EUROPEAN CYBER DIPLOMACY DIALOGUE

EU CYBER DIRECT

20-21 January 2020

European University Institute, School of Transnational Governance
Badia Fiesola, via dei Roccettini 9, 50014 San Domenico di Fiesole, Florence, Italy

Context

The second meeting of the **European Cyber Diplomacy Dialogue (ECDD)** will take place on 20-21 January 2020 at the European University Institute in Florence, as part of the European Cyber Diplomacy Initiative. The primary objective of the ECDD is to support the efforts of the European Union and its member states in conducting strategic cyber engagements with other countries and stakeholders by providing a platform for regular exchanges between policymakers and scholars.

Rationale

Open and regular dialogue between policymakers, researchers and scholars of cybersecurity and cyber diplomacy is a well-established practice in other parts of the world. The potential value of such meetings lies in their capacity to bridge the existing knowledge gaps, making policies more evidence-based, and research more policy-relevant. The ECDD serves two main aims: on one hand, it brings to policymakers the latest cutting-edge research on issues relevant to cyber diplomacy; on the other hand, it exposes scholars to the latest policy debates.

Format

The ECDD brings together selected researchers and analysts (members of the European Cyber Diplomacy Network) and senior level government officials involved in the design and implementation of cyber diplomacy policies in their respective countries or institutions. The two-day programme will include deep dive discussions, roundtables, and focused break-out sessions. Selected reading materials and input papers will be circulated to participants ahead of the meeting.

- Deep dive sessions focus on a very specific topic aimed at giving the participants a better understanding of the issue at hand;
- Roundtables focused on broader topics regarding cyber diplomacy;
- Working sessions address a specific policy challenge based on a case study drafted for this occasion. This year's sessions will focus on 'Cyberspace in 2030: how to keep the EU relevant?'. The working sessions aim at bringing together all relevant elements of the discussion and put forward actionable recommendations.

This event is co-organised with

European University Institute, School of Transnational Governance

Implementing organisations

European Union Institute for Security Studies

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

All sessions will take place in Teatro unless indicated otherwise
Registration and coffee breaks will take place in Antiteatro

19 January 2020

19:30 Welcome dinner

Osteria di Giovanni, Via del Moro, 22

20 January 2020

09:00-9:30 Registration and coffee

09:30-09:45 Opening remarks

Miguel POIARES MADURO
Director, School of Transnational Governance, European University Institute
Gustav LINDSTROM
Director, EU Institute for Security Studies
Rory DOMM
Deputy Head of Division for Security and Defence Policy, EEAS

09:45-10:45 Opening lecture: How to live with norm contestation?

Norms of responsible state behaviour are one of the main elements of the international stability framework in cyberspace, as established in the UNGGE reports and reaffirmed by the EU. The international community has devoted significant attention to norm development, implementation and operationalisation, largely ignoring the idea of norm contestation and the role it plays in establishing robust norms. Contestation of norms is a common phenomenon not only in the cyber domain. The key question this session will aim to address is: Should norm contestation be feared and avoided or embraced and leveraged?

Chair **Xymena KUROWSKA**
Associate Professor, Central European University, Austria
Speaker **Antje WIENER**
Professor of Political Science and Global Governance, University of Hamburg

10:45-11:00 Coffee/tea break

11:00-12.30 Roundtable discussion: Effective multilateralism and rules-based order in cyberspace: what role for the UN?

The EU's commitment to the rules-based international order and effective multilateralism has been expressed clearly in numerous Council Conclusions and policy documents. However, this vision is challenged by states who instrumentalise multilateral institutions, such as the UN, to undermine the EU's position and ultimately the values that it promotes. The purpose of this roundtable is to discuss the role that the UN plays in the governance of cyberspace.

Chair **Joyce HAKMEH**
Senior Research Fellow, International Security, Chatham House

Inputs **Adrian FARRELL**
Deputy Director, Department of Foreign Affairs and Trade, Ireland

Carmen GONSALVES
Coordinator for Cyber Issues, Ministry of Foreign Affairs, Netherlands

Mihaela POPESCU
Head of office for Cyber Issues, Ministry of Foreign Affairs, Romania

Wolfram VON HEYNITZ
Coordinator for Cyber Issues, Ministry of Foreign Affairs, Germany

Discussants **Jürg LAUBER**
Chair, UN Open-ended Working Group, Switzerland

Guilherme PATRIOTA
Chair, UN Group of Governmental Experts, Brazil

12:30-14:00 Lunch and informal exchange of views with Amb. Lauber and Amb. Patriota (closed session for government officials only)

Sala Giuseppe Buonsanti

Chair **Rory DOMM**
Deputy Head of Division for Security and Defence Policy, EEAS

Lunch for all remaining participants

Sala Rossa

14:00-15:00 Deep dive discussions

I. Rogue states in cyberspace

The global expansion of the Internet has brought many challenges to geopolitics. Cyberspace is a space of strategic priority for many states. Understanding and representing its geography remains an ongoing challenge. This session will look into how states such as Iran and North Korea have leveraged the geography of the internet to control the flow of information and to block access to content (going up to full disruption of the internet), or for active strategic purposes such as hijacking traffic or attacking infrastructures.

Seminar room 3

Chair **Caitriona HEINL**
Director and Founder, The Azure Forum for Contemporary Security Strategy, Ireland

Speaker **Kave SALAMATIAN**
Professor of computer science, LISTIC, Universite de Savoie, France

Respondent **Marek SZCZYGIEŁ**
Ambassador for Cyber Issues, Ministry of Foreign Affairs, Poland

II. Emotions in foreign and security policy

Discussion about states behaviour in cyberspace makes frequent references to emotions as an element behind state responses. Consequently, the effectiveness of measures adopted in response to violations of norms and/or international law is often addressed by invoking the feeling of 'shame', 'embarrassment', 'fear', 'pride' or 'humiliation'. This session provides an insight into the existing scholarship on the role of emotions in foreign policy and diplomacy.

Seminar room 4

Chair **Anna LEANDER**
Professor of International Relations, Graduate Institute, Switzerland

Speaker **Simon KOSCHUT**
DFG Heisenberg Fellow, Freie Universität Berlin, Germany

Respondent **Janne TAALAS**
Ambassador for Cyber Issues, Ministry of Foreign Affairs, Finland

15:00-15:15 Coffee/tea break

Antirefettorio

15:15-16:15 Deep dive discussions

III. Artificial intelligence and cybersecurity

The proliferation of AI solutions in different spheres of life has generated significant policy and research interest in the implications of these new technologies for growth and security. The purpose of this session is to focus specifically on the implications of AI for cybersecurity: both regarding the risks and opportunities that it offers.

Seminar room 3

Chair **Paul TIMMERS**
Visiting Research Fellow, Centre for Technology and Global Affairs, Oxford University

Speaker **Sven HERPIG**
Head of International Cybersecurity Policy, Stiftung Neue Verantwortung, Germany

Respondent **Wolfram VON HEYNITZ**
Coordinator for Cyber Issues, Ministry of Foreign Affairs, Germany

IV: Offensive operations in cyberspace

The use of offensive capabilities by states is no longer the taboo. Several countries have confirmed development of military cyber capabilities (without specifying their nature). Only in 2019, we have seen reports of several offensive operations conducted by states, with some of them developing explicit doctrines specifying the rationale and methods of engagement. What do these developments mean for international stability in cyberspace and great power competition?

Seminar room 4

Chair **Hannes EBERT**
Senior Advisor, The German Marshall Fund of the United States; Project lead, EU Cyber Direct

Speaker **Max SMEETS**
Senior researcher, Center for Security Studies (CSS), Switzerland

Respondent **Julio HERRAIZ ESPAÑA**
Coordinator for Cyber Issues, Ministry of Foreign Affairs, Spain

17:30-18:30 Public roundtable: Digital society in the age of great powers competition

Venue: Sala d'Arme, Palazzo Vecchio, Piazza della Signoria (transportation to the venue will be arranged)

The progressing reliance on digital platforms for delivery of key governmental functions and services has direct impact on the well-being of citizens – the way they communicate, commute to work, or benefit from public services. With the advent of smart cities, local authorities are often the first line of defence against digital risks and the victims of malicious activities against their energy, transportation or communication infrastructure. The cascading effects of digital risks from the local level to the regional, national and global level, calls for comprehensive action across all levels of government. The purpose of this public roundtable is to discuss the distribution of responsibilities and how such cooperation works in practice. What are the existing challenges and where is the room for improvement?

Welcome remarks **Cecilia DEL RE**
Deputy Mayor for Innovation and Information Systems, Municipality of Florence

Gianluca VANNUCCINI
Manager, IT Infrastructure Development Office, Municipality of Florence

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

Speakers **Laura CARPINI**
Coordinator for cybersecurity issues, Ministry of Foreign Affairs, Italy

Jürg LAUBER
Chair, United Nations Open-ended Working Group, Switzerland

Luigi MARTINO
Professor of international relations, University of Florence

Teijia TIILIKAINEN
Director, Centre of Excellence for Cyber Threats, Finland; Professor, School of Transnational Governance, European University Institute

The public roundtable will be followed by a visit of the Palazzo Vecchio organised by the Ministry of Foreign Affairs and Municipality of Florence

20:30 Dinner

B-Roof Restaurant, Grand Hotel Baglioni, Piazza dell'Unità Italiana, 6

21 January 2020

09:30-10:00 Registration and coffee

Antirefettorio

10:00-11:15 **Cyberspace in 2030: how to keep the EU relevant?**

The purpose of these scenario-based discussions in smaller groups is to question some of the key assumptions driving the EU policies and to formulate the long- and medium-term objectives in a clear and explicit manner. The sessions will also aim to design pathways to achieve or avoid specific outcomes. Based on a concrete scenario, the break-out sessions will aim to answer a number of questions: What is the vision of the internet we would like to see or avoid in the next 10-20 years? Can this vision evolve? What are the developments that could prevent or accelerates such visions from materialising (e.g. a new treaty discussion, failure of the OEWG/UNGGE, etc.)? How does this influence the strategic and tactical objectives of the EU's cyber diplomacy?

Part I: What cyberspace do we want to achieve and how do we get there?

Group A

Seminar room 3

Group B

Seminar room 4

Group C

Seminar room 1

11:15-11:30 Coffee/tea break

Antirefettorio

11:30-13:00 **Part II: What cyberspace do we want to avoid and how do we prevent such outcome?**

13:00-14:00 Lunch

Sala Giuseppe Buonsanti

14:00-15:30 **Wrap-up: European cyber diplomacy in 2020**

Chair **Patryk PAWLAK**

Brussels Executive Officer, EUISS

Analysis of the information from the survey conducted during the ECDD and discussion about lessons identified from the break-out sessions.

Teatro