# EU CYBER FORUM

14-17 September 2020

## Why the EU Cyber Forum?

Over the past years, cyber-related policy issues have become a permanent feature on the meeting agendas of European leaders with third countries. With the increased focus on **digital transition** and the relevance of the EU's cyber and digital policies in support of the **Geopolitical Commission**, the EU's diplomatic, economic and political actions attract international attention and scrutiny. As stated in the Commission Work Programme, a strong EU voice expressing our commitment to upholding, updating and upgrading the **rules-based global order** requires a more focused, open and proactive approach, including in our global engagements on cyber and digital issues.

To support these objectives and to deepen the EU's global engagement with various stakeholder communities and our strategic partners around the world, the European Union Institute for Security Studies (EUISS) and partners are organising the **EU Cyber Forum (14-17 September 2020, Brussels)** for the second consecutive year. Due to the COVID-19 related travel restrictions, this year's conference will be a blended event combining a limited physical presence and online engagement.

The EU Cyber Forum is a **platform for showcasing the European Union's efforts in a broadly defined area of cyber and digital policies**, while at the same time allowing for the exchange of best practices between participating countries. Organised in cooperation with the European External Action Service, the European Commission, the European Union Agency for Cybersecurity – ENISA, and the European Cybercrime Centre at Europol, the first edition of the Forum brought together over 150 individuals representing around 60 countries and different stakeholder communities.

## About EU Cyber Direct

The EU Cyber Direct project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through dialogues with strategic partner countries and regional/international organisations. EU Cyber Direct is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

# Draft Agenda

All times in CEST (UTC +2)
*Speakers to be confirmed

## 14 September 2020

| | |
|---|---|
| 10:20-10:30 | Welcome remarks |
| | **Gustav LINDSTROM**, Director, EU Institute for Security Studies |
| 10:30-10:45 | Keynote address |
| | **Cyber diplomacy and shifting geopolitical landscapes** |
| | **Josep BORRELL FONTELLES** EU High Representative for Foreign Affairs and Security Policy and Vice-President of the European Commission |
| 10:45-11:00 | Health break |
| 11:00-12:00 | Panel discussion |
| | **Digital society after COVID-19: building a global cyber resilience regime** |
| Chair | **Eneken TIKK**, Cyber Policy Institute, Finland |
| Speakers | **Juhan LEPASSAAR**, Executive Director, EU Agency for Cybersecurity (ENISA) |
| | **Gwenda FONG**, Assistant Chief Executive, Cyber Security Agency of Singapore |
| | **Katherine GETAO**, CEO, Information and Communications Technology Authority, Kenya |
| | **Shariffah Rashidah SYED OTHMAN,** Malaysian Administrative Modernisation and Management Planning Unit, Malaysia |
| | **Lise FUHR**, Director General, European Telecommunications Network Operators' Association (ETNO), Belgium |
| 12:00-13:30 | Health break |

| 13:30-14:30 | Panel discussion: |
| | **Preventing conflicts in cyberspace: navigating a multiconceptual world** |
| Chair | **Joyce HAKMEH**, Senior Fellow, Chatham House |
| Speakers | **Joanneke BALFOORT**, Director, Security and Defence Policy, European External Action Service |
| | **Guilherme PATRIOTA**, Chair of the UN Group of Governmental Experts, Brazil |
| | **Johanna WEAVER**, Assistant Secretary of Cyber Policy at the Australian Department of Foreign Affairs and Trade |
| | **Latha REDDY**, Co-Chair, Global Commission on Stability in Cyberspace, India |
| 14:30-15:30 | Health break |
| 15:30-16:30 | Panel discussion |
| | **Global efforts to counter cybercrime: leveraging commonalities, bridging differences** |
| Chair | **Nayia BARMPALIOU**, Head of Public Policy and Initiatives, Centre for Cybersecurity, World Economic Forum |
| Speakers | **Michael DANIEL,** President, Cyber Threat Alliance, United States |
| | **Olivier ONIDI**, Deputy Director-General, Directorate General Home Affairs, European Commission |
| | **Albert ANTWI-BOASIAKO**, National Cybersecurity Advisor, Ministry of Communications, Ghana |
| | **Alexander SEGER**, Head, Cybercrime Division, Council of Europe |

# Panel discussions and working sessions

## 15 September 2020

| | |
|---|---|
| 13:00 – 14:00 | Panel discussion |

**Navigating the world of data diplomacy**

*Data – both personal and non-personal - is at the core of digital transformation. It is an essential resource for economic growth and competitiveness. The EU aspires to lead in data-driven innovation by setting clear rules on data access and use. But given the importance of free data flows for global economy, it is clear that rules set in any part of the world have implications for other countries. The focus of this session is on exploring the consequences of these policies for the global economy, how to harness the opportunities, and navigate potential political tensions.*

| | |
|---|---|
| Chair | **Joanna ŚWIATKOWSKA**, Senior Research Fellow of the Kosciuszko Institute; University of Science and Technology, Cracow, Poland |
| Speakers | **Khalil ROUHANA**, Deputy Director General, European Commission, Communications Networks, Content & Technology |
| | **Teki AKUETTEH FALCONER**, Founder and Executive Director of Africa Digital Rights Hub, Ghana |
| | **ZHANG Jian,** Assistant President and the Director of Institute of European Studies, China Institutes of Contemporary International Relations (CICIR), China |
| | **Chizuru SUGA**, Head of the World Economic Forum Centre for the Fourth Industrial Revolution Japan, World Economic Forum, Japan |

| | |
|---|---|
| 14:30 – 15:45 | Working session (in cooperation with ENISA) |

**Cybersecurity certification: EU and global outlook**

*Securing network and information systems is a key to keep the online economy functional and secure. Failure to do so could have far-reaching consequences for citizens and threaten to affect citizen trust, industry, and public administration. This is why the EU and governments around the world are considering cybersecurity certification frameworks as a potential solution to establish and maintain the trust and security on cybersecurity products, services and processes. At the same time, the market of ICT products and services is global and there are market considerations to address. The purpose of this session is to explore how cybersecurity certification efforts contribute to establishing sustainable international partnerships committed to the rules-based global order.*

| | |
|---|---|
| Chair | **Andreas MITRAKAS**, Head of Certification Unit, ENISA |
| Speakers | **Katerina MEGAS**, Commercial Adoption Lead for the Trusted Identities Group & Program Manager for the Cybersecurity for Internet of Things (IoT), National Institute of Standards and Technology, United States |
| | **Aristotelis TZAFALIAS,** Cybersecurity and Digital Privacy Policy, Directorate-General Communications Networks, Content & Technology, European Commission |
| | **Warna MUNZEBROCK**, Radiocommunications Agency, Ministry of Economic Affairs and Climate Policy, The Netherlands |
| | **Soshi HAMAGUCHI,** Manager, Cosmos Corporation, Japan |
| | **Alberto DI FELICE**, Infrastructure, Privacy and Security, DigitalEurope |

| | |
|---|---|
| 16:00 – 17:00 | Panel discussion |

### Building a cyber-proof digital government

*Successful digital transition is the key to building resilient societies of the future. The use of eGovernment services - ranging from e-procurement, filling tax returns, to applying for social benefits - has increased since the outbreak of COVID-19. Effective eGovernment can provide a wide variety of benefits well beyond the current crisis, including more efficiency and savings for governments and businesses, increased transparency, and greater participation of citizens in political life. However, as digital societies become reality (e-health, e-government, e-democracy, etc.), new vulnerabilities emerge. This session will examine how to create eGovernment services that take full advantage of its potential and are also cyber secure.*

| | |
|---|---|
| Chair | **Ian WALLACE**, Senior Fellow, Digital Innovation and Democracy Initiative, German Marshall Fund of the United States |
| Speakers | **Tomicah TILLEMANN,** Director Digital Impact and Governance Initiative and Blockchain Trust Accelerator, New America, United States |
| | **Nicolás Pascual DE LA PARTE**, Ambassador for Hybrid Threats and Cybersecurity, Ministry of Foreign Affairs, Spain |
| | **Rama VEDASHREE,** CEO, Data Security Council, India |

# 16 September 2020

| 13:00 – 14:00 | Panel discussion |
| | |

## New era of digital and cyber alliances

*Progressing digital transition worldwide implies that societies and economies become increasingly dependent on complex value chains spanning across the world and beyond the control of a single actor. At the same time, different interests and value systems that underpin the existing models of cooperation result in new political tensions in areas that used to be considered purely technological. That has led some countries to conclude that they need to develop their own digital autonomy and cybersecurity measures independently. New ideas such as a new grouping of digital powers and companies (D20) or a proposal for a 5G alliance to reduce dependency on China are just a few examples.*

Chair **Patryk PAWLAK,** Brussels Executive Officer, EU Institute for Security Studies

Speakers **Lorena BOIX ALONSO**, Director, Policy Strategy and Outreach, Communications, Networks, Content & Technology, European Commission

**Samir SARAN**, President, Observer Research Foundation, India

**Casper KLYNGE**, Vice President, European Government Affairs, Microsoft

**Nanjira SAMBULI**, The Ford Global Fellow

**Abraham NEWMAN**, Director, Mortara Center for International Studies, Georgetown University, United States

| 14:30 – 15:30 | Panel discussion |

## Strengthening accountability in cyberspace

*Cyber-attacks and disinformation by malicious actors undermine stability and the proper functioning of our societies. The purpose of this session is to take stock of how to counter such activities and what other options exist – at diplomatic, legal and political levels – to make those responsible for such actions more accountable.*

Chair **Camino KAVANGH**, Visiting Senior Fellow, King's College London, United Kingdom

Speakers **Carmen GONSALVES**, Head of International Cyber Policy. Ministry of Foreign Affairs, The Netherlands

**Gerardo Isaac MORALES TENORIO**, Deputy Director General for Multidimensional Security, Ministry of Foreign Affairs, Mexico

**John SCOTT-RAILTON**, Senior Researcher, The Citizen Lab, University of Toronto, Canada

**Marietje SCHAAKE**, President, Cyber Peace Institute, Switzerland

| | |
|---|---|
| 16:00 – 17:30 | Working session (in cooperation with the European Cybercrime Centre)<br><br>**New trends in cybercrime and the future of international cooperation**<br><br>*Numerous reports by law enforcement and intelligence agencies highlight the evolving nature of cybercrime. Therefore, an effective international cooperation between the governments – and with the private sector – is essential. This session will analyse the current operational, political and legal approaches to fighting cybercrime and stress key elements needed for an effective international cooperation against cybercrime in the future.* |
| Chair | **Edvardas ŠILERIS,** Head, European Cybercrime Centre (EC3), Europol |
| Speakers | **Greg DAY**, VP & Chief Security Officer, EMEA, Palo Alto Networks, UK<br><br>**Cathrin BAUER-BULST**, Head of Unit, European Commission<br><br>**Tim DAVIS**, Joint Cybercrime Action Taskforce (JCAT) and Australian Federal Police, Australia<br><br>**Fernanda TEIXEIRA SOUZA DOMINGOS**, Cybercrime Supporting Group Coordinator, Federal Prosecutor, Government of Brazil<br><br>**Camila BOSCH CARTAGENA**, Lawyer, Money Laundering, White Collar, Environmental, Cyber and Organized Crimes Unit, Public Prosecution Office, Government of Chile |

## 17 September 2020

| | |
|---|---|
| 13:00 – 14:30 | Working session<br><br>**International security and emergency response cooperation**<br><br>*Over the past years, we have seen, on one hand, an increase in complexity and sophistication of cyber attacks and the increasing need for international cooperation among the computer incident response teams, on the other. However, such cooperation has often suffered due to the growing political and economic motivation behind the attacks, including with the involvement of state actors. The evolution of the threat landscape during the COVID-19 pandemic is just but one illustration of this trend. The focus of this session will be on looking into the evolving role of the CERT/CSIRT community in international cyber discussions, their cooperation mechanisms and possible methods for improvement in such an increasingly politicised context.* |

| | |
|---|---|
| Chair | **Louis Marie HUREL**, Igarape Institute, Brazil |
| Speakers | **Saad KADHI,** Head, CERT-EU, Belgium |
| | **Cristine HOEPERS**, General Manager, CERT.br, Brazil |
| | **Yukako UCHIDA**, Manager, Global Coordination Division, Japan<br>Computer Emergency Response Team Coordination Center (JPCERT/CC) |
| | **Maarten VAN HORENBEECK**, Board Member, FIRST, United States |
| | **Kaleem USMANI,** Head of operations, CERT-MU, Mauritius |
| | **Klee AIKEN,** CERT New Zealand |
| | **Jean-Robert HOUNTOMEY**, Executive Director, Global Coordination, AfricaCERT |
| 15:00 – 16:30 | Working session (in cooperation with European Commission, DG Home)<br><br>**Internationalising (critical) infrastructure and functions protection**<br><br>*Protection of critical infrastructure and functions is an objective that features prominently in the international discussion about cyber norms and confidence-building measures. However, the conversation among cyber diplomats rarely reflects the realities on the ground and the challenges faced by the operators. The purpose of this working session is to compare notes between these two groups of stakeholders in order to identify common areas of interest and investigate how the innovation and research undertaken in the area of critical infrastructure protection can be leveraged to address the challenges to international security cooperation.* |
| Chair | **Max BRANDT**, Directorate General for Home Affairs, European Commission |
| Speakers | **Mary MCGINLEY**, Strategic Mission Director, Physical and Cyber Security, Department of Homeland Security (DHS), Science and Technology Directorate, United States |
| | **Clement FUGGINI**, RINA, Italy |
| | **Mihoko MATSUBARA,** NTT, Japan |
| | **Joanna KULESZA**, Professor, Faculty of Law and Administration, University of Lodz, Poland |
| | **Caitirona HEINL**, Executive Director, The *Azure* Forum for Contemporary Security Strategy, Ireland |

# Side events

| | |
|---|---|
| 14-17 September | Virtual EU Cyber Expo<br><br>*The aim is to create a one-stop-shop virtual space where participants of the EU Cyber Forum will have a chance to learn about various ongoing EU initiatives and projects around the world.* |

## 17 September

13:00 – 14:30      **Civil Society Cyber Forum**

*Civil society organisations are an important partner in the design and implementation of cyber-related policies and initiatives. This year's Civil Society Cyber Forum will provide an opportunity for exchanges on the role of the EU in shaping the global cyber, digital and technology landscape. Representatives of civil society will share their inputs that later will be integrated in the official Forum report.*

15:00 – 16:30      **Youth Cyber Forum**

*Younger generations grew up with the internet and computers, are frequent users of social media, more tech-savvy than previous generations and offer unique insights into cybersecurity challenges. However, they find themselves only on the margins of cyber diplomacy and policy debates. How do younger generations from various global regions experience digitalization? What do they identify as the most urgent policy priorities? And how can we create more awareness about these issues among younger generations and increase their engagement in the policy debate? During this session youth (ages 18-25) from Europe, the United States, Asia, Latin-America and Africa will share their views and experiences.*