GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

ARTIFICIAL INTELLIGENCE AND THE INTERNET OF THINGS

EVENT SUMMARY

13-14 March 2023

OECD

総務省
Ministry of Internal Affairs and Communications

Foreword

This report provides a summary of the fourth annual event of the OECD Global Forum on Digital Security for Prosperity (hereafter, "Global Forum"), which took place on 13-14 March 2023 at the OECD headquarters. The report was drafted by Andras Hlács and Peter Stephens of the OECD and reviewed by speakers, moderators and members of the Working Party on Security in the Digital Economy. The report was approved and declassified via written procedure by the Committee on Digital Economy Policy (CDEP) on 15 September 2023 and prepared for publication by the OECD Secretariat.

This event was sponsored by Japan's Ministry of Internal Affairs and Communications (MIC).

The Secretariat wishes to thank all the moderators and speakers, as well as the Japanese delegation to the OECD, who helped organise the event, including, in particular, Tatsuya Amauchi.

The Global Forum was launched in 2018 to foster sharing of experiences and good practice on digital security risk and its management, mutual learning and convergence of views on core thematic issues related to digital security for economic and social prosperity. Its outputs feed OECD policy discussions and can lead to the development of analytical work, principles and international policy recommendations.

Events are proposed by OECD delegations and organised by the Secretariat in co-operation with the host.

More information about the Global Forum and its events is available at https://oe.cd/gfdsp.

Table of contents

Introduction

This document provides a summary of the fourth annual event of the OECD Global Forum on Digital Security for Prosperity (hereafter, "Global Forum"), hosted at OECD headquarters on 13 - 14 March 2023 in partnership with Japan. The Global Forum brought together over 200 invited experts from 36 countries' governments, businesses, civil society organisations, and academic and technical communities.

The Global Forum was divided into three themes, each represented by two panels and a moderated discussion to capture perspectives from attendees. These themes were:

- As some policymakers move to implement legislation, how can the multistakeholder community support better security practices across the Internet of Things (IoT)?
- How can a 'secure by design' approach be embedded within government policies relating to Artificial Intelligence?
- How can we better promote collaboration between the technical and policy making communities to address future security challenges within new and emerging technologies?

Mathias Cormann, OECD Secretary-General, and **Tomoo Yamauchi**, Director-General for Cyber Security at the Ministry of Internal Affairs and Communications, Japan, opened the Global Forum and welcomed participants with some scene-setting remarks.

Minister **Paula Bogantes**, Minister of Science, Innovation, Technology and Telecommunications in Costa Rica, presented on the lessons learned from the 2022 cyber-attack on the UK infrastructure.

Sushil Pal Joint Secretary from the Ministry of Electronics and Information Technology, India presented on India's Presidency in the G20.

Andrew Wyckoff, Director of Science, Technology and Innovation at the OECD, closed the event.

This summary reflects discussions among panel speakers. It does not necessarily reflect the views of the OECD Secretariat or Members.

Overview of panel discussions

Scene setting: The scale of the challenge of IoT security

Moderator: **Peter Stephens**, Policy Advisor, OECD

Panellists:

- **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

The panel discussed how the IoT, especially at the consumer level, is a broad spectrum of products and services at different price points, and that this poses challenges for effectively embedding security into this category. The conversation referred to the multiple challenges for consumers, who are not presented with key information at the point of purchase and are a broad community who engage with product information and risk tolerance in different ways. The panel recognised the need for further research and engagement with consumers so that they can better consider how an Internet-connected device (such as a camera or a door lock) could be misused.

Given the importance of data driven decision making, Shinya Tahata presented the NICTER and NOTICE projects, under which the Japanese Ministry of Internal Affairs and Communications have been investigating since 2019 on IoT devices with weak security settings and have notified consumers (via the ISP) if a product's password is especially vulnerable, such as those with repetitive or consecutive characters (e.g. '12345').

The panel discussed regulatory approaches, such as the European Union's Cyber Resilience Act, the United Kingdom's Product Security and Telecommunications Infrastructure Bill and various other regulatory initiatives, such as the SB327 (the 'California Bill'), as well as regulatory initiatives in the United States that target federal procurement of devices. Whilst the panel was pleased by these initiatives, they also stressed the important balance of minimum baseline requirements and the need to enable innovation above this threshold. Panellists also expressed concerns that, if done incorrectly, less secure products would move to more price sensitive markets, which could have a less developed capacity to cope with future cyber-attacks within the IoT.

Panellists argued that legislation should be framed as an opportunity to enable innovative practices within a more secure ecosystem, whilst also referring to the powers of distributors and vendors. They mentioned the important role of Technical Standards in reducing international friction within transactions. The panel also discussed the importance of products being built with 'ethics in mind' and encouraging shared languages between the builders and consumers of IoT products.

Policy maker approaches: Insights on IoT security in 2023

Moderator: **Constance Mougenot,** European and International Political Affairs Officer, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France

Panellists:

- **Daisuke Hoshi**, Director for International Affairs, Cyber Security Division, Ministry of Economics, Trade and Industry, Japan 3
- **Gaurav Keerthi,** Deputy Chief Executive, Cyber Security Agency of Singapore
- **Christiane Kirketerp de Viron,** Head of Unit, Cybersecurity and Digital Privacy Policy, DG CNECT, European Commission
- **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

This panel brought together leading experts in the development and delivery of policy addressing security challenges for the IoT. Members of the panel each took the opportunity to discuss current policy approaches in their jurisdictions, as well as the historic approach to developing legislation.

The panel outlined the range of approaches to addressing the issue of vulnerabilities across the IoT. These included voluntary approaches, consumer labelling initiatives, approaches that focus on federal procurement and approaches that set minimum requirements for the security of the products available on the general market, placing liability within the supply chain.

Erika Lewis presented the United Kingdom's approach of creating a Code of Practice in 2018 and then developing a series of legislative proposals and consultations so as to assess the proportionate level for legislation, and the process taken to convert this approach into the Product Security and Telecommunications Infrastructure Bill.

The panel discussed the role of monitoring and evaluating policy interventions, especially in smaller markets. Gaurav Keerthi discussed the role that Singapore, and its labelling scheme on consumer connected products, can play in helping policy makers and manufacturers better recalibrate the role of security as a potential point of difference in a crowded market.

Following on from the previous panel, the panel discussed the important need to secure a balance of fundamental baselines, so that security is not only for the most premium of products. In addition, the panel discussed the need to raise consumer awareness as to the requirements of effective security in consumer products.

The panel raised the importance of harmonisation and the potential role for Technical Standards and best practices. 2023 is a critical year for the security of the Internet of Things and this will continue as various policy approaches are implemented, and the effectiveness monitored. The panel discussed the issue of fragmentation, and the need to maintain an open conversation with policymakers, so as to learn from one another and work alongside one another towards a shared ambition on heightened cyber resilience in the sector.

Security risks in artificial intelligence

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

Panellists:

- **Vijay Bolina,** Chief Information Security Officer, DeepMind
- **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
- **Clara Neppel,** Senior Director, IEEE
- **Taylor Reynolds,** Technology Policy Director, MIT Internet Policy Research Initiative (IPRI)

The fast-paced development of Generative AI – including Large Language Models (LLM) such as ChatGPT or LLaMA, and their image-generating counterparts Midjourney and Stable Diffusion – has found its way to the centre of policy discussions with an increasing focus on the benefits of this exciting technology as well as its social, economic, and political risks. Generative AI has an immense potential to revolutionise industries and sectors including finance, healthcare, personalisation of services, law, simulation, and manufacturing. On the other hand, there are serious critical security considerations and threats accompanying the adoption of Generative AI. These risks include the creation of convincing fake content, which can be used to conduct phishing attacks, for example. Furthermore, adversarial attacks on Generative AI involve exploiting vulnerabilities in AI systems to manipulate or deceive them by changing input data to produce incorrect results or misclassifying information.

The session discussed the key security considerations for policymakers and whether some of the lessons learned from broader security policy work in emerging technologies can be applied to the AI space. Panellists agreed that at a foundational level, there are significant intersections between traditional system security, privacy engineering, and security in Generative AI systems. Hence, it is imperative for AI security experts to possess a comprehensive understanding of both the foundational concepts of machine learning and the various potential attack surfaces that AI systems may encounter throughout their development and deployment phases.

The panel also touched upon the need for ongoing research and development to ensure that AI systems are secure, reliable, and explainable by referring to the 'black box problem' – the difficulty to understand the internal workings of complex machine learning models. Moreover, the panellists discussed ways the private sector, academia, and standard-setting associations could work together to achieve better outcomes.

The Q&A session allowed the audience to share their perspectives and different ideas of what automated, trustworthy, explainable AI security means. A recurring theme was the role of standards in rating AI systems based on potential information vulnerability to criminal influences, particularly related to privacy and property.

The panel concluded by listing the lessons learned from other technology policies in the public and private sectors that can best transfer to the current era of IoT and AI-enhanced devices. Panellists agreed that distinguishing between risks to personal information and risks to personal property is crucial, but classifying and measuring these risks effectively is challenging, especially considering future uncertainties. To foster transparent communication, it is essential for businesses, governments, and technical standards organisations to ensure that consumers are informed about the handling of their data.

Policy responses to security challenges in artificial intelligence

Moderator: **Karine Perset,** Head of AI Unit, OECD

Panellists:

- **Amit Elazari**, Director of Global Cybersecurity Policy, Intel
- **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

The rapid progress and implementation of AI systems underline the need for a stable policy environment that promotes secure, safe, and trustworthy AI. Furthermore, the complex challenges of AI and IoT require a multifaceted approach, involving secure IoT management, vulnerability reporting programs, and the advancement of security standards. Therefore, governments, organisations, and stakeholders need to take steps in a collaborative manner and build on their best practices to mitigate security risks as they develop, deploy, or operate AI-based systems. Moreover, it is crucial that they apply systematic risk management approaches to each phase of the AI system lifecycle on a continuous basis. The panel provided the opportunity to discuss existing national policy practices as well as international initiatives and frameworks, new approaches, and potential next steps.

Approaches to AI risk are currently being evaluated across governments and international organisations with a focus on recognising and regulating the application of technology, including generative AI, while complying with democratic values, human rights, and the rule of law. Governance and security by design are prioritised, alongside the need for broader discussions encompassing security, political education, and disinformation. Efforts are underway at the Council of Europe, the European Commission, the OECD, UNESCO, and the United Nations to address these critical aspects of AI governance and actively promote effective solutions through the analysis of AI developments. Additionally, multistakeholder expert groups play a crucial role in assisting policymakers in understanding technological advancements and promoting risk measures to ensure the safe development and use of AI. The panel also discussed the importance of interoperability among diverse risk management frameworks, the use of practical tools and metrics, and evidence-based policy development through monitoring AI incidents.

One speaker called for mechanisms to address unintended consequences in AI, suggesting vulnerability disclosure programs, while also highlighting the need for supporting the research community in addressing underlying vulnerabilities. An additional intervention emphasised the concept of security by obscurity and advocated addressing automated disinformation and fostering trust in the digital realm. A third speaker highlighted the multi-stakeholder approach in developing AI instruments and standards, underlying collaboration between organisations, and the importance of protecting human rights and democracy. Additionally, academic institutions were identified as key players in AI development, with a focus on integrating ethics into education, fostering interdisciplinary skills, and serving as trusted stakeholders for policymakers, while also addressing societal and security risks in AI research and promoting collaboration with corporations.

During their final statements, panellists agreed that principles should be translated into practical implementation and underlined the significance of including and empowering users, particularly individuals and marginalised communities, in AI discussions. The interventions also stressed the need for international regulatory approaches, multi-stakeholder engagement, and interoperability. Lastly, panellists reiterated the need for resolving conflicts between principles to navigate complex dilemmas in AI, highlighting the importance of appropriate global entities assuming this responsibility.

Policymaking in security: Effectively working with security agencies across emerging technologies

Moderator: **Audrey Plonk**, Head of Digital Economy Policy Division, OECD

Panellists:

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

This panel brought together decades of experience leading policy at the highest levels of government, as well as experience leading the security community and its movements to contribute more actively to policymaking.

The panel discussed the varying approaches to digital security policymaking in the United Kingdom, France and the United States. Whilst the organisational structures differed, all panellists agreed on the critical role of partnerships between the technical, advisory and policy communities in their shared endeavours of designing and delivering better policies for citizens. The panel also discussed incident response and how the technical community plays a critical role in building resilience and developing policy approaches. The panel opined that the role of incident responders would become intertwined with policy makers and the inputs and knowledge of incident responders would be extremely valuable to address national security, public safety and economic prosperity.

The panel discussed the changing relationship between governments and the security research (also known as the 'hacker') community. Audience members learned about the growing role of the DEF CON hacker conferences, held in Las Vegas since 1993. As the conferences grew, the communities directly engaging within security have broadened. Most recently, the decision of governments to apply regulation have galvanised the security research community to seek opportunities to engage with public policy makers. Regarding emerging technologies such as IoT, the panel concurred that policy makers should prioritize responses to IoT vulnerabilities based on the strategic impact they pose to individuals, organizations, and society.

The panel discussed the breadth of communities involved in public policy making across security, and the need to 'speak multiple languages' across academia, civil society, industry, incident responders, policymakers, and security researchers. The issues faced by policymakers are fundamentally global in nature. Panellists recognised regulation was a necessary lever to address market failure.

The panel also referred to longer term challenges in training, skills and recruitment across the digital security workforce and the need to address these issues to sustain progress in addressing future risks. The panel also discussed the important role of security researchers and penetration testers, and the desire to provide more support for them.

Building bridges between the security research and policy communities

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

Panellists:

- **Jen Ellis,** Founder, NextJenSecurity
- **Harley Geiger,** Counsel, Venable LLP
- **Sebastian Hallensleben,** Chair, CEN CENELEC JTC21
- **Amélie Koran**, Director, External Technical Relations at Electronic Arts
- **Kirsty Paine**, Strategic Advisor, Splunk
- **Beau Woods**, Cyber Safety Advocate, I am the Cavalry

This panel brought together experts across the security community, each of whom have direct experience leading engagements and advising the work of policymakers and Technical Standards bodies across digital security.

The panel disused the ubiquitous nature of security for the digital economy and the need for it not to be seen as a 'niche' concern. Global events, such as NotPetya, WannaCry, Mirai and Russia's invasion of Ukraine have helped to focus attention on digital security, but there was still a spectrum of opinions among policy makers around the world.

The panel was keen to stress that security within the digital economy should not be seen solely as a technical concern, but that it also relied on effective partnerships and the importance of shared communication and openness to new ideas, from policy makers and from members of the security research community.

The panel mentioned the importance of openness within policy and security communities, and expressed a recognition and respect that it can be difficult for experts in one field to properly understand how valuable their experience is. The panel discussed the importance of 'breaking out of (our existing) bubbles', whether they be in security or policy, so as to find ways to understand new perspectives to the security challenges faced in the digital economy. Community events, such as the Global Forum on Digital Security for Prosperity, Cyber UK or DEF CON were highlighted as examples of community events to allow policymakers to build relationships and future partnerships with this community.

As a longer-term solution, the panel followed up on the previous panel by highlighting the need to inform curriculum design so that the future workforce is better prepared to face digital security challenges.

The panel discussed changing attitudes towards safe harbour and security research. The panel focused on the criticality of vulnerability research and coordinated vulnerability disclosure, and the risks associated with mandating a particular mechanism through which vulnerabilities would be disclosed.

The panel raised the important role of Technical Standards in addressing fragmentation, but also in offering a space, beyond community events, to allow dialogue and partnerships between the technical and policymaking 'bubbles'.

The Global Forum on Digital Security for Prosperity in 2024

The 2024 annual event of the Global Forum on Digital Security for Prosperity will be hosted in partnership with Korea. The specific dates and location are to be determined.