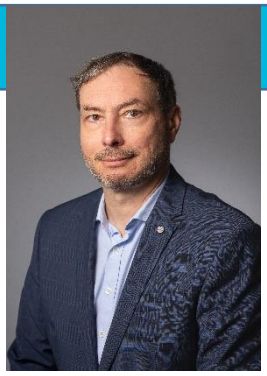
Colloque IMT

« Gestion de crise et numérique : nouvelles menaces et nouvelles solutions »

31 mars 2022 à Palaiseau

Biographies des intervenants



Hervé Debar

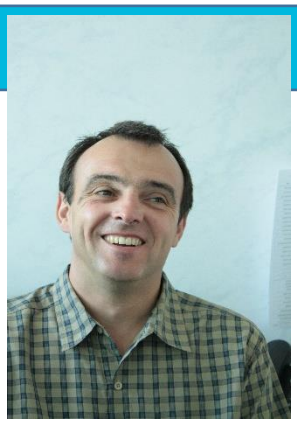
Directeur de la recherche et des formations doctorales

(Télécom SudParis)

Hervé Debar effectue ses recherches dans le domaine de la détection d'intrusion et de la supervision de sécurité depuis 1990. Après avoir développé une des premières sondes comportementales à base de réseaux de neurones (Hyperview, 1994), il a co-inventé en 2000 le domaine de la supervision de sécurité, en publiant l'un des deux premiers articles sur le sujet (RAID, 2000), en contribuant au développement du premier produit commercial sur le sujet (Tivoli Risk Manager, 2000), en éditant le standard IDMEF (RFC4765, mars 2007) et en déposant plus de 10 brevets sur ces sujets.
Il a encadré à ce jour 19 doctorants (4 en cours).
Il a participé à plus de 25 projets collaboratifs français et européens dans le domaine de la cyber sécurité et a coordonné 7 projets européens.
Il est ingénieur de l'Institut National des Télécommunications (1990), docteur de Paris 6 (1993), HDR de l'université de Caen (2004).

Présentation conjointe avec Gilles Dusserre :

Etat des lieux de la recherche en risques et cybersécurité à l'IMT



Gilles Dusserre

Enseignant-chercheur (IMT Mines Alès)

Titulaire d'un Doctorat de Pharmacie (1987-1993), d'un Mastère Sécurité Industrielle et Environnement délivré par la Conférence des Grandes Ecoles (1994), d'un DEA « Chimie de l'Environnement et Santé – Université de Marseille» (1995),
d'un Doctorat *es* Sciences (Chimie, Environnement et Santé) et une Habilitation à Diriger les recherches à l'Université Jean Monnet (St Etienne).
Depuis 1997, il dirige l'équipe Risques Industriels et Naturels de l'Ecole des Mines d'Alès (environ 20 personnes). Il est Directeur de Recherches à l'Ecole des Mines d'Alès depuis Mars 2009. Depuis 1998, il est régulièrement expert à la Commission Européenne (à la DG Environnement, INFSO et REA) en tant qu'évaluateur de projets.

De 2005 à 2007, il anime le Groupe de Travail « Risques industriels majeurs (un des 4 axes du Pôle de Compétitivité Gestion des Risques et Vulnérabilité des Territoires). De 2007 à 2010, il a été Directeur d'un Groupement d'Intérêt Scientifique avec l'INERIS, l'ENSOSP et l'INHESJ portant sur la gestion de crise. De 2010 à 2011, il a été membre du Comité d'évaluation du Programme ANR « Concepts systèmes et Outils pour la Sécurité Globale ». De 2011 à 2014, il a dirigé l'Institut des Sciences des Risques à l'Ecole des Mines d'Alès. Depuis 2018, il co - anime la Thématique Phare Cybersécurité & Risques au sein de la DG Recherche de l'IMT.
Auteur ou co-auteur de près de 30 publications, ouvrages ou conférences dans le domaine des risques et de la gestion de crise, il est membre de The International Emergency Management Society.

Présentation conjointe avec Hervé Debar :

Etat des lieux de la recherche en risques et cybersécurité à l'IMT

Laurent Aprin

Enseignant-chercheur (IMT Mines Alès)

Laurent APRIN est professeur à IMT Mines Alès et directeur du Laboratoire des Sciences des Risques. Après un doctorat en mécanique des fluides et énergie de l'Université de Provence en 2003, il intègre en 2004 le CNRS en tant qu'ingénieur de recherche pour étudier les écoulements diphasiques et les changements de phase dans les milieux poreux.
En 2005, il rejoint IMT Mines Alès pour étudier les mécanismes de dispersion des polluants chimiques en mer. Ses activités de recherche et d'enseignement portent sur la compréhension et la modélisation des écoulements et plus particulièrement sur les mécanismes de transfert lors des pollutions chimiques et des rejets de gaz dans les milieux aquatiques.
Depuis 2012, cette recherche est portée par des projets européens (HNS-MS et MANIFESTS) et s'intègre dans une démarche d'aide à la prise de décisions pour les différentes parties prenantes.

Présentation conjointe avec Alicja Tardy : Jeux sérieux et gestion de crise : de nouveaux outils pour la formation des citoyens à la gestion de crise

Résumé : *La pandémie liée au COVID nous rappelle que les crises sont des événements extraordinaires, avec des intensités et des durées très différentes qui mettent les pouvoirs publics, les organisations et les citoyens dans des situations imprévisibles et complexes à gérer. La préparation à de tels évènement passe traditionnellement par l'emploi de cours transmissifs éventuellement suivis d'exercices sur table préparatoires. Or, l'utilisation de ces méthodes classiques peut entrainer des biais pédagogiques (maîtrise de nombreux prérequis techniques et non-techniques, difficulté d'engagement, asynchronisme…) et donc une difficulté d'apprentissage des concepts et des mécanismes de gestion. De nombreux travaux récents issus des sciences de l'éducation soutiennent l'idée que le jeu sérieux, qu'il soit issu d'un processus de création ex nihilo ou la résultante d'un processus de ludification, est un moyen efficace pour engager des participants et contribue positivement à l'acquisition de connaissances et de compétences. C'est dans ce contexte que les chercheuses et chercheurs d'IMT ont développé de nouveaux outils basés sur ces jeux sérieux. Leur utilisation permet alors aux apprenants de vivre des situations qui ne sont pas familières et ainsi d'apprendre de façon ludique et de développer de nouvelles compétences (travail collaboratif, communication, action proactive, stratégie, tactique…) nécessaires à une meilleure gestion des*

évènements. Parmi ces outils, un focus sera porté sur Cit'in crise, simulateur de gestion de crise inondation à destination du grand public, développé en commun par Mines Saint-Etienne et Mines d'Alès.

Alicja Tardy

Enseignante-chercheuse (Mines Saint-Etienne)

Enseignante-chercheuse au sein de l'IMT Mines Saint-Etienne/ UMR 5600 Environnement Ville Société, Hydrogéologue Minier, responsable de la formation ICM dans le domaine du management et de la maîtrise des risques majeurs (technologiques et NaTech), fiabilité et la gestion de crise. Dans le cadre de RDT 2006, elle a codirigé avec Mines de Nancy (PAST 2008-2010), le projet national iCrisis – un dispositif de simulation de la gestion de crise - en collaboration notamment avec 5 laboratoires de recherches de l'Université de Loraine et la participation des experts de niveau national. Ses travaux de recherche, initialement focalisés sur les thématiques de la gestion de ressources en eau et de l'ingénierie pédagogique, ont pour objet ces dernières années la problématique de la résilience territoriale et les risques majeurs/naturels (DDRM, RDT Restoterin - présentation des résultats à Osaka au Japon en 2015-, Cit'in crise).

Présentation conjointe avec Laurent Aprin :

Jeux sérieux et gestion de crise : de nouveaux outils pour la formation des citoyens à la gestion de crise

Sandrine Bayle

Enseignante-chercheuse (IMT Mines Alès)

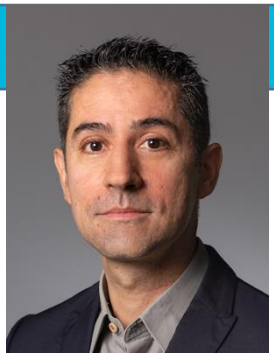
Sandrine Bayle est maitre-assistant à IMT Mines Alès et travail au sein du Laboratoire des Sciences des Risques. Après un doctorat en écologie microbienne à l'IMT Mines Alès et l'université de Lyon I. En 2006 en tant qu'ingénieur de recherche, elle développe des capteurs biologiques pour détecter les contaminants dans les eaux. Depuis 2012, elle a orienté ses recherches sur les aérosols microbiens. Elle étudie notamment les émissions de ces contaminants à partir des procédés biologiques de dépollution et les méthodes de détection applicable sur le terrain.

Présentation conjointe avec Joaquin Garcia Alfaro :

Plateforme de sécurisation des villes - le projet européen IMPETUS

Résumé : *Les villes connectées ou « smart cities » reposent sur un concept visant à surveiller et à intégrer les conditions de toutes leurs infrastructures critiques afin de relever les défis actuels et futurs de*

l'urbanisation. L'objectif est ainsi d'optimiser leurs ressources, de planifier des activités de maintenance préventive et de contrôler les aspects de sûreté et de sécurité.
La sécurité publique est un pilier de l'infrastructure mis en place dans les « smart cities ». La sécurisation des villes Européennes est aujourd'hui une problématique importante. La sécurité doit prendre en considération aussi bien la sécurité personnelle, que la sécurité numérique, la sécurité sanitaire ou la sécurité des infrastructures.
Le projet IMPETUS s'intéresse à ces différents aspects. Il souhaite le développement d'une plateforme éthique regroupant des outils pour améliorer la sécurisation des villes.
Dans le cadre de ce projet, deux équipes de l'IMT participent, pour améliorer la détection des cyberattaques, ainsi que détecter les attaques bioterroristes.



Joaquin Garcia-Alfaro

Professor (Télécom SudParis)

Joaquin Garcia-Alfaro is Professor in the Networks and Telecommunication Services department at Télécom SudParis (Institut Mines-Télécom) and Adjunct Research Professor at Carleton University (Ottawa, Canada).

His research interests include a wide range of cybersecurity problems, with an emphasis on the management of formal policies, analysis of vulnerabilities, and enforcement of countermeasures. He holds a double PhD diploma in Computer Science and a research Habilitation from Université Pierre et Marie Curie. He is involved in several research projects at National and European levels, related to ICT security. He has served as general chair of conferences such as RAID and ATC; and in the technical committee of conferences such as ESORICS and AsiaCCS.
He has been the recipient of several awards for excellence in his career. His work has also been disseminated in terms of patents, industrial transfer of proof-of-concept tools and science divulgation magazines.

Présentation conjointe avec Sandrine Bayle :

Plateforme de sécurisation des villes - le projet européen IMPETUS

Frédérick Benaben

Professeur (IMT Mines Albi)

Frederick Benaben est professeur à IMT Mines Albi (Centre Génie industriel), adjunct-professor adjoint à Georgia Tech (ISyE - School of Industrial and Systems Engineering) et à l'Université JiaoTong de Beijing (SEM - School of Economics and Management).
Il est responsable de l'axe de recherche "Sécurité et Gestion de Crise", et Directeur de l'option GSI (système d'information) d'IMT Mines Albi. Il est en charge de la plateforme IOMEGA-VR sur les technologies immersives et co-dirige le laboratoire international SIReN (Sentient Immersive Response Network), entre IMT Mines Albi et Georgia Tech.

Il travaille sur l'utilisation des données pour modéliser des situations instables et accompagner la prise de décision. Il est l'instigateur et le coordinateur des travaux sur la plateforme logicielle R-IOSuite pour la gestion de crise qui a été demi-finaliste du concours IBM Call4Code 2019 (l'un des 5 logiciels européens sélectionnés parmi les 25 demi-finalistes mondiaux, issus de plus de 5 000 concurrents). Il dirige également l'initiative POD sur la physique de la décision pour le pilotage par la performance selon des paradigmes hérités de la physique.
Au cours des 20 dernières années, il a été le superviseur ou le directeur de 31 doctorants, acteur ou coordinateur de 19 projets de recherche collaborative ou industrielle financés (pour plus de 7 millions d'euros de financement), et auteurs ou co-auteurs de plus de 180 communications à des conférences internationales et de 30 articles de journaux internationaux.

Présentation : La réalité virtuelle et les technologies immersives au service de la gestion de crise illustration issues des résultats de différents projets de recherche

Résumé : *Les technologies immersives (réalité virtuelle, réalité augmentée, réalité mixte) envahissent littéralement tous les domaines du quotidien. Depuis plus de 15 ans, le Centre Génie Industriel (IMT Mines Albi) propose des contributions scientifiques dans le domaine de la gestion des risques et des crises. Plus particulièrement, les travaux menés l'ont été dans le domaine des systèmes d'information et des nouvelles technologies pour la prise de décision en situation de crise, le pilotage collaboratifs des schémas de réponse et l'entrainement opérationnel aux situations de crise.*
Durant les dernières années, les apports et contributions des technologies immersives au domaine de la gestion des risques et des crises ont pris une place centrale dans ces travaux. Plusieurs projets de recherche (reposant sur des financements publiques et privés) ont ainsi pu être lancés et menés. Ces projets s'intéressent autant à l'entrainement des acteurs opérationnels aux situation de crise en environnement virtuel représentatifs de sites sensibles, qu'à la cellule de crise immersive du futur permettant une participation distanciée et distribuée des décideurs ou l'accès à de nouvelles fonctionnalités riches et innovantes. Certains projets se penchent également sur l'utilisation de la réalité virtuelle pour la gestion des risques selon des modes innovants de prise de décision permettant d'appréhender des concepts abstraits au travers d'objets concrets virtuels.
C'est un panorama de ces projets, des résultats qu'ils apportent et des perspectives qu'ils ouvrent qui sera présenté durant cet intervention.

Jean-Max Dutertre

Professeur (Mines Saint-Etienne)

Jean-Max Dutertre est professeur, responsable du département Systèmes et Architectures Sécurisés de Mines Saint-Etienne. Sa thématique de recherche porte sur les attaques matérielles visant les circuits et systèmes sécurisés : attaques par injection de fautes et attaques par observation. Son travail porte sur la compréhension des mécanismes, leur modélisation, et la conception de contre-mesures.

Aurélien Francillon

Professeur classe 2 (EURECOM)

Aurélien Francillon est professeur dans le département sécurité d'EURECOM (France).
Il s'intéresse principalement aux aspects pratiques de la sécurité des dispositifs embarqués.

Dans ce contexte, il a travaillé sur des sujets tels que la sécurité matérielle, logicielle et des communications radio. Ses travaux ont souvent été couverts par la presse généraliste, comme "Le Monde", MIT Technology review ou CSO Online.
Plus de 10 doctorants sont actuellement sous sa supervision ou ont déjà obtenu leur diplôme. Il est l'auteur de plus de 50 publications dans des conférences internationales.
Il est chair du steering committee du workshop sur les technologies offensives (WOOT), membre du bureau du GDR Sécurité et du comité scientifique de l'ANSSI (Agence Nationale de la Cybersécurité).

Présentation : Analyse de la sécurité des Firmware de systèmes embarqués, avancées et défis

Grégory Blanc

Maître de conférences (Télécom SudParis)

Gregory BLANC est maître de conférences en réseaux et sécurité à Télécom SudParis depuis 2015, membre du laboratoire SAMOVAR. Il coordonne la spécialisation de dernière année d'études d'ingénieur en sécurité des systèmes et réseaux (SSR) depuis 2020.

Il a obtenu son doctorat en ingénierie informatique sur le thème de l'analyse des scripts malveillants côté navigateur en 2012 au Nara Institute of Science and Technology, Japon. Il a participé au montage et à la coordination technique de quelques projets tels l'action de coordination et de support conjointe européenne-japonaise sur la cybersécurité EUNITY (H2020, 2017-2019), le projet européen sur la sécurité des IoT VARIoT (CEF, 2019-2022) et le projet de recherche collaboratif GRIFIN (ANR, 2021-2024).

Ses intérêts se portent sur la détection d'intrusion, l'automatisation de la réponse, et l'application de l'IA à la cybersécurité sur des domaines d'application tels que les IoT ou les réseaux SDN et 5G.

Présentation : Sécurité du smart home : détection d'anomalies réseau

Résumé : *Avec une croissance de 9% entre 2020 et 2021, le nombre d'objets connectés en usage dans le monde atteint désormais 12,3 milliards. Une large majorité appartient à la catégorie domotique (ou Smart*

Home) et sont directement au contact des utilisateurs soit via des interfaces physiques (boutons, molettes, écrans tactiles), soit via leur smartphone. Ces objets du quotidien (ampoule, prise, détecteur de mouvement ou de fumée, caméra) sont connectés au réseau sans fil domestique, et ont souvent accès à Internet. Ces objets sont cependant bien souvent vulnérables et offrent l'opportunité à des criminels de les compromettre et les détourner afin d'espionner leurs propriétaires, ou d'attaquer de manière massive une tierce victime sur Internet.

Dans nos travaux, nous nous sommes demandés comment détecter des attaques perpétrées par ces objets ainsi détournés. La détection d'attaques est susceptible d'être contournée lorsque des vecteurs d'attaques jusqu'alors inconnus sont exploités par les criminels. Nous nous sommes donc concentrés sur la détection d'anomalies qui requiert de connaître le comportement sain des objets, plutôt que le comportement malveillant des objets compromis. En effet, nous avons remarqué le que le déterminisme de la plupart des comportements des objets connectés nous permettait assez aisément de construire des profils de trafic normal issu des objets de type Smart Home dans une plateforme que nous avons développé dans le cadre du projet VARIoT.

Nous avons ainsi pu construire un détecteur d'anomalies sur la base d'un auto encodeur, un type de réseaux de neurones, très efficace pour détecter des déviations par rapport à des comportements appris par celui-ci. Nous sommes conscients cependant des limites de l'approche, et de la capacité d'un attaquant déterminé à reproduire de tels comportements comme nous l'avons démontré par la suite avec notre générateur de trafic réseau légitime basé sur les réseaux génératifs antagonistes (GAN). Finalement, nous avons aussi étudié la capacité des algorithmes d'apprentissage machine et profond à correctement classifier les objets connectés de type Smart Home au travers d'une étude approfondie de la littérature du domaine.

Marc-Olivier Pahl

Directeur de recherches (IMT Atlantique)

Prof. Dr. Marc-Oliver Pahl heads the Chair Cybersecurity for Critical Networked Infrastructures (cyberCNI.fr) at IMT Atlantique Rennes, France. The chair hosts 18 professors, 8 PhDs, 8 PostDocs, and multiple engineers and interns. Marc-Oliver is an adjunct professor of Carleton University in Canada. Marc-Oliver's research focus is on a holistic approach to cybersecurity. He is an experienced teacher and an eLearning pioneer, holding several teaching awards.

Présentation : Cybersécurité collaborative renforcée par la réalité virtuelle pour les infrastructures critiques

Philippe Jaillon

Enseignant-chercheur (Mines Saint-Etienne)

Philippe Jaillon est enseignant chercheur à l'école des mines de St-Etienne. Il a obtenu son doctorat en 1993 et est membre de l'équipe de recherche commune entre les Mines de St-Etienne et le CEA : "Systèmes et Architectures Sécurisés" (SAS). Ses centres d'intérêts portent sur les interactions entre le hardware et le software dans les infrastructures réseaux. L'objectif de ces travaux est de rendre plus sûr les communications, que ce soit dans les réseaux très haut débit où il étudie les canaux auxiliaires qui pourraient être portés par la lumière, ou dans les réseaux radio bas débit et longues distances pour rendre l'accès aux objets connectés plus transparents et plus sûr. Ces travaux sont appliqués ces dernières années au domaine de l'industrie du futur et mis en œuvre dans les ateliers pilotes des Mines de St-Etienne : l'IT'm Factory et DIWII.

Présentation conjointe avec Ludovic Apvrille : Influence des mises à jour de sécurité sur le comportement d'un système critique

Résumé : *Les systèmes cyber-physiques sont des systèmes critiques qui sont capable d'interagir avec leur environnement par le biais de capteurs et d'actionneurs. Ces éléments étant contrôlés par des logiciels, une cyber-attaque qui les toucherait aurait des conséquences inacceptables.*

Il convient donc de les protéger des attaques en déployant des contre-mesures, tout en s'assurant que les modifications apportées n'induisent pas à leur tour des comportements néfastes aux systèmes.

Dans cet exposé, nous présenterons W-Sec, une méthode conçue par Mines de St-Eienne et Télécom Paris dans le cadre du projet européen SPARTA. Cette méthode vise à évaluer quantitativement, en amont de leur déploiement, les impacts que peuvent avoir des contremesures sur des systèmes cyber-physiques.

Cette évaluation, qui se fait en termes de sûreté, de sécurité et de performances et s'appuie sur l'utilisation de TTool, un outil de modélisation et de vérification formelles développé au sein de l'équipe LabSoC de Télécom Paris.

Ludovic Apvrille

Enseignant-chercheur (Télécom Paris)

Prof Ludovic Apvrille obtained his M.Sc. in Computer Science, Network and Distributed Systems specialization in 1998 from ENSEIRB and ISAE. He then completed a Ph.D. in 2002, in the Department of Applied Mathematics and Computer Science at ISAE, in collaboration with LAAS-CNRS and Alcatel Space Industries (now, Thalès Alenia Space).

After a postdoctoral term at Concordia University (Canada), he joined LabSoc in 2003 as an assistant professor at Telecom Paris, in the Communication and Electronics department.

He obtained his HDR (Habilitation à Diriger les Recherches) in 2012, and became Professor in 2018.

His research interests focus on tools and methods for the modeling and verification of embedded systems and Systems-on-Chip. Verification techniques target both safety and security properties.

He's the inventor and the main contributor of the free and open-source UML/SysML toolkit named TTool. He's the team leader of the LabSoC.

Présentation conjointe avec Philippe Jaillon : Influence des mises à jour de sécurité sur le comportement d'un système critique

Serge Vaudenay

Professor EPFL

Serge Vaudenay entered at the École normale supérieure in Paris in 1989

with a major in mathematics. He received his PhD in computer sciences from University of Paris 7 – Denis Diderot in 1995.

He subsequently became a research fellow at CNRS. In 1999, he was appointed as a Professor at the EPFL, where he created the Security and Cryptography Laboratory.

He works on cryptography and the security of digital information. Most of his work relates to security analysis and provable security of cryptographic algorithms and protocols, specially in secure communication, post-quantum cryptography, RFID protocols and distance bounding. Recently, he joined the GlobalID company where he develops secure privacy-preserving applications based on biometry.

Hieu Phan

Professeur (Télécom Paris)

Hieu Phan has been a professor at Télécom Paris since 2020.

He is leader of the Cybersecurity-Cryptography team at Telecom Paris.

He obtained a Ph.D degree at Ecole Normale Supérieure in 2005.

Before joining Telecom Paris, he was a professor at XLIM, University of Limoges (2015-2020), an Associate Professor at University of Paris 8 (2007-2015) and a Postdoctoral Researcher (2005-2006) at University College London.

His research focuses on the use of mathematical/algorithmic methods in the design of cryptographic schemes and he has published in top venues of the field (Eurocrypt, Crypto, Asiacrypt, ACM CCS, ICALP, Algorithmica, IEEE TIFS etc).

He has been a member of the IACR Asiacrypt's steering committee since 2013, and a member of IACR Board of Directors in 2015-2016 as a General co-Chair for ASIACRYPT '16. He has served on the program committees of more than 30 international conferences, including Eurocrypt, Asiacrypt, PKC

Présentation : Privacy in Advanced Cryptographic Protocols

Summary: *Cryptography is a fundamental cornerstone of cybersecurity, traditionally supporting data confidentiality, integrity, and authenticity. However, when cryptographic protocols are deployed in emerging*

applications such as cloud services or big data, the demand for security grows beyond these requirements. Data nowadays are being extensively stored in the cloud, and users also need to trust the cloud servers/ authorities that run powerful applications. Collecting user data, combined with powerful tools (e.g., machine learning), can come with a huge risk of mass surveillance or of undesirable data-driven strategies for profit making, while ignoring users'needs.

Privacy protection, which allows individuals to have control over how their personal data is collected and used, therefore, becomes more and more important. New techniques should be developed, first, to protect personal privacy, and, second, to reduce centralized trust in authorities or in technical solutions providers. In this talk, we discuss privacy protecting methods of various cryptographic protocols, in particular in electronic voting systems and in multi-user cryptography.

Claire Levallois

Maître de conférences (Télécom Paris)

Claire Levallois-Barth est enseignante-chercheure en droit à Télécom

Paris, grande école composante de l'Institut Mines-Télécom (IMT) et de l'Institut Polytechnique de Paris IP Paris.

Elle est la Coordinatrice de la Chaire Valeurs et Politiques des Informations Personnelles de l'IMT, en charge pour l'IMT du programme Living Lab 5G et responsable de l'axe 5 Protection des données personnelles impliquées dans le véhicule connecté de la Chaire Connected Cars & Cyber Security (C3S) de Télécom Paris.

Claire Levallois-Barth est membre du Comité national pilote d'éthique du numérique, du comité scientifique du Forum International de la Cybersécurité (FIC), du Data Privacy Expert Panel d'AXA, du Comité d'éthique sur l'intelligence artificielle de Pôle Emploi et membre du Comité éthique de la Data et de l'IA d'Orange.

Présentation : Informations personnelles et cybersécurité : le risque par essence indissociable : la Chaire VP-IP et l'état de l'art 2022

Fen Zhou

Professor (IMT Nord Europe)

Fen Zhou is a Professor at IMT Nord Europe.

He received his Ph.D. degree on networking from INSA of Rennes in 2010 and the HDR degree at the University of Avignon in 2018. Before joining IMT Nord Europe, he worked as an

Associate Professor at the University of Avignon from 2012 to 2018, and then at Institut Supérieur d'Electronique de Paris (ISEP) until 2020. His research interests include network survivability and security, routing and resource allocation, as well as network function virtualization. He has published more than 90 papers in peer-reviewed international journals and conferences. He served as the TPC co-chair of IEEE BMSB 2020, Optical and Grid Networking symposium co-chair of IEEE ICNC 2018, publicity co-chair of IEEE Wimob 2015/2019, and Springer NetgCOOP 2016, session chair of IFIP Networking 2020 and IEEE Mascots 2019.

He is a Senior Member of IEEE since 2015, and was in the review panel of IEEE Senior Membership application held in Paris on 2016.

Présentation : Disaster Protection in Inter-DataCenter Networks leveraging Cooperative Storage