Rencontre

INSTITUT DE FRANCE
Académie des sciences

ACADÉMIE NATIONALE DE MÉDECINE

ASSEMBLÉE NATIONALE — RÉPUBLIQUE FRANÇAISE — SÉNAT

OFFICE PARLEMENTAIRE D'EVALUATION
DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Cybersécurité

Mercredi 19 juin de 8h30 à 10h00
Restaurant du Sénat, Salon Pourpre,
15 ter, rue de Vaugirard, 75006 Paris

Académie des sciences - Académie nationale de médecine - Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST)

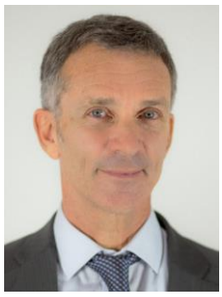
Le rapprochement entre le monde politique et le monde scientifique est important à un moment où les problèmes sont plus complexes et où les fausses nouvelles et les croyances sont propagées avec beaucoup de facilité par Internet et les réseaux sociaux. Ce rapprochement a pour objectif d'établir une relation entre deux mondes qui ont beaucoup de sujets à partager. Pendant plus de dix ans, l'OPECST et l'Académie des sciences ont développé cette connaissance mutuelle par le biais d'un programme de jumelage dans lequel un parlementaire était mis en relation avec un académicien et un jeune chercheur. Ce programme a permis aux uns et aux autres d'échanger leurs points de vue et de découvrir leurs environnements respectifs (Assemblée nationale, Sénat, circonscription, laboratoires, instituts de recherche, établissements d'enseignement supérieur). Avec ces mêmes idées de rapprochement et d'échanges, l'Académie des sciences, en association avec l'Académie nationale de médecine, et l'OPECST, ont choisi d'engager un nouveau partenariat plus ciblé sur les questions les plus actuelles et les plus complexes en organisant des échanges périodiques de haut niveau permettant une discussion ouverte. Ces échanges prennent la forme de réunions restreintes entre des parlementaires et des académiciens. Les sujets traités sont choisis en commun parmi les questions prioritaires, notamment celles qui sont abordées dans les travaux parlementaires. Les parlementaires développent leurs visions et un ou plusieurs académiciens présentent les points de vue des scientifiques sous une forme concrète et didactique. Le débat est ensuite engagé pour confronter ces points de vue. Une synthèse est réalisée en fin de séance pour rassembler les propositions, les conclusions principales et les pistes de réflexion.

Participants Académie des sciences

Serge ABITEBOUL

Membre de l'Académie des sciences

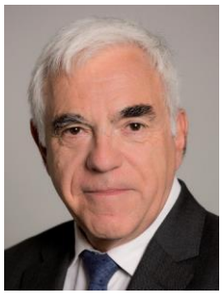
Serge Abiteboul est depuis 2018 Membre du Collège de l'Arcep (Autorité de régulation des communications électroniques et de la Poste). Il est chercheur à l'Inria depuis 1982 et à l'École normale supérieure, Paris. Il a été maître de conférences à l'École polytechnique et professeur invité à Stanford et Oxford University. Il a été détenteur de la Chaire au Collège de France en 2011-12 et de la Chaire Francqui à l'université de Namur 2012-2013. Il a co-fondé la société Xyleme en 2000. Serge Abiteboul a reçu le prix de l'innovation ACM SIGMOD en 1998, le prix EADS de l'Académie française des sciences en 2007 ; le prix Milner de la Royale Society en 2013. Il est devenu membre de l'Académie des sciences en 2008, et membre de l'Académie de l'Europe en 2011. Ses travaux de recherche portent principalement sur les données, la gestion de l'information et des connaissances, en particulier sur le Web. Serge Abiteboul écrit également des romans, des essais, et est éditeur et fondateur du Blog binaire.



Nicholas AYACHE

Membre de l'Académie des sciences

Nicholas Ayache est directeur de recherche chez Inria, où il anime l'équipe de recherche EPIONE, dédiée au patient numérique et à la médecine numérique. Nicholas Ayache est le directeur scientifique du nouvel institut interdisciplinaire d'intelligence artificielle «3IA Côte d'Azur ». Ses recherches actuelles portent sur l'introduction d'algorithmes d'intelligence artificielle pour guider le diagnostic, le pronostic et la prise en charge thérapeutique des patients à partir de leurs images médicales et de l'ensemble des données cliniques, biologiques, et comportementales disponibles. Nicholas Ayache est membre de l'Académie des sciences depuis 2014 et membre libre de l'Académie nationale de chirurgie depuis 2017. Il fut professeur invité au Collège de France en 2013-2014. Nicholas Ayache a publié plus 400 articles scientifiques (40.000+ citations, h-index 101, Google Scholar). Il a co-fondé sept entreprises de haute technologie et fut le directeur scientifique de l'Institut hospitalo-universitaire (IHU) de Strasbourg (2012-2015). Il est co-fondateur et co-rédacteur en chef de la revue scientifique *Medical Image Analysis* (Elsevier, IF 5.36).



Gérard BERRY

Membre de l'Académie des sciences

Ancien élève de l'École polytechnique, ingénieur général du corps des Mines, membre de l'Académie des sciences, de l'Académie des technologies et de l'*Academia Europaea*, Gérard Berry a été chercheur à l'École des mines de Paris et à l'Inria de 1970 à 2000, directeur scientifique de la société Esterel Technologies de 2001 à 2009 puis directeur scientifique Inria et président de la commission d'évaluation de cet institut de 2009 à 2012. Il tient la chaire Informatique et sciences numériques au Collège de France depuis 2012, après y avoir tenu deux chaires annuelles en 2007-2008 et 2009-2010. Sa contribution scientifique concerne quatre sujets principaux : le traitement formel des langages de programmation et leurs relations avec la logique mathématique, la programmation parallèle et temps réel, la conception assistée par ordinateur de circuits intégrés, et la vérification formelle des programmes et circuits. Il est le créateur du langage de programmation Esterel. Ses intérêts concernent également l'enseignement de l'informatique dans le cadre scolaire général, la diffusion de sa compréhension auprès du grand public, et l'interaction avec les décideurs politiques dans les domaines reliés.

Sébastien CANDEL

Ancien président et membre de l'Académie des sciences

Sébastien Candel est professeur des universités émérite à CentraleSupélec (université Paris-Saclay), membre honoraire de l'Institut universitaire de France. Ses recherches concernent la dynamique de la combustion, la structure, la modélisation et la simulation des flammes turbulentes et la combustion cryotechnique avec comme applications la propulsion aéronautique et spatiale et la production d'énergie. Sébastien Candel est membre de l'Académie des technologies, de l'Académie de l'Air et de l'Espace et membre étranger de la *National Academy of Engineering* des États-Unis.

Pierre CORVOL

Président de l'Académie des sciences et membre de l'Académie nationale de médecine

Pierre Corvol, médecin et scientifique, est président de l'Académie des sciences, professeur émérite au Collège de France et administrateur honoraire du Collège de France. Il a consacré ses travaux à l'étude des mécanismes hormonaux de régulation de la pression artérielle. Il a établi le rôle crucial du système rénine angiotensine aldostérone dans le contrôle de la fonction rénale et cardiaque. Les travaux de son équipe ont contribué au développement des traitements couramment utilisés dans l'hypertension artérielle et les maladies cardiovasculaires. Il a mené les premières études sur la génétique de l'hypertension artérielle humaine et a récemment travaillé sur le rôle des peptides vasoactifs dans les mécanismes de l'angiogénèse.

Pascale COSSART

Secrétaire perpétuel de l'Académie des sciences

Professeur à l'Institut Pasteur, Pascale Cossart, microbiologiste, a axé ses recherches sur l'étude des mécanismes moléculaires et cellulaires impliqués dans les infections bactériennes en utilisant comme modèle la bactérie *Listeria monocytogenes*. Pascale Cossart a été pionnière de cette discipline qu'elle a baptisée « microbiologie cellulaire ». Elle a mis en évidence de nombreuses stratégies utilisées par les bactéries lors d'une infection. Ses travaux ont permis l'élaboration de nouveaux concepts en biologie des infections, biologie cellulaire, épigénétique et microbiologie fondamentale et ont été reconnus par plusieurs prix internationaux. Pascale Cossart est membre de la Leopoldina ; de la *National Academy of Sciences* (USA), de la *National Academy of Medicine* (USA) et de la *Royal Society* (UK).

Patrick FLANDRIN

Vice-président de l'Académie des sciences

Patrick Flandrin est directeur de recherche CNRS à l'École normale supérieure de Lyon. Les travaux de Patrick Flandrin portent sur la représentation, l'analyse et le traitement des signaux, avec une attention toute particulière pour les situations non stationnaires et multi-échelles. Il a contribué à l'élaboration de méthodes "temps-fréquence" et "temps-échelle" dont les applications multiples concernent aussi bien des phénomènes naturels (allant de la physique au génie biomédical) que des réalisations technologiques (allant de la mécanique au trafic internet).

Etienne GHYS

Secrétaire perpétuel de l'Académie des sciences

Étienne Ghys est mathématicien. Directeur de recherche CNRS de classe exceptionnelle, il a contribué à la création et au développement du laboratoire de mathématiques de l'ENS de Lyon. Ses travaux scientifiques portent sur la géométrie, la topologie et les systèmes dynamiques. On lui doit par exemple des résultats permettant de mieux comprendre la topologie du fameux papillon de Lorenz, paradigme de la théorie du chaos. Depuis quelques années, il s'est investi dans plusieurs actions de diffusion, comme la réalisation de films mathématiques ou encore la fondation d'une revue en ligne destinée au public général. Cela lui a valu le prix Clay pour la dissémination des mathématiques. Il porte un intérêt tout particulier aux questions d'éducation.

Olivier PIRONNEAU

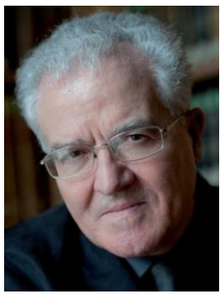
Vice-président délégué aux relations internationales de l'Académie des sciences

Olivier Pironneau est un ancien élève de l'École polytechnique et de UC Berkeley (PhD 1971 en EECS). Après un postdoc avec Sir James Lighthill à Cambridge UK, il soutient une thèse d'état en 1975. D'abord chercheur à l'INRIA avec Jacques-Louis Lions, il est nommé professeur d'informatique à Paris XIII en 1978 puis à Paris VI en mathématiques appliquées en 1985. Auteur de plus de 300 publications et de 5 livres sur la simulation et le contrôle des équations aux dérivées partielles sur ordinateur pour l'aéronautique, l'électromagnétisme, la finance quantitative et d'autres problèmes à la frontière des mathématiques et de l'informatique, il a été membre de la Commission nationale d'évaluation des recherches et études relatives à la gestion des matières et des déchets radioactifs, et membres des conseils de INRIA, UPMC, GENCI, CINES, etc. Membre senior de l'Institut universitaire de France de 1993 à 2003, il a été élu membre de l'Académie des sciences en 2002. Il est actuellement professeur émérite à Sorbonne-université et vice-président délégué aux relations internationales de l'Académie des sciences.

Didier ROUX

Délégué à l'information et à la communication de l'Académie des sciences

Didier Roux est né en 1955, ancien élève de l'École normale supérieure de Saint-Cloud, membre du Centre national de la recherche scientifique (CNRS) de 1980 à 2005. Il est lauréat de nombreux prix et distinctions. Il est titulaire de la médaille d'argent du CNRS. Il crée deux *start-up* en 1994 et 1998, il est directeur scientifique adjoint de Rhône-Poulenc puis de Rhodia entre 1997 et 2005. Il occupe entre 2007 et 2017 le poste de directeur de la R&D et de l'Innovation du Groupe Saint-Gobain. Il est membre de l'Académie des sciences et de l'Académie des technologies. Il a été professeur au Collège de France (chaire annuelle 2016-2017 « Innovation technologique Liliane Bettencourt »). Il est président d'Unitec et vice-président de la fondation *La Main à la Pâte*.



Eric WESTHOF

Délégué à l'éducation et à la formation de l'Académie des sciences

Eric Westhof est professeur émérite de biochimie structurale à l'université de Strasbourg. Il a été directeur de l'Institut de biologie moléculaire et cellulaire du CNRS (IBMC) à Strasbourg et de l'unité « Architecture et réactivité de l'ARN » pendant plus de dix ans. Il a été vice-président recherche et formation doctorale d'abord de l'université Louis Pasteur (2007-2008) puis de l'université de Strasbourg (2009-2012). Il a été président de la RNA Society (2005) et de la Société française de biochimie et biologie moléculaire (2004-2009). Spécialiste de biochimie structurale, Éric Westhof a réalisé des travaux concernant la dynamique et les fonctions catalytiques des acides nucléiques et plus particulièrement de l'ARN, par des approches cristallographiques et bioinformatiques. Ces travaux ont permis de dégager de nombreuses règles du repliement et de l'auto-assemblage de l'ARN.

Participants Académie nationale de médecine

Jean François ALLILAIRE

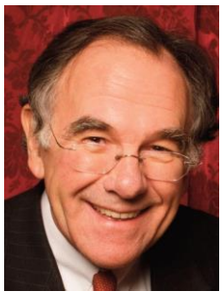
Secrétaire perpétuel de l'Académie nationale de médecine

Jean François Allilaire est docteur en médecine, spécialiste en psychiatrie. Il a été formé à la faculté des sciences puis à la faculté de médecine Pitié-Salpêtrière de l'université Paris VI. Ancien interne des hôpitaux de Paris et des hôpitaux psychiatriques d'Ile-de-France, chef de clinique de la faculté, puis professeur d'université, il a dirigé le service de psychiatrie de l'hôpital de la Salpêtrière intégré à l'UFR de neurosciences Charcot et au pôle des maladies du système nerveux du CHU Pitié-Salpêtrière. Chercheur-clinicien au sein de l'INSERM-U302 « Psychopathologie et pharmacologie des comportements » puis à l'unité mixte de recherche CNRS-université 7593 « Vulnérabilité, adaptation et psychopathologie », ses travaux de recherche concernent les mécanismes et les traitements des maladies psychiatriques dans les domaines de l'anxiété, la dépression et la bipolarité. Il est élu à l'Académie nationale de médecine en 2004.

Raymond ARDAILLOU

Secrétaire perpétuel honoraire de l'Académie nationale de médecine

Raymond Ardaillou s'est essentiellement consacré à la physiologie et à la physiopathologie rénales ainsi qu'au contrôle hormonal des fonctions rénales et de l'équilibre hydro-électrolytique. Il a travaillé dans le domaine de la physiologie du glomérule, montrant qu'il ne s'agissait pas simplement d'un filtre passif, mais d'un système contrôlé par des hormones et, aussi, du lieu de synthèse de cytokines et facteurs de croissance. Il a décrit les récepteurs glomérulaires de l'angiotensine II et les a localisés dans le mésangium de même que les récepteurs des peptides natriurétiques. Il démontra aussi le rôle des cellules propres du glomérule dans la progression des glomérulonéphrites expérimentales à côté de celui déjà connu des leucocytes et macrophages. Toujours soucieux d'associer des travaux d'investigation clinique aux études purement expérimentales, il a, en particulier, montré que l'équilibre de la balance du sodium dans l'insuffisance rénale chronique dépendait directement de la synthèse accrue du facteur auriculaire natriurétique dans cette maladie.



Emmanuel Alain CABANIS

Président de l'Académie nationale de médecine

Professeur Emmanuel Alain Cabanis, M.D. (1970), Ph.D. Paris 5 (1983) est professeur des universités-praticien hospitalier U. P.M.Curie-Paris 6 (1986-2008), neuroradiologue, chef du service de neuro-imagerie, président CME (2 mandats), au Centre hospitalier national d'ophtalmologie des XV-XX (1973-2008, ministère de la Santé), expert Cour de Cassation. Il contribue au second scanner RX français puis concoit et dirige la 1ère évaluation clinique de l'IRM (1983-1987). Il est chargé de mission auprès du Premier Ministre en 2008. Il totalise 300 000 patients examinés ; est l'auteur de 450 publications, de 120 participations à ouvrages, plus de 200 thèses, 75 rapports, il a initié et guidé jusqu'à l'inauguration, l'Institut de la vision, 437 publications réf, 75 rapports, 38 interventions à l'Académie nationale de médecine, il est Officier dans l'Ordre national de la Légion d'honneur, chevalier dans l'Ordre national du mérite, médaille du service de santé des Armées, président 2019 de l'Académie nationale de médecine.

Daniel COUTURIER

Secrétaire perpétuel honoraire de l'Académie nationale de médecine

Professeur honoraire à l'université René Descartes (Paris) et ancien chef du service d'hépatogastroentérologie de l'hôpital Cochin (Paris).
Il est président honoraire de la Commission médicale d'établissement AH-HP.
Ses recherches ont été consacrées à la physiopathologie-pharmacologie de la motricité digestive, à la cancérogenèse des tumeurs de l'intestin et à la prédisposition familiale aux tumeurs de l'appareil digestif.

Antoine DURRLEMAN

Membre de l'Académie nationale de médecine

Ancien directeur général de l'Assistance publique - Hôpitaux de Paris, ancien directeur de l'Ecole nationale d'administration, membre de l'Académie nationale de médecine, Antoine Durrleman est président de chambre à la Cour des comptes dont il a présidé jusque récemment la chambre sociale. A ce titre, il a notamment piloté les enquêtes régulièrement consacrées par la Cour à la sécurité des systèmes d'information de la sécurité sociale, et tout particulièrement du Système national interrégimes de l'assurance maladie (SNIIRAM), qui constitue une des bases de données personnelles médico-administratives parmi les plus riches et les plus importantes au monde et qui pose des problématiques de confidentialité particulièrement sensibles. Il s'est également intéressé aux questions posées à cet égard par le développement des téléservices en santé, notamment du dossier médical partagé.

Patrick NETTER

Membre de l'Académie nationale de médecine

Patrick Netter, médecin et scientifique, PU-PH de pharmacologie à l'université de Lorraine a consacré ses travaux de recherche aux mécanismes cellulaires et moléculaires des pathologies articulaires.
Directeur de l'UMR "Physiopathologie et Pharmacologie articulaire CNRS/Université de lorraine de 1997 à 2008, Doyen de la Faculté de Médecine de Nancy de 2003 à 2008, il a été Directeur de l'Institut des Sciences biologiques du CNRS de 2008 à 2013, Vice-Président d'AVIESAN (Alliance pour les Sciences de la vie et la Santé) de 2010 à 2013, Président d'IBISA (infrastructures en biologie, Santé et Agronomie) de 2010 à 2012, Conseiller Europe ERC du Président du CNRS de 2013 à 2016,
Membre de l'Académie nationale de Médecine depuis 2004, du Conseil de l'AERES (Agence d'évaluation de la recherche et de l'enseignement supérieur) de 2007 à 2011, du Conseil scientifique de l'ATIH (agence technique de l'information sur l'hospitalisation (2016-) et de l'OPECST (Office parlementaire d'évaluation des choix scientifiques et technologiques (2016-), il a été élu en 2017 Président de la Division des sciences biologiques et pharmaceutiques de l'Académie nationale de Médecine.
Conseiller Expert à la Cour des Comptes (4e chambre) (2014-), il participe à des expertises et des évaluations de politique publique.

Bernard NORDLINGER

Membre de l'Académie nationale de médecine

Bernard Nordlinger est chirurgien, PUPH spécialiste des cancers digestifs, et a été chef de pôle, chef du service de chirurgie digestive et oncologique de l'Hôpital Ambroise Paré (APHP). Il a été membre de la Commission médicale d'établissement (CME) de l'APHP, du directoire de l'APHP et a Présidé le comité cancer de l'APHP. Au plan de la recherche, il a dirigé une équipe Inserm, il a présidé le groupe digestif de l'Organisation européenne de recherche et de traitement des cancers (EORTC) et de l'intergroupe européen PETACC. Il a organisé et coordonné de nombreux essais cliniques nationaux et internationaux, publiés dans des revues internationales. L'essai EORTC 40983 (T*he Lancet*) a établi le standard international de traitement des métastases hépatiques des cancers du côlon résécables par la chirurgie. Il a monté avec Cédric Villani le groupe de travail « Santé et Intelligence Artificielle » de l'Académie nationale de médecine et de l'Académie des sciences, et dirigé la publication de l'ouvrage homonyme en octobre 2018.

Patrice TRAN BA HUY

Membre de l'Académie nationale de médecine

Patrice Tran Ba Huy est professeur d'oto-rhino-laryngologie à la faculté de médecine Lariboisière-St-Louis - université Paris 7. Ancien chef de service ORL à l'Hôpital Lariboisière 1995-2010. Ancien président de la Société française d'ORL et de chirurgie cervico-faciale.

Participants invités

Gildas AVOINE

Professeur de cryptographie à l'INSA Rennes

Gildas Avoine effectue ses recherches au sein du laboratoire IRISA (Unité mixte de recherche du CNRS). Il est également membre de l'Institut universitaire de France depuis 2014. Il a fondé et il dirige en collaboration avec Pierre-Alain Fouque le groupe de recherche en sécurité et cryptographie embarquées (EMSEC) de l'IRISA qui regroupe aujourd'hui 35 chercheurs. Gildas Avoine est également le directeur du Groupement de recherche (GDR) du CNRS en sécurité informatique. Ce réseau scientifique regroupe plus de 1000 chercheurs académiques et industriels. Il est également le président du conseil scientifique de l'ANSSI. Enfin, de 2014 à 2019, Gildas Avoine a été le directeur de l'Action COST Cryptacus du programme européen H2020. Auparavant, Gildas Avoine a été chercheur postdoctoral au MIT (États-Unis) et chercheur à l'EPFL (Suisse) où il a obtenu un doctorat ès sciences dans le domaine de la cryptographie. Il a étudié les mathématiques, puis l'informatique, à l'Université de Caen.

Bernard BARBIER

Membre de l'Académie des technologies

Bernard Barbier est CEO de BBCYBER, société de conseil.
Depuis 2015, il met en place, pour le groupe CAPGEMINI, un programme de transformation interne, CySIP (*Cyber Security and Information Protection*).
Expert en cryptographie, cybersécurité et cyberdéfense, il a dirigé tout au long de sa carrière des projets à forts enjeux technologiques. D'abord au Commissariat à l'énergie atomique, où, au sein de la direction des applications militaires, il est chargé du déploiement du programme d'équipement des super - calculateurs nécessaires aux calculs de simulation de l'arme nucléaire française. Bernard barbier a travaillé dans le domaine des nanotechnologies, au sein du LETI à Grenoble, qu'il a dirigé de 2003 à 2006. Il a participé très activement à l'élaboration et à la mise en place du pôle MINATEC. Puis à la direction générale de la sécurité extérieure (DGSE), dont il a notamment assuré la direction technique en charge des interceptions des communications électroniques et des opérations cyber (2006 à 2013).

Véronique CORTIER

Directrice de recherche CNRS au Loria (Nancy)

Véronique Cortier est titulaire d'un doctorat en informatique de l'École normale supérieure de Cachan, dont elle est ancienne élève. Ses travaux portent sur l'étude de la sécurité des systèmes informatiques à l'aide de concepts mathématiques et informatiques comme la logique, la réécriture ou la démonstration automatique. Elle s'intéresse en particulier aux protocoles de sécurité comme le paiement en ligne, les communications sécurisées ou le vote électronique. Elle est l'auteur de plus de 80 publications, et membre de comités éditoriaux de quatre journaux. En 2015, elle a obtenu le prix INRIA - Académie des sciences du jeune chercheur.

Bruno JARRY

Président honoraire de l'Académie des technologies

Après une carrière universitaire – il a été chercheur au CNRS puis professeur de génétique à l'Université Louis Pasteur, fondateur et premier directeur de l'Ecole supérieure de Biotechnologie de Strasbourg, Bruno JARRY est nommé en 1988 vice-président R&D d'ORSAN, la filiale biotechnologique du Groupe Lafarge-Coppée. Il sera à partir de 1995 Directeur R&D du Groupe amidonnier belge Amylum, puis, à partir de 2000, Directeur scientifique du Groupe sucrier américano-britannique Tate & Lyle. De 2004 à 2007 il est conseiller du Président de l'Institut Curie et de 2007 à 2013, chargé de mission au cabinet du Premier Ministre pour les questions liées aux biocarburants et à la chimie verte. Au cours de sa carrière il a participé à la création de 3 start-ups du domaine des biotechnologies. Bruno Jarry est administrateur de l'Institut Français du pétrole et des énergies nouvelles et de plusieurs entreprises du domaine de la biotechnologie industrielle. Il est membre de l'Académie des technologies depuis 2003 et en a été le vice-président puis le président (2017-2018).

Jean-Yves MARION

Directeur de recherche, CNRS

Jean-Yves Marion est directeur du Loria, laboratoire lorrain de recherche en informatique et ses applications, commun au CNRS, à l'Inria et à l'université de Lorraine, depuis 2013 (www.loria.fr #Loria_lab). Jean-Yves Marion a soutenu sa thèse d'informatique à l'université Paris Diderot en 1991. Il a effectué deux ans de post-doctorat à l'université d'Indiana, Etats-Unis. Professeur à l'université de Lorraine depuis 2002, il enseigne à l'École nationale supérieure des mines de Nancy (ENSMN). Ses recherches sur la sécurité informatique ont débuté en 2007 et il a été un des premiers à travailler sur les codes malveillants (malwares, virus, botnet, ransomware ...) dans le monde académique français. Dès 2010, il a créé le laboratoire de haute sécurité (LHS) au Loria. Aujourd'hui, on trouve d'autres LHS dans les universités françaises. Il est l'auteur d'environ une centaine de publications académiques et il présente ses travaux en Europe, en Amérique du Nord et au Japon. Ses travaux sont reconnus par toute la communauté scientifique, par le monde associatif et professionnel. Il est membre senior de l'Institut universitaire de France (http://www.iufrance.fr/), membre du CA du GDR CNRS Sécurité, membre du CA de CecyF et de l'AFSIN et du CS de l'ANSSI. Avec ses travaux sur l'analyse morphologique de codes malveillants, il a fondé la start-up cyber-detect. Il a été invité sur France Culture, France Inter (tête au carré) et sur France 2 (Envoyé spécial) et fait partie des 100 Français qui comptent suivant l'Usine nouvelle.

Ludovic MÉ

Enseignant-chercheur, INRIA

Ludovic Mé est enseignant-chercheur à Supélec de 1988 à 2014, puis à CentraleSupélec de 2015 à 2017, il est depuis début 2018 en détachement chez Inria où il est adjoint au directeur général délégué à la sciences, en charge du domaine de la cybersécurité. Son domaine de recherche de prédilection est la sécurité réactive (détection d'intrusions, corrélation d'alertes). Il s'est néanmoins également intéressé à la sécurité des réseaux auto-organisés et à la virologie informatique. Dans ces domaines, il est auteur ou co-auteur de plus de soixante-dix communications nationales et internationales. Il a encadré à ce jour 15 doctorants et a par ailleurs été directeur de thèse de 14 autres étudiants. Ludovic Mé est ingénieur Supélec (1987), docteur de l'université de Rennes 1 (1994) et titulaire d'une HDR de cette même université (2003).

David NACCACHE

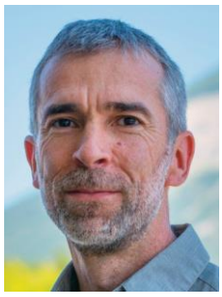
Professeur à l'École normale supérieure

David Naccache, est un cryptologue français, actuellement professeur à l'École normale supérieure où il dirige l'équipe de sécurité de l'information. De 1993 à 2005 il dirige le département de la recherche et innovation de la société Gemplus. En 2004, il soutient son habilitation à diriger des recherches à l'université Paris 7. Il rejoint en 2005 l'université Paris 2 en tant que professeur, et l'équipe de recherche en cryptographie de l'École normale supérieure. En 2009 il est nommé à l'Observatoire de la sécurité des cartes de paiement où il est actuellement personnalité qualifiée. Pendant cette période il est également professeur invité à Royal Holloway. Les travaux de D. Naccache portent majoritairement sur la cryptographie à clé publique (notamment les signatures numériques basées sur RSA), la sécurité informatique, et l'expertise judiciaire. À ce titre il intervient pour la cour de cassation, la cour pénale internationale, et la cour d'appel de Paris. D. Naccache est membre du comité éditorial du journal *Cryptologia* et du magazine *IEEE Security and Privacy*. Il est l'auteur de 200 publications scientifiques et plus de 100 familles de brevets et le directeur (ou co-directeur) de plus de 30 thèses de doctorat. Il est membre de l'IUF et professeur titulaire de la chaire « Droit et expertise judiciaire en informatique » à l'Ecole des officiers de la Gendarmerie nationale.

Guillaume POUPARD

Directeur général de l'Agence nationale de sécurité des systèmes d'information

Guillaume Poupard est ancien élève de l'École polytechnique, promotion X92. Ingénieur de l'armement en option recherche, il est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques Stern à l'École normale supérieure de Paris. Il est également diplômé de l'enseignement supérieur en psychologie. Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la direction centrale de la sécurité des systèmes d'information (DCSSI). Il rejoint en 2006 le ministère de la Défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense. En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la direction générale de l'armement (DGA). Le 27 mars 2014, il est nommé directeur général de l'Agence nationale de sécurité des systèmes d'information.



Vincent ROCA

Chercheur Inria

Après un doctorat de Grenoble INP en 1996 puis avoir rejoint l'université Paris 6 en qualité maître de Conférences en 1997, Vincent Roca est Chercheur Inria depuis 2000. Spécialiste réseaux, auteur d'une dizaine de standards Internet, il co-dirige depuis 2017 un groupe de recherche de l'IETF, l'organisme international en charge de l'évolution d'Internet. Il est membre depuis 2012 de l'équipe de recherches Privatics de l'Inria où il s'intéresse à différents aspects liés au respect de la vie privée, notamment les risques associés à l'usage de nos smartphones ainsi que de l'Internet des Objets qui envahit progressivement notre quotidien. Il est l'un des créateurs du très populaire cours en ligne « Protection de la vie privée dans le monde numérique » de la plateforme FUN, qui en trois sessions a déjà rassemblé plus de 28 000 participants. En parallèle, ses importantes actions de transfert industriel lui ont valu d'être lauréat du 3e prix de la recherche appliquée décerné par la Fédération des industries électriques, électroniques et communications (FIEEC) en 2014. Il est enfin l'un des quatre auteurs du Livre Blanc Inria sur la Cybersécurité, publié début 2019, qui brosse un large panorama des activités de recherche académique en sécurité informatique, il est membre du "Security Directorate" de l'IETF et membre du comité d'éthique Inria.

Daniel VERWAERDE

Président de TERATEC depuis septembre 2018

Daniel VERWAERDE est spécialiste en modélisation numérique, Daniel Verwaerde est un expert mondial en calcul de haute performance, proche des applications civiles et militaires. Il est un spécialiste du développement des clusters de technologies, avec des réalisations pratiques autour des centres du CEA : Calcul de haute performance autour de bruyères Le Chatel, Route des lasers à Bordeaux, Microélectronique à Grenoble, Energies alternatives au Ripault près de Tours. Il entre au CEA en 1978 au Département de mathématiques appliquées dont il assure la direction à partir de 1991. En 1996, il devient directeur du programme Simulation, destiné à garantir la pérennité de la dissuasion nucléaire française après l'arrêt définitif des essais nucléaires. Il dirige ensuite le Centre CEA-DAM Ile-de France (2000 – 2004), les programmes Armes et Simulation (2004 – 2007), puis les applications militaires CEA-DAM Ile-de-France (2007 – 2015) avant de devenir administrateur général (2015 – 2018).

Philippe VIGOUROUX

Directeur général du Centre hospitalier universitaire de Bordeaux

Philippe Vigouroux est titulaire d'une maîtrise de droit des affaires et diplômé de l'Ecole nationale de la santé publique (ENSP, aujourd'hui Ecole des hautes études en santé publique -EHESP), après avoir été notamment directeur général des CHU de Nancy (2008 à 2013) et de Limoges (2004 à 2008) et directeur général adjoint du CHU de Bordeaux (1997 à 2004). Philippe Vigouroux est également vice-président de la Conférence des directeurs généraux de CHU, chargé des questions de recherche et, à ce titre, membre des Conseils d'administration de l'Inserm, de l'Alliance pour les sciences de la vie et de la santé (AVIESAN), vice-président du Comité national de coordination de la recherche (CNCR) et membre du Conseil d'administration de la Fédération hospitalière de France.

Participants Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST)

Députés

Émilie CARIOU

Élue le 18 juin 2017 - Meuse (2e circonscription)
Née le 14 octobre 1971 à Verdun (Meuse)

Fonctionnaire de catégorie A, essentiellement au ministère de l'Économie et des Finances, membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, référente parmi les membres députés sur les questions du nucléaire, du traitement et de la gestion des déchets nucléaires. Désignée co-rapporteure pour l'Office sur l'évaluation du plan national de gestion des matières et déchets radioactifs (PNGMBR) 2019-2021. Membre titulaire du conseil d'administration de l'Agence nationale pour la gestion des déchets radioactifs (ANDRA) jusqu'à juin 2019. Membre titulaire du Comité local d'information et de suivi du laboratoire souterrain de Bure. Vice-présidente de la commission des finances, de l'économie générale et du contrôle budgétaire. Membre du groupe d'études « économie numérique de la donnée, de la connaissance et de l'intelligence artificielle ».

Jean-François ELIAOU

Élu le 18 juin 2017 - Hérault (4e circonscription)
Né le 13 août 1956 à Nice (Alpes-Maritimes)

Professeur à la faculté de médecine de Montpellier, ancien interne des hôpitaux et médecin chef de service au CHU de Montpellier. Pédiatre de formation, il s'est orienté vers l'immunologie. Il réalise ses activités de recherche sur l'immunité et le cancer à l'Institut de Recherche en cancérologie de Montpellier. Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, référent parmi les membres députés sur les questions médicales, de biotechnologies, de bioéthique, de valorisation dans le domaine des sciences du vivant. Co-rapporteur sur l'évaluation de l'application de la loi n° 2004-800 du 6 août 2004 et de la loi n° 2011-814 du 7 juillet 2011 relatives à la bioéthique. Membre de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République. Secrétaire de la mission d'information de la Conférence des présidents sur la révision de la loi relative à la bioéthique. Membre de la mission d'information sur la gestion des événements climatiques majeurs dans les zones littorales de l'hexagone et des Outre-mer. Vice-président du groupe d'études « Santé et numérique », membre du groupe d'études « Fin de vie ». Rapporteur du groupe de travail sur les moyens de contrôle et d'évaluation, mis en place par le Président de l'Assemblée nationale François de Rugy. Membre du groupe de travail sur les droits et libertés constitutionnels à l'ère numérique.

Claude de GANAY

Élu le 20 juin 2012 - Réélu le 18 juin 2017 – Loiret (3e circonscription)
Né le 5 septembre 1953 à Paris

Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques depuis 2012. Co-rapporteur pour l'Office du rapport « Pour une intelligence artificielle maîtrisée, utile et démystifiée », 15 mars 2017. Membre suppléant du Conseil national de l'enseignement supérieur et de la recherche. Membre de la Commission de la défense nationale et des forces armées. Vice-Président des groupes d'études « Forêt, bois, nouveaux usages et industrie du bois » et « Économie numérique de la donnée, de la connaissance et de l'intelligence artificielle ». Secrétaire du groupe d'étude « Autisme ». Membre des groupes d'études « Modernisation des activités agricoles et structuration des filières » et « Secteur aéronautique et spatial ».

Pierre HENRIET

Élu le 18 juin 2017 - Vendée (5e circonscription)
Né le 26 novembre 1991 à Fontenay-le-Comte (Vendée)

Professeur du secondaire et technique, doctorant en philosophie des sciences à l'université de Nantes depuis 2015. Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, référent parmi les membres députés sur les questions de la culture scientifique, technique et industrielle. Membre titulaire du Conseil national de la culture scientifique, technique et industrielle. Membre titulaire du Conseil national de l'enseignement supérieur et de la recherche artistiques et culturels. Co-rapporteur du rapport d'information de l'Office « Recherche, sciences et techniques : perspectives technologiques ouvertes par la 5G ». Désigné co-rapporteur pour l'Office sur l'intégrité scientifique et les politiques de publications scientifiques. Membre de la commission des affaires culturelles et de l'éducation. Membre du groupe d'études « internet et société numérique ».

Cédric VILLANI

Élu le 18 juin 2017 - Essonne (5e circonscription)
Né le 5 octobre 1973 à Brive (Corrèze)

Professeur de l'université de Lyon en mathématiques, titulaire 2010 de la médaille Fields et lauréat 2014 du prix Doob, membre de l'Académie des sciences et de l'Académie pontificale des Sciences. Président de l'Office parlementaire d'évaluation des choix scientifiques et technologiques du 18/07/2017 au 09/11/2017, puis Premier Vice-Président de l'Office depuis. Rapporteur des notes scientifiques : - « Le transport à hypergrande vitesse sous vide (Hyperloop) » (note n° 5 - juillet 2018) - « Les grands accélérateurs de particules » (note n° 12 - mars 2019) - « Les technologies quantiques » (note n° 13 - avril 2019). Rapporteur sur les rapports d'information (issus d'auditions publiques) : - Quelle prise en compte de l'hypersensibilité électromagnétique ? - Enjeux des compteurs communicants - Algorithmes au service de l'action publique : le cas du portail admission post-bac - Expérimentation animale - Zones restrictives de recherche - Intelligence artificielle et données de santé - Sciences et technologies en appui à la restauration de monuments historiques : le cas de Notre-Dame de Paris. Membre de la commission des affaires culturelles et de l'éducation. Membre des groupes d'études « Autisme », « Condition animale » et « Handicap Inclusion ». Auteur de deux rapports au gouvernement : - « 21 mesures pour l'enseignement des mathématiques », avec Charles Torossian, février 2018 - « Donner un sens à l'intelligence artificielle », mars 2018. Co-rapporteur, en tant que parlementaire en mission pour le Gouvernement, du groupe de travail sur la recherche sur projets, le financement compétitif et le financement des laboratoires, pour la préparation du projet de loi de programmation de la recherche.

Sénateurs

Jérôme BIGNON

Sénateur de la Somme depuis 2014
Né le 1er janvier 1949
Avocat

Député de la Somme de 1993 à 1997 et de 2002 à 2012. Conseiller général de la Somme de 1980 à 2014. Conseiller régional de Picardie de 1986 à 1993. Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Rapporteur d'une note scientifique de l'Office sur les pertes de biodiversité. Membre de la commission de l'aménagement du territoire et du développement durable. Rapporteur de la loi pour la reconquête de la biodiversité, de la nature et des paysages. Rapport d'information sur la mise en œuvre par la France des objectifs de développement durable. Membre du Conseil d'administration de l'Agence française de la biodiversité. Membre du Conseil d'administration du Conservatoire de l'espace littoral et des rivages lacustres. Membre du Conseil consultatif des terres australes et antarctiques françaises. Membre du Conseil de surveillance de la société du canal Seine-Nord Europe. Chargé d'une mission temporaire auprès du ministre d'État, ministre de la transition écologique et solidaire sur la préservation des zones humides (rapport publié en janvier 2019).

Laure DARCOS

Élue sénatrice de l'Essonne le 24 septembre 2017
Née le 27 novembre 1970
Conseillère départementale de l'Essonne (canton : Gif-sur-Yvette)

Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Membre de la commission de la culture, de l'éducation et de la communication – Rapporteur du budget de la recherche. Vice-Présidente de la délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes. Membre des groupes d'études Agriculture et alimentation, Cancer, et Numérique
Membre du Conseil d'administration du Centre national du livre.

Véronique GUILLOTIN

Élue sénatrice de Meurthe-et-Moselle le 24 septembre 2017
Née le 3 novembre 1962
Médecin
Conseillère régionale de Grand Est

Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Vice-Présidente de la commission des affaires européennes. Membre de la commission des affaires sociales. Secrétaire de la mission d'évaluation et de contrôle de la sécurité sociale. Membre du groupe d'études Cancer. Membre de la mission commune d'information sur les politiques publiques de prévention, de détection, d'organisation des signalements et de répression des infractions sexuelles susceptibles d'être commises par des personnes en contact avec des mineurs dans le cadre de l'exercice de leur métier ou de leurs fonctions. Membre du Conseil d'administration de l'Agence nationale de santé publique. Auteur d'un rapport sur les médicaments innovants, au nom de la mission d'évaluation et de contrôle de la sécurité sociale de la commission des affaires sociales.

Gérard LONGUET

Sénateur de la Meuse depuis 2001 (réélu en 2011 et 2017)
Né le 24 février 1946

Ministre chargé des Postes et des Télécommunications (1986-1988). Ministre de l'Industrie, des Postes et des Télécommunications et du Commerce extérieur (1993-1994). Ministre de la Défense et des Anciens combattants (2011-2012). Député de la Meuse (1978-1981 et 1988-1993). Député européen (1984-1986). Président du conseil régional de Lorraine (1992-2004). Conseiller général de la Meuse (1979-1992 et 1998-2001). Président de l'Office parlementaire d'évaluation des choix scientifiques et technologiques depuis le 9 novembre 2017. Membre de la commission des finances – Rapporteur spécial des crédits de l'Enseignement scolaire. Président du groupe interparlementaire France-Russie. Rapporteur de la commission d'enquête du Sénat sur la souveraineté numérique.

Stéphane PIEDNOIR

Élu sénateur de Maine-et-Loire le 24 septembre 2017
Né le 25 février 1970
Professeur
Conseiller municipal de Montreuil-Juigné
Vice-Président de la communauté urbaine Angers Loire métropole

Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Co-rapporteur de l'étude sur « Les scénarios technologiques permettant d'atteindre l'objectif d'un arrêt de la commercialisation des véhicules thermiques en 2040 ». Membre de la commission de la culture, de l'éducation et de la communication. Membre des groupes d'études Énergie, Forêt et filière bois, et Pratiques sportives et grands événements sportifs. Membre de la commission d'enquête sur la souveraineté numérique. Secrétaire de la mission commune d'information sur les politiques publiques de prévention, de détection, d'organisation des signalements et de répression des infractions sexuelles susceptibles d'être commises par des personnes en contact avec des mineurs dans le cadre de l'exercice de leur métier ou de leurs fonctions. Membre du Conseil d'administration de l'Institut de radioprotection et de sûreté nucléaire.

Angèle PRÉVILLE

Elue sénatrice du Lot le 24 septembre 2017
Née le 23 novembre 1955
Professeur de physique-chimie

Membre de l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Rapporteure d'une note scientifique sur le stockage de l'électricité. Rapporteure d'une étude sur la pollution plastique. Membre de la commission de l'aménagement du territoire et du développement durable. Membre des groupes d'études Agriculture et alimentation et Énergie. Présidente déléguée du groupe interparlementaire France-Europe du Nord (Suède). Membre de la mission d'information sur le développement de l'herboristerie et des plantes médicinales.

Bruno SIDO

Sénateur de la Haute-Marne depuis 2001 (réélu en 2011 et 2017)
Né le 19 février 1951
Ingénieur agronome, exploitant agricole

Conseiller général (puis départemental) de la Haute-Marne depuis 1994, président du Conseil général (puis départemental) de la Haute-Marne de 1998 à 2017. Vice-président du conseil régional de Champagne-Ardenne de 1998 à 2001. Président de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) de 2012 à 2014 et premier vice-président de 2011 à 2012 et de 2014 à 2017. Très nombreux rapports parlementaires pour l'OPECST, notamment sur l'évaluation de la stratégie nationale de recherche et de la recherche en énergie, sur les équipements sous pression nucléaires, sur le brouillage des communications électroniques, sur les maladies à transmission vectorielle, sur les ressources génétiques végétales, sur la politique spatiale européenne, sur l'innovation et le changement climatique, sur la sécurité numérique, sur la filière semencière française, sur les médicaments biosimilaires, sur la recherche environnementale, sur le tournant énergétique allemand, sur les drones et la sûreté des installations nucléaires, sur la transition énergétique, sur les progrès de la génétique, etc.
Co-rapporteur de l'évaluation du plan national de gestion des matières et déchets radioactifs (PNGMDR) 2019-2021. Membre de la commission des affaires étrangères, de la défense et des forces armées. Membre du groupe d'études Énergie. Membre de la commission consultative de suivi des conséquences des essais nucléaires. Membre du Conseil d'administration de l'Agence nationale pour la gestion des déchets radioactifs (ANDRA).

GÉNÉRALITÉS SUR LES ATTAQUES

La sécurité informatique est un problème dont l'importance croît rapidement par suite d'une floraison massive de nouvelles attaques à grande échelle. Le *World Economic Forum* vient de classer les dangers économiques majeurs : en 1e et 2e positions se trouvent les catastrophes climatiques, en 3e les cyberattaques sur les systèmes informatisés (réseaux électriques, transports, industries, hôpitaux, etc.) et en 4e celles sur les données (personnelles, bancaires, médicales, etc.). Il faut noter que les attaques sur les systèmes, beaucoup moins médiatisées que celles sur les données, sont vues comme encore plus dangereuses.

Il y a deux grandes catégories d'attaques contre les systèmes et données : d'une part, celles massives et non ciblées, qui visent à atteindre un grand nombre de personnes ou de systèmes sans s'intéresser a priori à qui ils sont, comme les rançongiciels Wannacry ou NotPetya qui se sont répandus très vite dans le monde entier en touchant beaucoup de systèmes d'information, d'hôpitaux et de systèmes industriels ; d'autre part, les attaques ciblées qui visent une ou quelques personnes ou entreprises : celles-là sont moins nombreuses et plus difficiles à mettre en œuvre, mais également plus difficiles à détecter et potentiellement d'impact très élevé. Des exemples caractéristiques d'attaques ciblées sont les attaques dévastatrices sur Sony Pictures et TV5 Monde en 2015, ou sur les serveurs du parti Démocrate aux USA lors des dernières élections. En termes de défense, les attaques massives sont généralement plus faciles à détecter que les attaques ciblées, mais ça pourrait ne pas durer. Toutes ces attaques, souvent automatisées, peuvent venir d'individus, d'organisations criminelles (de plus en plus), et même d'États. La surface d'attaque va aussi s'étendre considérablement avec la connexion généralisée des moyens de production et de transport (cf. transport ferroviaire suédois en 2018) et des objets de toutes sortes.

Les attaques s'appuient soit sur des faiblesses des utilisateurs et organisations (mots de passe trop simples, hameçonnage, mauvaise protection de systèmes informatiques dans une entreprise), soit sur des failles logicielles ou matérielles qui sont de la responsabilité des constructeurs. Ces dernières, souvent subtiles et souvent pas encore connues des fabricants (nommées alors zero-day), peuvent être découvertes par des agents malfaisants puis revendues sur le Web dans un marché très actif. Elles peuvent

aussi l'être par des chercheurs ou d'autres individus indépendants qui les communiquent aux constructeurs pour qu'ils les corrigent avant qu'elles ne soient rendues publiques, soit parce que cela fait partie de leur métier, soit pour recevoir une récompense. Mais la relation recherche / industrie n'est pas toujours simple sur ces sujets, et la correction des systèmes de protection n'est pas toujours possible. De plus, les mises à jour des systèmes obsolètes ne sont pas toujours bien faites et de nombreux systèmes vulnérables continuent à fonctionner, par exemple dans l'appareillage technique ou médical. Il est indispensable de réduire considérablement le nombre de bugs dans les systèmes, actuellement trop élevé, pour garantir à la fois leur sûreté de fonctionnement et leur sécurité face aux attaques.

CHIFFREMENT, PROTOCOLES DE SÉCURITÉ, CANAUX CACHÉS

La clef de la protection reste la sécurisation des données et des communications, qui s'appuie sur plusieurs piliers. Sur le plan scientifique, on distingue deux activités algorithmiques complémentaires et imbriquées : d'une part le chiffrement, de nature mathématique, et d'autre part les protocoles de sécurité qui permettent par exemple d'échanger en ligne des clefs de chiffrement de façon sûre, de signer des documents ou transactions, de voter, etc. Ces deux domaines posent des défis scientifiques difficiles mais passionnants. La recherche française est en pointe sur ces sujets, en mathématiques pour le chiffrement moderne et en informatique pour la conception et la validation formelle des protocoles. Le chiffrement moderne est mathématiquement très sûr, mais il reste deux problèmes importants.

D'abord, les algorithmes y sont complexes et leur implémentation reste très délicate, provoquant quelquefois des trous de sécurité difficiles à détecter et engendrant potentiellement des catastrophes (la fameuse faille HeartBleed est un bel exemple). Une implémentation qui n'est pas assez soignée peut aussi permettre des attaques par canaux cachés (mesure d'oscillations de la consommation électrique ou du bruit provoqué par les composants électroniques, etc.). Enfin, certains chiffrements trop faibles restent en place pour diverses raisons, fournissant des points d'attaque faciles.

Les protocoles de sécurité restent cependant le principal point faible, car ils sont nombreux, délicats, et pas toujours difficiles à attaquer. La recherche scientifique dans ce domaine est très difficile mais progresse, la France y étant très active. Par exemple, l'Inria et Microsoft développent une version prouvée mathématiquement sûre par rapport à ses spécifications de TLS, le principal protocole de transfert de données du Web, et le LORIA Nancy a développé Belenios, le premier protocole de vote en ligne prouvé mathématiquement sûr modulo des hypothèses raisonnables sur l'honnêteté des autorités du vote.
Par ailleurs il existe toujours des dangers liés à des canaux cachés, portes latérales permettant d'accéder à des informations normalement inaccessibles, même lorsque des systèmes ne comportent pas de faille logique. Il en a même été trouvé récemment au plus profond des optimisations internes des microprocesseurs, difficiles à exploiter mais qui permettent de lire la mémoire d'autres utilisateurs sur la même machine. La détection et la correction de ces canaux cachés est une question scientifique jamais terminée par construction.

DÉTECTION AUTOMATIQUE DES ATTAQUES

Un autre point important est celui de la détection des attaques, qui doit être automatisée car la réaction doit être rapide. Des méthodes formelles spécifiques ainsi que des algorithmes de traitement du signal ou d'apprentissage peuvent y être efficaces, et doivent de toutes façons être employés pour tout système sensible. Ce sujet plus jeune mérite des efforts scientifiques accrus.

L'IMPACT POTENTIEL DES ORDINATEURS QUANTIQUES

Dans un avenir encore largement hypothétique, des ordinateurs quantiques pourraient casser les chiffrements principaux du Web, mais de nouveaux chiffrements post-quantiques sont en cours de normalisation ; la transition sera cependant longue et complexe, et doit être démarrée dès maintenant pour éviter tout risque majeur ultérieur. Faute de s'y prendre à temps, il n'est pas exclu qu'on ne parvienne pas à installer en temps utile de nouvelles protections à l'échelle voulue au vu de la taille et de la complexité des réseaux et applications modernes, ni à rechiffrer l'ensemble des documents devant rester confidentiels pour une longue période. Tout cela est bien décrit dans un remarquable rapport récent de la *National Academy of Sciences* américaine (https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects).

QUESTIONS ORGANISATIONNELLES ET SOCIÉTALES

Mais la science n'est pas seule actrice et de loin, les questions organisationnelles et sociétales étant tout aussi importantes.
Sur le plan des procédures, la mise en place de la sécurité des systèmes informatiques matériels et logiciels est délicate : un très bon protocole de sécurité peut être mal implémenté et mal utilisé, ou encore n'être déployé que partiellement. De plus, le poids de l'existant rend souvent la sécurité problématique. Par exemple, des attaques par Internet peuvent forcer l'usage de chiffrements trop faibles mais encore conservés dans les protocoles de sécurité courants afin de garder l'accès à des équipements ou systèmes logiciels anciens qui ne peuvent plus être remis à jour.
D'une manière générale, le maillon faible reste souvent du côté des utilisateurs : contrôle d'accès, contrôle des flux, mécanismes continus de supervision et de détection sont ainsi essentiels.
Il reste de fait un fossé considérable entre les connaissances scientifiques et ce qui est réellement implémenté, que ce soit dans les systèmes commerciaux ou dans les systèmes industriels, voire même dans les instituts de recherche. Même si une sécurité à 100% est un leurre, il faut que les différents acteurs, dont les scientifiques, se parlent mieux et se coordonnent mieux. Étant donné le nombre d'aspects différents concernés et le fait qu'il suffit souvent d'un seul point faible pour casser un système, c'est de plus en plus indispensable.

ENJEUX ET DÉFIS

Les types de menaces évoqués se traduisent par autant de risques majeurs : prise de contrôle de systèmes industriels, de transports, d'énergie, hospitaliers ; attaques de déni de service, vol de données et de comptes, pistage géographique ou comportemental, atteintes à la vie privée, etc.
Un point crucial est la faiblesse actuelle des composants de l'Internet des objets (automobiles, petits équipements, caméras, réseaux de capteurs, etc.), mal protégés par des industries peu habituées au sujet, et souvent difficiles à protéger à cause des coûts énergétiques associés. Le nombre d'objets mal sécurisés est inquiétant, et la compétence en sécurité peu répandue chez leurs fabricants. Ceci prend une importance particulière dans le cadre du développement de la 5G, prévue essentiellement pour l'Internet des objets et dont l'ambition est de connecter un million d'objets par km^2 avec une faible latence et une forte sécurité. Les contraintes associées sont heureusement plutôt mieux prises en compte au niveau des réseaux que pour les générations précédentes, mais on trouve encore des failles dans les propositions actuelles.

Si d'autres enjeux de sécurité existent dans des contextes comme le *cloud computing* (lorsque les données sont stockées chez un prestataire), celui du médical requiert une attention particulière du fait d'une culture généralement trop faible des acteurs du domaine, que ce soit en médecine hospitalière ou en

médecine de ville. À l'exemple déjà cité du rançonnage massif des hôpitaux anglais, on peut ajouter celui des trous de sécurités nombreux et faciles à exploiter des pacemakers et pompes à insuline implantés, et des démonstrations de vulnérabilité des robots chirurgiens. L'absence de certification pose par ailleurs un problème majeur, ce qui a motivé aux USA une injonction récente du department of Health à la FDA (*Food and Drug Administration*) afin de prendre en compte la sûreté et la sécurité des circuits logiciels embarqués dans les autorisations médicales d'implants ou appareils informatisés avec le même sérieux que pour les études de médicament, ce qui n'est pas le cas actuellement.
On notera enfin que le problème de la sécurité dans son entier soulève des questions de souveraineté nationale et européenne sur les outils, les stockages et les systèmes.

RECOMMANDATIONS

Afin d'aider à relever les défis posés, on peut décliner quelques recommandations selon trois axes :

- Scientifique : en soutenant la recherche française en sécurité (mathématiques du chiffrement, conception et vérification formelle des protocoles de sécurité, etc.) et en favorisant davantage la recherche systématique des failles dans les systèmes, des canaux cachés, etc., ainsi que les approches scientifiques à la détection d'intrusion (apprentissage, etc.) et à la détection de codes malveillants. De manière plus prospective, même si les machines quantiques de taille suffisante n'apparaîtront probablement pas dans les 10 prochaines années (si elles apparaîtront un jour), il faut se préparer à la possibilité pour elles de casser certaines des briques cryptographiques actuelles (RSA, Diffie-Hellmann). Ceci implique des efforts de recherche, et en particulier de travailler dès maintenant sur les méthodes de chiffrement post-quantiques en vue d'une normalisation future, d'étudier comment réaliser la conversion progressive de tous les ordinateurs et réseaux, ou encore de préparer l'organisation du rechiffrement complet de documents confidentiels dont le chiffrement actuel pourrait être cassé avant qu'ils ne passent dans le domaine public.

- Éducatif : en augmentant la participation aux actions de formation à la sécurité des acteurs divers, en particulier celle des futurs formateurs à la sécurité pour les entreprises ou administrations qui ne seront pas nécessairement issus du monde scientifique. On peut distinguer au moins trois niveaux de formation : niveau d'hygiène pour tous, niveau technique de base pour tous les ingénieurs développant des systèmes, et niveau expert pour les ingénieurs dédiés. La participation des chercheurs à ces formations est souhaitable, voire indispensable. Un volet important est la diffusion de bonnes pratiques comme par exemple l'utilisation de coffres-forts à mots de passe permettant de n'en connaître qu'un et de générer les autres aléatoirement sans jamais les voir.

- Législatif : en détectant et corrigeant les manques ou incomplétudes de la situation actuelle (par exemple, dans le cas du vote électronique, la CNIL n'aborde, de par ses prérogatives, qu'un aspect du problème : le secret du vote ; elle ne se soucie pas de la question tout aussi importante de la transparence du scrutin, c'est-à-dire de la possibilité offerte à un électeur de s'assurer que son vote est pris en compte) ; en agissant aussi contre le manque de formation du côté des juges, qui doivent désormais décider de la bonne ou mauvaise protection des données : la définition d'expert en informatique doit être précisée et rendue plus rigoureuse.