle confiance dans la cryptographie ? Une approche historique*
- 10 h 10 Pr Jean-Jacques Quisquater <sup>A</sup> (*Université catholique de Louvain*)  
G<sup>al</sup> Jean-Louis Desvignes <sup>A</sup>  
• *Les grandes désillusions des temps modernes*
- 11 h 00 *Pause\**
- 11 h 30 IGA (2s) Joël Hosatte <sup>A</sup>  
• *Les réponses et remèdes apportés par l'État jusqu'aux années 2000*
- 12 h 20 Table ronde animée par M. Thierry Buffenoir <sup>A</sup> (*VP BDS MCS Business Development - Atos*)  
avec les intervenants de la matinée  
• *Ce qui a marché, ce qui a échoué*
- 13 h 00 *Cocktail déjeunatoire\**
- 14 h 30 Pr Jean-Paul Delahaye <sup>A</sup> (*Université de Lille 1 - CNRS*)  
• *Les blockchains : outils pour une meilleure confiance ou pour de nouvelles fraudes et des dangers aggravés !*
- 15 h 15 M. Jean-Luc Moliner (*Groupe Orange*)  
• *La 5G : une question de confiance ?*
- 15 h 45 M. Franck Sadmi (*Autorité de certification cyber de l'ANSSI*)  
• *Évolutions en matière d'évaluation des produits et services de sécurité*
- 16 h 15 *Pause\**
- 16 h 45 Pr Bertrand Warusfel <sup>A</sup> (*Université Paris 8 Vincennes Saint-Denis*)  
• *Le droit du numérique, un instrument utile pour redonner confiance dans la technologie*
- 17 h 30 Table ronde animée par M. Laurent Bloch <sup>A</sup> (*Université Paris Dauphine*)  
avec les intervenants de l'après-midi et M. Christophe Labbé (*Journaliste*)  
• *Des raisons d'espérer ?*
- 18 h 10 G<sup>al</sup> Jean-Louis Desvignes <sup>A</sup>  
• *Allocution de clôture*
- 18 h 15 *Fin des Rencontres*

<sup>A</sup> Membre de l'ARCSI

\* *Durant les pauses, visite des stands de nos partenaires et démonstrations par Jon Paul <sup>A</sup> sur le stand de l'ARCSI*