Day 1 Programme

13 March 2023 | OECD Auditorium

09:30-09:45

Event Opening and Keynotes

- **Mathias Cormann**, Secretary-General, OECD
- **Tomoo Yamauchi**, Director-General for Cyber Security, Ministry of Internal Affairs and Communications, Japan (pre-recorded)

Theme 1: As some policy makers move to implement legislation, how can the multistakeholder community support better security practices across the Internet of Things (IoT)?

09:45-10:45

Scene setting: The scale of the challenge of IoT security

Poor security across the IoT presents a range of challenges for consumers, businesses and governments alike. This session will offer opportunities for senior representatives from civil society, consumer and business representatives, government and the security community to share a range of perspectives on the growing challenge in this sector as well as on opportunities to address them quickly through legislative and non-legislative measures.

- Moderator: **Peter Stephens,** Policy Analyst, OECD
- **Melanie Garson**, Cyber Security Lead, Tony Blair Institute for Global Change
- **Michelle Levesley**, Cyber Security Awareness Lead, Channel 4
- **Javier Ruiz Diaz**, Senior Advisor for Digital Rights, Consumers International
- **Shinya Tahata**, Director, Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications, Japan
- **Beau Woods**, Cyber Safety Advocate, I am the Cavalry

10:45-11:05

Coffee Break

11:05-12:05

Policy maker approaches: An insight on IoT security in 2023

2023 represents a new frontier for the security of IoT, with the development of legislative approaches in the European Union, United States and United Kingdom, as well as broader policy endeavours underway in Japan, Singapore, and many others. This session will convene senior policy makers from around the world to share their perspective on their approach and the upcoming steps to deliver more secure products and services.

- Moderator: **Constance Mougenot-Gallais,** European and International Political Affairs Officer, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France
- **Daisuke Hoshi**, Director for International Affairs, Cyber Security Division, Ministry of Economics, Trade and Industry, Japan
- **Gaurav Keerthi**, Deputy Chief Executive Officer, Cyber Security Agency of Singapore (virtual)
- **Christiane Kirketerp de Viron,** Head of Unit, Cybersecurity and Digital Privacy Policy, DG CNECT, European Commission (virtual)
- **Erika Lewis,** Director, Cyber Security and Digital Identity, Department for Science, Innovation and Technology, United Kingdom
- **Katerina Megas,** Cybersecurity for IoT Program Manager, National Institute of Standards and Technology (NIST), United States

12:05-12:25

Coffee Break

12:25-12:45

Moderated discussion

Attendees will share their perspectives and insights on the core questions for the morning, so that they can also be captured in the future work and collaboration opportunities of the Global Forum.

- Moderator: **Peter Stephens**, Policy Analyst, OECD

12:45-13:00

G20: A perspective from India

India holds the Presidency of the G20 from 1 December 2022 to 30 November 2023. Within this tenure, there is ambition for the G20 to make progress in digital security policy, particularly on the security of products and services. Attendees will be able to learn more about the advances being made and opportunities to support these efforts during the course of the year.

- **Sushil Pal**, Joint Secretary, Ministry of Electronics and Information Technology, India

13:00-14:30

Lunch

Theme 2: How can a 'secure by design' approach be embedded within artificial intelligence policies?

14:30-15:45

Security risks in artificial intelligence

This session will share insights from across the public and private sectors to highlight the challenges of security within artificial intelligence (AI), with risks including lack of transparency and explainability, bias and discrimination, vulnerability to attacks, lack of human oversight, and privacy concerns. These risks can lead to flawed decisions negatively impacting individuals or groups. In addition, the safety of AI is interlinked with other digital security matters. For example, security risks in AI can affect product safety if connected products such as driverless cars or AI-powered home appliances are not sufficiently secure.

- Moderator: **Daniel Faggella**, Head of Research, Emerj
- **Vijay Bolina**, Chief Information Security Officer, DeepMind (virtual)
- **Sophie Kuijt**, Chief Technology Officer for IBM Consulting North and Central Europe
- **Yutaka Miyake**, Director, Information System and Security Department General Affairs Division KDDI Research, Inc (virtual)
- **Clara Neppel**, Senior Director, IEEE
- **Taylor Reynolds**, Technology Policy Director, MIT Internet Policy Research Initiative (IPRI)

15:45-16:05

Coffee break

16:05-16:30

Moderated discussion

Attendees will share their perspectives and insights on the core questions for the afternoon, so that they can also be captured in the future work and collaboration opportunities of the Global Forum.

- Moderator: **Daniel Faggella**, Head of Research, Emerj

16:30-17:45

Policy responses to security challenges in artificial intelligence

The rapid development and implementation of artificial intelligence (AI) systems underline the need for a stable policy environment that promotes a digitally secure and safe approach to trustworthy AI. Therefore, it is important for governments, organisations, and stakeholders to take steps to mitigate security and safety risks as they develop, deploy or operate AI-based systems, and to apply systematic risk management approaches to each phase of the AI system lifecycle on a continuous basis. The panel will provide the opportunity to discuss existing policy practices and frameworks, as well as new approaches and potential next steps so policy makers can lean toward more security-focused approaches in AI policy making.

- Moderator: **Karine Perset**, Head of AI Unit, OECD
- **Amit Elazari**, Director of Global Cybersecurity Policy, Intel (virtual)
- **Sebastian Hallensleben**, Chair, CEN CENELEC JTC21 (virtual)
- **Patrick Penninckx**, Head of the Information Society Department, Council of Europe
- **Benjamin Prud'homme**, Executive Director, AI for Humanity Department, Mila – Québec AI Institute
- **Madhulika Srikumar**, Program Lead for Safety-Critical AI, Partnership on AI (virtual)

18:00-20:00

Cocktail

OECD Salle George Marshall

Day 2 Programme

14 March 2023 | OECD Auditorium

Theme 3: How can we better promote collaboration between the technical and policy making communities address future security challenges within new and emerging technologies?

09:30-09:45

A Case-study of partnerships between the policy making and security communities

In 2022, nearly thirty institutions across the Costa Rican government infrastructure were victim to a coordinated ransomware attack. In response to this, the government has moved quickly to build effective partnerships with the security research community to boost resilience across the digital infrastructure. This talk will set the scene for the importance of partnerships between policy making and security communities.

- **Paula Bogantes**, Minister of Science, Innovation, Technology and Telecommunications, Costa Rica (pre-recorded)

09:45-10:45

Policy making in security – effectively working with security agencies across emerging technologies

Within this session, senior representatives from a range of security agencies will share their insights of what makes for effective partnerships between policy makers and security agencies. This can include evidence of successful partnerships, or lessons acquired from their experience.

- Moderator: **Audrey Plonk,** Head of Digital Economy Policy Division, OECD
- **Sanjay Bahl,** Director General, Indian Computer Emergency Response Team (CERT-In), India (virtual)
- **Erika Lewis**, Director, Cyber Security and Digital Identity, Department for Science, Innovation and Technology, United Kingdom
- **Jeff Moss**, President, DEFCON Communications Inc
- **Jonathan Murphy**, Director of Cyber Policy, Department of Homeland Security, United States
- **Christopher Painter**, President, Global Forum on Cyber Expertise
- **Yves Verhoeven**, Director of Strategy, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France

10:45-11:00

Coffee break

11:00-12:15

Building bridges between the security research and policy communities

This session will bring together security and technical professionals with experience in partnering with policy makers in a range of domestic and international settings. They will share their experience leading and delivering impact across emerging technologies. Building on the previous session, this will offer useful insight for policy makers to apply to future challenges.

- Moderator: **Florian Schütz**, Director of National Cyber Security Centre, Switzerland
- **Jen Ellis**, Founder, NextJenSecurity
- **Harley Geiger**, Counsel, Venable LLP
- **Sebastian Hallensleben**, Chair, CEN CENELEC JTC21 (virtual)
- **Amélie Koran**, Director, External Technical Relations, Electronic Arts (virtual)
- **Kirsty Paine**, Strategic Advisor, Splunk
- **Beau Woods**, Cyber Safety Advocate, I am the Cavalry

12:15-12:25

Moderated feedback

Attendees will share their perspectives and insights on the core questions for the afternoon, so that they can also be captured into future work and collaboration opportunities in the Global Forum.

- Moderator: **Florian Schütz**, Director of National Cyber Security Centre, Switzerland

12:25-12:30

Closing Remarks

- **Andrew Wyckoff**, Director of Science, Technology and Innovation, OECD