

Programme – Jour 1

13 mars 2023 | Auditorium de l'OCDE

09:30-09:45

Ouverture de l'événement

- **Mathias Cormann**, Secrétaire général, OCDE
- **Tomoo Yamauchi**, Directeur général de la cybersécurité, Ministère des affaires intérieures et des communications, Japon (pré-enregistré)

Thème 1 : Alors que les décideurs politiques s'apprêtent à mettre en œuvre des politiques de sécurité, comment pouvons-nous soutenir l'application de meilleures pratiques dans l'internet des objets (IdO) ?

09:45-10:45

Planter le décor : L'ampleur du défi de la sécurité de l'IdO

Une mauvaise sécurité dans l'IdO présente une série de défis pour les consommateurs, les entreprises et les gouvernements. Cette session offrira l'opportunité aux hauts représentants de la société civile, aux représentants des consommateurs et des entreprises, aux gouvernements et à la communauté de la sécurité de partager une série de perspectives sur les défis croissants dans ce secteur ainsi que sur les possibilités de les relever rapidement par des mesures législatives et non législatives.

- Modérateur : **Peter Stephens**, Analyste des politiques, OCDE
- **Melanie Garson**, Responsable de la cybersécurité, Tony Blair Institute for Global Change
- **Michelle Levesley**, Responsable de la sensibilisation à la cybersécurité, Channel 4
- **Javier Ruiz Diaz**, Conseiller principal pour les droits numériques, Consumers International
- **Shinya Tahata**, Directeur, Bureau du directeur général pour la cybersécurité, Ministère des affaires intérieures et des communications, Japon
- **Beau Woods**, Défenseur de la cybersécurité, I am the Cavalry

10:45-11:05

Pause-café

11:05-12:05

Approches des décideurs politiques : Un aperçu de la sécurité de l'IdO en 2023

2023 représente une nouvelle frontière pour la sécurité de l'IdO, avec le développement d'approches législatives dans l'Union européenne, aux États-Unis et au Royaume-Uni, ainsi que des efforts politiques plus larges en cours au Japon, à Singapour et dans bien d'autres pays. Cette session réunira des décideurs politiques de haut niveau du monde entier qui partageront leur point de vue sur leur approche et les étapes à venir pour fournir des produits et services plus sûrs.

- Modératrice : **Constance Mougnot-Gallais**, Chargée des affaires politiques européennes et internationales, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France
- **Daisuke Hoshi**, Directeur aux affaires internationales, Division de la cybersécurité, Ministère de l'économie, du commerce et de l'industrie, Japon
- **Gaurav Keerthi**, Directeur général adjoint, Agence de cybersécurité de Singapour (à distance)
- **Christiane Kirketerp de Viron**, Cheffe d'unité, Politique de cybersécurité et vie privée numérique, DG CNECT, Commission européenne (à distance)
- **Erika Lewis**, Directrice, Cybersécurité et identité numérique, Département de la science, de l'innovation et de la technologie, Royaume-Uni
- **Katerina Megas**, Responsable du programme Cybersécurité pour l'IdO, Institut national des normes et de la technologie (NIST), États-Unis

12:05-12:25 | **Pause-café**

12:25-12:45 | **Discussion (débat modéré)**

Les participants partageront leurs points de vue et leurs idées sur les questions centrales de la matinée, afin qu'ils puissent également être pris en compte dans les travaux futurs et les possibilités de collaboration du Forum mondial.

- Modérateur : **Peter Stephens**, Analyste des politiques, OCDE

12:45-13:00 | **G20 : Une perspective de l'Inde**

L'Inde assure la présidence du G20 du 1er décembre 2022 au 30 novembre 2023. Dans le cadre de cette présidence, le G20 a l'ambition de progresser en matière de politique de sécurité numérique, notamment en ce qui concerne la sécurité des produits et des services. Les participants pourront en apprendre davantage sur les progrès réalisés et les possibilités de soutenir ces efforts au cours de l'année.

- **Sushil Pal**, Secrétaire adjoint, Ministère de l'électronique et des technologies de l'information, Inde (pré-enregistré)

13:00-14:30 | **Déjeuner**

Thème 2 : Comment intégrer une approche de « sécurité dès la conception » dans les politiques d'intelligence artificielle ?

14:30-15:45 | **Risques de sécurité dans l'intelligence artificielle**

Cette session partagera des idées provenant des secteurs public et privé pour mettre en évidence les défis de la sécurité au sein de l'intelligence artificielle, avec des risques tels que le manque de transparence et d'explication, les préjugés et la discrimination, la vulnérabilité aux attaques, le manque de surveillance humaine et les problèmes de confidentialité. Ces risques peuvent conduire à des décisions erronées ayant un impact négatif sur des individus ou des groupes. En outre, la sécurité de l'IA est liée à d'autres questions de sécurité numérique. Par exemple, les risques de sécurité de l'IA peuvent affecter la sécurité des produits si les produits connectés tels que les voitures sans conducteur ou les appareils ménagers alimentés par l'IA ne sont pas suffisamment sécurisés.

- Modérateur : **Daniel Faggella**, Responsable de la recherche, Emerj
- **Vijay Bolina**, Chef de la sécurité de l'information, DeepMind (à distance)
- **Sophie Kuijt**, Directrice de la technologie, IBM Consulting North and Central Europe
- **Yutaka Miyake**, Directeur, Information System and Security Department General Affairs Division KDDI Research, Inc (à distance)
- **Clara Neppel**, Directrice principale, IEEE
- **Taylor Reynolds**, Directeur de la politique technologique, MIT Internet Policy Research Initiative (IPRI)

15:45-16:05 | **Pause-café**

16:05-16:30 | **Discussion (débat modéré)**

Les participants partageront leurs points de vue et leurs idées sur les questions centrales de l'après-midi, afin qu'ils puissent également être pris en compte dans les travaux futurs et les possibilités de collaboration du Forum mondial.

- **Daniel Faggella**, Responsable de la recherche, Emerj

16:30-17:45

Réponses politiques aux défis de sécurité de l'intelligence artificielle

Le développement et la mise en œuvre rapides des systèmes d'IA soulignent la nécessité d'un environnement politique stable qui favorise une approche numériquement sûre et sécurisée pour une IA digne de confiance. Par conséquent, il est important que les gouvernements, les organisations et les parties prenantes prennent des mesures pour atténuer les risques de sécurité et de sûreté lorsqu'ils développent, déploient ou exploitent des systèmes basés sur l'IA, et qu'ils appliquent en permanence des approches systématiques de gestion des risques à chaque phase du cycle de vie des systèmes d'IA. Ce panel sera l'occasion de discuter des pratiques et des cadres politiques existants, ainsi que des nouvelles approches et des prochaines étapes potentielles, afin que les décideurs politiques puissent s'orienter vers des approches plus axées sur la sécurité dans l'élaboration des politiques d'IA.

- Modératrice : **Karine Perset**, Cheffe de l'unité IA, OCDE
- **Amit Elazari**, Directrice de la politique mondiale de cybersécurité, Intel (à distance)
- **Sebastian Hallensleben**, Président, CEN CENELEC JTC21 (à distance)
- **Patrick Penninckx**, Chef du département Société de l'information, Conseil de l'Europe
- **Benjamin Prud'homme**, Directeur exécutif, Département IA pour l'humanité, Mila – Institut québécois d'intelligence artificielle
- **Madhulika Srikumar**, Cheffe de programme pour l'IA critique pour la sécurité, Partnership on AI (à distance)

18:00-20:00

Cocktail

Salle George Marshall de l'OCDE

Programme – Jour 2

14 mars 2023 | Auditorium de l'OCDE

Thème 3 : Comment mieux promouvoir la collaboration entre les communautés techniques et politiques pour relever les futurs défis de sécurité liés aux technologies nouvelles et émergentes ?

09:30-09:45

Étude de cas sur les partenariats entre la communauté politique et celle de la sécurité

En 2022, près de trente institutions de l'infrastructure gouvernementale costaricienne ont été victimes d'une attaque coordonnée par *ransomware*. En réponse à cette attaque, le gouvernement a rapidement mis en place des partenariats efficaces avec la communauté des chercheurs en sécurité afin de renforcer la résilience de l'infrastructure numérique. Cet exposé présentera l'importance des partenariats entre les communautés chargées de l'élaboration des politiques et de la sécurité.

- **Paula Bogantes**, Ministre des sciences, de l'innovation, de la technologie et des télécommunications, Costa Rica (pré-enregistré)

09:45-10:45

Élaboration de politiques en matière de sécurité – travailler efficacement avec les agences de sécurité sur les technologies émergentes

Au cours de cette session, des représentants de haut niveau d'une série d'agences de sécurité partageront leurs idées sur ce qui constitue des partenariats efficaces entre les décideurs politiques et les agences de sécurité. Il peut s'agir d'exemples de partenariats réussis ou de leçons tirées de leur expérience.

- Modératrice : **Audrey Plonk**, Cheffe de la Division de la politique de l'économie numérique, OCDE
- **Sanjay Bahl**, Directeur général, Indian Computer Emergency Response Team (CERT-In), Inde (à distance)
- **Erika Lewis**, Directrice, Cybersécurité et identité numérique, Département de la science, de l'innovation et de la technologie, Royaume-Uni
- **Jeff Moss**, Président, DEFCON Communications Inc
- **Jonathan Murphy**, Directeur de la cyberpolitique, Département de la sécurité intérieure, Etats-Unis
- **Christopher Painter**, Président, Global Forum on Cyber Expertise
- **Yves Verhoeven**, Directeur de la stratégie, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France

10:45-11:00

Pause-café

11:00-12:15

Construire des ponts entre la communauté de la recherche et la communauté politique en matière de sécurité

Cette session réunira des professionnels de la sécurité et de la technique ayant l'expérience de partenariats avec les décideurs politiques dans des contextes nationaux et internationaux. Ils partageront leur expérience en matière de direction et d'impact des technologies émergentes. Dans le prolongement de la session précédente, cette session offrira aux décideurs politiques un aperçu utile à appliquer aux défis futurs.

- Modérateur : **Florian Schütz**, Directeur du Centre national de cybersécurité, Suisse
- **Jen Ellis**, Fondatrice, NextJen Security
- **Harley Geiger**, Conseiller, Venable LLP
- **Sebastian Hallensleben**, Président, CEN CENELEC JTC21 (à distance)
- **Amélie Koran**, Directrice, External Technical Relations at Electronic Arts (à distance)
- **Kirsty Paine**, Conseillère stratégique, Splunk
- **Beau Woods**, Défenseur de la cybersécurité, I am the Cavalry

12:15-12:25

Commentaires (session modérée)

Les participants partageront leurs points de vue et leurs idées sur les questions centrales de l'après-midi, afin qu'ils puissent également être pris en compte dans les travaux futurs et les possibilités de collaboration au sein du Forum mondial.

- Modérateur : **Florian Schütz**, Directeur du Centre national de cybersécurité, Suisse

12:25-12:30

Remarques de clôture

- **Andrew Wyckoff**, Directeur de la science, de la technologie et de l'innovation, OCDE