GENEVA DIALOGUE
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

How can we strengthen global collaboration for developing trustworthy supply chains and secure digital technologies?

Join leading company and government representatives in a conversation on how we can enhance digital trust and cooperation to reset our economies after COVID-19!

Digital Security and Economic Recovery: Boosting Confidence and Productivity through Secure Digital Technology

Thursday, 26th November 2020, 7:30–9:00am UTC / 08:30–10:00am CET

Introduction

Keynote speech by **Federal Councillor Ueli Maurer**,
Head of the Federal Department of Finance FDF, Switzerland

Panel discussion

Ms Sabine Keller-Busse, *Member of the Group Executive Board, UBS AG*
Mr Eugene Kaspersky, *CEO, Kaspersky*
Mr Jeremy Thompson, *Executive Vice President, Huawei Western European Region*
Mr Casper Klynge, *Vice President, European Government Affairs, Microsoft Corporation*

Moderator:

Mr Jovan Kurbalija, *Founding Director, DiploFoundation and Head, Geneva Internet Platform*

Register for the event at:
https://www.diplomacy.edu/calendar/digital-security-and-economic-recovery

Speakers

Federal Councillor Ueli Maurer, Head of the Federal Department of Finance FDF, Switzerland
Federal Councillor Ueli Maurer has twice served as President of the Swiss Confederation, in 2019 and 2013. He has been the Head of the Federal Department of Finance since 2016. Earlier, Federal Councillor Maurer headed the Federal Department of Defence, Civil Protection and Sport DDPS from 2009 until 2015.

Ms Sabine Keller-Busse, Member of the Group Executive Board, UBS AG, and Group Chief Operating Officer and President UBS Europe, Middle East and Africa
Ms Sabine Keller-Busse was appointed Group Chief Operating Officer of UBS Group AG and UBS AG as well as President of the Executive Board of UBS Business Solutions AG in 2018. In addition, she was appointed President UBS Europe, Middle East and Africa in October 2019. She was Group Head Human Resources from 2014 to 2017. Ms. Keller-Busse became a member of the GEB in 2016. Having joined UBS in 2010, she served as Chief Operating Officer UBS Switzerland until 2014. Prior to that, she led Credit Suisse's Private Clients Region Zurich division for two years. From 1995 to 2008, she worked for McKinsey & Company, where she was a Partner from 2002. Ms. Keller-Busse holds a PhD and a master's degree, both in business administration, from the University of St. Gallen.

Mr Eugene Kaspersky, CEO, Kaspersky
Mr Kaspersky is a world-renowned cybersecurity expert and successful entrepreneur. He is a co-founder and the Chief Executive Officer of Kaspersky, the world's largest privately-held vendor of endpoint protection and cybersecurity solutions. Mr Kaspersky began his career in cybersecurity accidentally when his computer became infected with the 'Cascade' virus in 1989. Mr Kaspersky's specialized education in cryptography helped him analyze the encrypted virus, understand its behavior, and then develop a removal tool for it. After successfully removing the virus, Mr Kaspersky's curiosity and passion for computer technology drove him to start analyzing more malicious programs and developing disinfection modules for them. This exotic collection of antivirus modules would eventually become the foundation for Kaspersky's antivirus database. In 1997 Kaspersky was founded, with Mr Kaspersky heading the company's antivirus research. In 2007 he was named Kaspersky's CEO.

Mr Jeremy Thompson, Executive Vice President, Huawei Western European Region
Mr Thompson oversees the development of Huawei's business in Western Europe with a focus on security. This includes aligning Huawei's strategic development activities and security capabilities with key customers and European Governments. Mr. Thompson joined Huawei UK in 2012 as Deputy Managing Director with specific responsibility for carrier strategy, business change and the key customers. In 2015 he was based in Shenzhen, China. This role included supporting the development of Huawei's carrier strategy globally and strategy development in Asia, Europe and South America. Prior to Huawei, Mr. Thompson worked for 20 years in senior management roles for BT Group in the UK, Spain and the Nordics. Mr. Thompson previously worked in the USA and UK for an IBM Software company and consulting businesses. He is a British citizen and attended University of London, London Business School and University of Greenwich.

Mr Casper Klynge, Vice President, European Government Affairs, Microsoft Corporation
Mr Klynge is Microsoft's Vice President for European Government Affairs with responsibility for all of Microsoft's government affairs and public policy work across the continent. He serves on the senior leadership team of Microsoft's CELA group. Prior to joining Microsoft, Mr. Klynge most recently served as Denmark's (& the world's first) Ambassador to the global tech industry. Previous posts include: Ambassador to Indonesia, Timor Leste, Papua New Guinea & ASEAN (2014-2017), Ambassador to the Republic of Cyprus (2013-2014), Deputy Head of NATO's Provincial Reconstruction Team in Helmand Province, Afghanistan & Head of Mission of the EU's civilian crisis management planning mission in Kosovo (2006-2008). Mr. Klynge holds a M.Sc. in Political Science and is a 2009 Marshall Memorial Fellow.

Mr Jovan Kurbalija, Founding Director, DiploFoundation and Head, Geneva Internet Platform (GIP)
Dr Kurbalija is the Founding Director of DiploFoundation and Head of the Geneva Internet Platform (GIP). He was a member of the UN Working Group on Internet Governance (2004–2005), special advisor to the Chairman of the UN Internet Governance Forum (2006–2010), and a member of the High Level Multistakeholder Committee for NETmundial (2013-2014). During 2018–2019, he served as Co-Executive Director of the Secretariat of the United Nations (UN) High-level Panel on Digital Cooperation. A former diplomat, Kurbalija has a professional and academic background in international law, diplomacy, and information technology. His book, An Introduction to Internet Governance, has been translated into nine languages and is used as a textbook for academic courses worldwide.

Background

Malicious activities in cyberspace are a significant drag on the global economy. A 2018 assessment by the US government estimated that cyber incidents are likely to have cost the US economy up to USD$106 billion in 2016, amounting to about 0.5% of GDP. Furthermore, cyber-attacks and security deficiencies in digital products undermine trust in digital technologies. As a result, delays in employing productivity-enhancing technologies throughout the economy are often an unfortunate, but regular occurrence. At the same time, the COVID-19 pandemic has made the need to adopt digital solutions and their crucial value for the global economy all the more clear. As highlighted by the UN Secretary General in his Roadmap for Digital Cooperation, issues of trust and security need to be addressed in order to reap the benefits of the digital transformation and for reaching the UN Sustainable Development Goals. This is a fundamental discussion to be held among all stakeholders, but one of particular importance to private sector investors, without whose confidence the global digital agenda will face significant hurdles.

The majority of cyber-attacks exploit vulnerabilities in digital products and services. Although there is a lively international debate about the responsibility of governments to establish baseline requirements for cybersecurity, and for manufacturers and service suppliers to apply the available standards, there is currently no consensus about these issues. Hence, there is a risk that governments set widely different requirements, while businesses pursue divergent industry practices.

In this context, the Geneva Dialogue on Responsible Behavior in Cyberspace has been discussing industry roles and responsibilities throughout 2020, with the aim to establish globally shared best practices and baseline requirements for the security of digital products and services. An output document, which includes definitions of key concepts and a collection of good corporate practices about threat modelling, supply chain security, secure development, vulnerability management, and transforming internal processes to embrace security by design, has been published for comments.

This high-level event will discuss how the fragmented regulatory environment impacts the security of digital products and services, including those in supply chains. It aims to clarify possible collaborative responses from both industry and governments on how to facilitate financial and economic recovery through trusted digital technologies.

Thematic coverage

The event will address the following questions:

- How can governments and corporations work together to strengthen the digital economy and accelerate the post-COVID-19 economic recovery?
- How can governments and businesses make trustworthy and secure digital technologies a central pillar for reviving the post-pandemic economy?
- How does the fragmented regulatory environment impact the security of digital services, including those in supply chains?
- Will corporations and governments be able to work together in creating common requirements for the security of digital products by harmonizing good corporate practices and existing standards, regulatory requirements, and global principles?
- What capacities need to be strengthened within the public and private sectors to enable (such) joint efforts?

For more information on the Geneva Dialogue on Responsible Behaviour in Cyberspace, please visit **https://genevadialogue.ch/**

The event is hosted by DiploFoundation and the Swiss Confederation.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

DiPLO
www.diplomacy.edu