EU CYBER FORUM

EU CYBER DIRECT

15-16 April 2019, Brussels, Belgium

The Residence Palace, Rue de la Loi 155, Brussels, Belgium

Why the EU Cyber Forum?

Over the past years, cyber-related policy issues – such as building cyber resilience, the fight against cybercrime, or stability in cyberspace – have become a permanent feature on the agendas of meetings between European policymakers and partners from around the world. This is not surprising given that the European Union is one of the key actors in shaping the regulatory and institutional landscape in this domain. At the same time, however, the EU's role, its policies and institutional set up are still poorly understood in other parts of the world. Consequently, the EU Cyber Forum will provide a platform where different EU actors and partner countries will have an opportunity to engage in an effort to gain a better understanding of their respective cyber policies, share best practices, and explore concrete ways of cooperating in the cyber domain.

What is the added value?

Organised in cooperation with the relevant services of the European Commission and the European External Action Service (EEAS), the EU Cyber Forum will bring together all relevant EU actors, including the European Cybercrime Centre (EC3) at the Europol and the European Union Agency for Network and Information Security (ENISA). This will ensure that the agenda of the Forum remains policy relevant and feeds directly into the policy dialogues and cooperative arrangements that the EU pursues with partner countries. At the same time, the 'Cyber Expo' that accompanies the Forum will give the partner countries a chance to obtain information about concrete EU-funded external projects and initiatives with a cyber focus. The EU Cyber Forum will bring together 120-150 international experts from governments, the research community and the private sector to discuss issues along three pillars: cyber security, cybercrime and justice, and cyber diplomacy.

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 extensive 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.

This event is co-organised with

European Union EXTERNAL ACTION

European Commission

ISS European Union Institute for Security Studies

Implementing organisations

G | M | F The German Marshall Fund of the United States STRENGTHENING TRANSATLANTIC COOPERATION

Stiftung Neue Verantwortung

This project is funded by the European Union.

Agenda

15 April 2019

08:30-9:15 Registration and coffee

09:15-09:30 Welcome

Gustav Lindstrom
Director, EU Institute for Security Studies

09:30-09:45 Opening remarks

Despina Spanou
Director for Digital Society, Trust and Cybersecurity, Directorate-General Communications Network, Content and Technology, European Commission

09:45-10:30 Introductory talk

International law in cyberspace: does it exist and do we need it?

Whereas the UN in its resolutions has accepted that the existing international law applies also in cyberspace, many observers of this debate still raise the questions about 'how' the existing international law applies. Consequently, the focus of this session is to clarify some of the key questions linked to binding rules and norms of state behaviour in cyberspace.

Chair **Eneken Tikk**
Head of normative, power and influence studies, Cyber Policy Institute

Speaker **Martti Koskenniemi**
Director, Erik Castrén Institute of International Law and Human Rights, University of Helsinki, Finland

10:30-11:00 Coffee break

11:00-12:30 Panel discussion

Societal cyber resilience and multi-stakeholder cooperation

It is often stressed that building resilience in cyberspace requires the involvement of governments, the private sector and civil society organisations. This multi-stakeholder approach has been consistently supported and promoted by the European Union. However, the growing complexity of the cyber-related challenges and the increasing number of actors required for an effective policy response are challenging traditional models of cooperation. This session will be an opportunity to share good practices and lessons learned from past and ongoing initiatives.

Chair **Lea Kaspar**
Executive Director, Global Partners Digital, United Kingdom

Speakers **Nayia Barmpaliou**
Head of Public Sector, Centre for Cybersecurity, World Economic Forum, Switzerland

Frédérick Douzet
Chairwoman, Castex Chair of Cyberstrategy, Institute for Higher National Defence Studies, France

Gregory Mounier
Head of Outreach and Prevention, European Cybercrime Centre, Netherlands
Gbenga Sesan
Executive Director, Paradigm Initiative, Nigeria
Bárbara Simão
Researcher in telecommunications and digital rights, Brazilian Institute of Consumer Defense, Brazil

12:30-13:30 Lunch

13:30-14:45 Panel discussion

National cyber resilience and international cooperation

Strengthening national resilience is a universally acknowledged goal. However, the solutions adopted by individual countries and regions are not always compatible. Recognising that state institutions play a key role in building a healthy economy, ensuring the security of their citizens and proper functioning of the institutions (all within the existing normative frameworks and international law), the purpose of this session is to discuss the challenges that governments face in performing these functions.

Chair **Joanna Kulesza**
Assistant Professor, Faculty of Law and Administration, University of Lodz, Poland

Speakers **Albert Antwi-Boasiako**
National Cyber Security Advisor, Ghana
Robert Collett
Senior Adviser and GFCE Liaison, Foreign and Commonwealth Office, United Kingdom
Marvic Leonen
Justice, Supreme Court of the Philippines
Mary Jane Lau Yuk Poon
Parliamentary Counsel, Attorney General's Office, Mauritius
Steve Purser
Head of Core Operations, ENISA

14:45-15:15 Coffee/Tea break

15:15-16:45 Breakout sessions

Session I
Room Maelbeek

IoT cybersecurity and consumers rights. Supply chain integrity-related threats

Security and privacy by design/by default are until now mostly aspirations in the discussions about IT services, systems and devices, including the Internet of Things (IoT). Consequently, consumers are increasingly concerned about the security and privacy of their devices. While the general need for the safety of products and services is already well understood and guaranteed through legislation providing consumer protection, the state of play regarding the cybersecurity of IoT devices is far from ideal. In addition, the need for cybersecurity standards for critical information infrastructure and the challenges linked to the issues of supply chain integrity have now opened new debates.

With systems relying on a large number of software and hardware components, designed and manufactured by different parties spread all over the world, supply chain integrity is a requirement that needs to be re-visited. The purpose of this panel is to discuss these issues and reflect on the potential contribution of the certification framework provided in the EU Cybersecurity Act.

Chair **Steve Purser**
Head of Core Operations, ENISA

Speakers **Jan-Peter Kleinhans**
Stiftung Neue Verantwortung, Germany

Rob van Kranenburg
Founder, Council of IoT, Belgium

Ikuo Misumi
Deputy-Director General for Cybersecurity and Information Technology, Ministry of Economy, Trade and Industry, Japan

Ursula Pachl
Deputy Director General, The European Consumer Organisation

Miguel Gonzales Sancho Bodero
Head of Unit, Cybersecurity Technology and Capacity Building, European Commission

Rama Vedashree
Chief Executive Officer, Data Security Council of India (DSCI)

Session II Trends in countering cybercrime

Room Polak

Given that cyber criminals disregard borders and have established criminal networks in specific jurisdictions to strike at victims around the globe, there is a significant need for greater cooperation and collaboration within the law enforcement community, as well as with other relevant public and private sector organisations. The EU has developed an innovative cooperation model with the establishment of the European Cybercrime Centre which allows EU member states and third party countries to coordinate complex cross-border cybercrime investigations. However, many questions still remain: what are the new challenges linked to cybercrime and are the existing models of international cooperation fit to address them? What bilateral and multilateral cooperation models exist that contribute to the establishment of the necessary level of trust between states to coordinate sensitive cross-border cybercrime operations?

Chair **Nathalie van Raemdonck**
Associate Analyst, EU Institute for Security Studies

Speakers **Teki Akuetteh Falconer**
Founder and Executive Director, Africa Digital Rights’ Hub, Ghana

Alex Uriel Durán Santos
Head of the Cyber Center, Colombia

Jan Kerkhofs
Federal Magistrate, Federal Prosecutor’s Office, Belgium

Graham Willmott
Head of Unit for Cybercrime, Directorate-General Home Affairs, European Commission

Steven Wilson
Head, European Cybercrime Centre, Europol

Session III
Room Passage

Free, fair and secure elections – a new task for cyber diplomacy?

One of the main objectives of the EU's cyber diplomacy is to promote a free, open and secure cyberspace through multi-stakeholder engagement. Despite the obvious overlap between this objective and the focus on free, fair and secure elections, the latter is rarely discussed among cyber diplomats, despite potential for backlash for online freedom and security. Already now, several governments use election interference and disinformation as a pretext to silence their political opponents and limit freedom of expression online. The focus of this session is to identify ways through which these two debates can be linked and on the roles that different actors can play in this process.

Chair **David Salvo**
Deputy Director, Alliance for Securing Democracy, United States

Speakers **Toba Paul Ayeni**
Independent National Electoral Commission, Nigeria

Yuri González
Director, Security and IT Control, National Electoral Institute, Mexico

Fabrice Pothier
Chief Strategy Officer, Alliance of Democracies

Julia Schuetze
Project Manager, Stiftung Neue Verantwortung, Germany

Madhulika Srikumar
Associate Fellow, Cyber Initiative, Observer Research Foundation, India; India-US Fellow, New America

Harry Sufehmi
Founder, Mafindo, Indonesia

16:45-17:00 Coffee/Tea break

17:00-18:30 Panel discussion

Cyber diplomacy: navigating values, interests and principles

Over the past 20 years, the international community in various formations (e.g. UN Group of Governmental Experts, G7/G20, OSCE, NATO, etc.) has invested significant resources in attempts to clarify the rules and principles of state behaviour in cyberspace. Even though these efforts have advanced our understanding of what constitutes unacceptable behaviour, the situation has not improved: states continue to be targets of sophisticated cyber-attacks, which increases the risk of interstate conflict. Against this background, and as the new chapter in international negotiations at the UN is about to begin, this session will discuss the challenge to reconcile values, interests and principles in the digital domain.

Chair **Natalia Drozdiak**
Bloomberg

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

Isaac Morales
Deputy Director, General for Multidimensional Security, Ministry of Foreign Affairs, Mexico

Sithuraj Ponraj
Director, International Cyber Policy Office, Cyber Security Agency, Singapore
Shariffah Rashidah Binti Syed Othman
Director, Cyber Security Policy and International Cooperation Division, Malaysia
Heli Tiirmaa-Klaar
Ambassador for Cyber Issues, Ministry of Foreign Affairs, Estonia

18:30 – 20.00 Cocktail dînatoire

16 April 2019

08:45-9:30 Registration and coffee

09:30 – 10:45 Panel discussion

Resilience and (in)stability in cyberspace: role of regional organisations

For the past 20 years, the primary role of regional organisations *vis-à-vis* the internet and new technologies was to ensure their positive impact on economic growth, competitiveness, prosperity and security. The focus on sustainable development and human security have served as the guiding principle for cross-regional activities and engagements. Faced with the destabilising impact of cybercrime and large-scale cyber-attacks, on the one hand, and limited capacities of the individual states and global institutions to tackle new sources of vulnerabilities, on the other hand, regional organisations have emerged as important players in between these two levels. The purpose of this session is to discuss the challenges that regional bodies are facing and potential role of the European Union in supporting their efforts.

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

Speakers **Abdul Gapar bin Hj. Abu Bakar**
Undersecretary, International Division, Ministry of Home Affairs, Malaysia; Chair of Senior Officials Meeting on Transnational Crime, ASEAN
Alison August Treppel
Inter-American Committee against Terrorism (CICTE), Organization of American States
Marjeta Jager
Deputy Director General, International Cooperation and Development, European Commission
Antonio Missiroli
Assistant Secretary General for Emerging Security Challenges, NATO
Alexander Seger
Head of the Cybercrime Division, Council of Europe

10:45-11:15 Coffee/Tea break

11:15-12:30 Panel discussion

Digital society in 2030: visions and divisions

As a critical factor in influencing growth, security and a proper functioning of our societies, cyberspace has also become a venue for and the subject of ideological debates driven by great power politics. The stakes are high as the political decisions taken today will have significant implications for the open, free, secure and peaceful character of the internet of tomorrow. The purpose of this session is to look critically at some of the unfolding conversations in light of various trends and visions that guide national policies with the aim of shedding light on often neglected ideas originating from civil society and the private sector.

Chair **Florence Gaub**
Deputy Director, EU Institute for Security Studies

Speakers **Olaf Kolkman**
Chief Technology Officer, Internet Society, The Netherlands

Mihoko Matsubara
Chief Cybersecurity Strategist, The Nippon Telegraph and Telephone Corporation, Japan

Nikhil Pahwa
Founder and Editor, MediaNama, India

Nanjira Sambuli
Lead for Policy Advocacy, World Wide Web Foundation, Kenya

Paweł Świeboda
Deputy Director, European Political Strategy Centre, European Commission

12:30-13:00 Closing remarks

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

Speakers **Kristina Posavec**
Deputy State Secretary of the Central State Office for the Development of the Digital Society, Croatia

Iulian Alecu
Deputy Director General, CERT Romania

Hanna Lehtinen
Ambassador. Representative to the Political and Security Committee, Finland

13:00-14:00 Lunch

14:00-17:00 Civil Society Cyber Forum (organised by EU Cyber Direct, by invitation only)

14:00-17:30 Meeting of the GLACY+ Steering Committee (organised by the Council of Europe, by invitation only)