EU CYBER DIPLOMACY OUTREACH

CYBERSPACE AS THE NEW NORMATIVE FRONTIER?
EUROPREAN APPROACHES TO CYBER NORMS AND DIPLOMACY

November 22, 2019

Pontifical Catholic University of Rio de Janeiro, Auditorium, Brazil

The European Union (EU) is one of Brazil's strategic partners since 2007 and a cyber dialogue partner since 2014. In the past five years, the EU has deepened and widened its engagements in the cybersecurity and internet governance debates. Numerous EU institutions and mechanisms have been created to support EU member states' efforts to maintain a sufficient degree of resilience against cyber-enabled interference. While initially focusing on cyber crime, EU institutions gradually paid increasing attention to more political dimensions of resilience. Institutions evolved at the supranational and intergovernmental levels to increase the costs of malicious activities against EU networks, including the development of a sanctions regime against cyber attacks, defensive measures such as increasing election security, and congressional oversight enhancement in member states. In 2013, the EU published a cyber security strategy that described ways in which governments can protect cyberspace from misuse and malicious activities. The same year, the European Commission proposed the Network and Information Security (NIS) Directive, the first EU-wide legislation to set standards for legal measures to minimize cyber threats. The European Parliament adopted the NIS in 2016.

In addition, the EU published a joint communication on resilience, deterrence and defense in 2017 that outlined ways to build resilience, create effective deterrence, and strengthen international cooperation to secure its member states' cyberspace from interference. In 2017, the Council agreed to develop the EU Cyber Diplomacy Toolbox, which included among other measures the imposition of sanctions against cyber attacks and established that a particularly serious cyber incidents or attack could constitute sufficient ground for a member state to invoke the EU Solidarity Clause. In March 2019, the European Parliament approved new cyber security regulation known as the EU "Cybersecurity Act", which reinforced the mandate of the European Network and Information Security Agency (ENISA) and established an EU cybersecurity certification framework to increase resilience of European infrastructures and ICT products. Finally, in December 2018, the EU outlined an action plan to step up efforts to counter disinformation in Europe and beyond that focuses on building EU's capabilities to detect disinformation, coordinate responses, collaborate with the online platforms and industry and raise awareness among citizens. The action plan built on a multistakeholder consultation process since 2017. Given the proliferation of legislative and strategic initiatives in the EU during the past years, there is a growing demand of outreach and engagement.

Against this background, the EU Cyber Direct project is collaborating with the Institute of Technology and Society (ITS Rio) and the Legalite project of PUC-Rio's Law and Information Technology departments to provide a platform for a public discussion of EU cybersecurity policy. Taking place at the sidelines of the track 1.5 *Brazil-EU Cyber Consultations on Conflict Prevention, Diplomacy and Norms in Cyberspace*, the event will invite senior EU and Brazilian governmental and non-governmental experts to map the evolving institutional EU architecture relevant for defending its member states against cyber-enabled attacks and external interference, illustrate the EU's strategic interests and approaches in global cybersecurity governance and how they are perceived in Brazil and other major actors, and assess the past and prospects for Brazil-EU cyber cooperation. By engaging with a broad audience of stakeholders and interested citizens including students in an open discussion, the event seeks to contribute to greater awareness and transparency of EU cybersecurity policy-making.

This event is co-organised with

Implementing organisations

This project is funded by the European Union.

Agenda

November 22

10:00-10:15 **Welcome remarks by PUC-Rio and EU Cyber Direct**

Gustavo Robichez
Professor of Computer Science, PUC-Rio, and Coordinator, Legalité Project

Gustav Lindstrom
Director, European Union Institute for Security Studies

10:15-11.15 **Cyberspace as the New Normative Frontier? European Approaches to Cyber Security and Governance**

A Member State's Perspective on European Cyber Policy
H.E. Luís Barreira de Sousa
Ambassador for Cyber Diplomacy, Ministry of Foreign Affairs, Portugal

Building Strategic Autonomy in Cyberspace
Paul Timmers
Visiting Research Fellow, Oxford University, and former Director, Digital Society, Trust and Cybersecurity, European Commission

Understanding Europe's Normative Power in Cyberspace
Anna-Maria Osula
Senior Researcher, Tallinn University of Technology, and Senior Policy Officer, Guardtime

How Brazil and the World Perceive Europe's Cyber Policies
H.E. Guilherme Patriota
Chair of the United Nations Governmental Group of Experts

Moderator
Rosa Balfour
Senior Fellow, The German Marshall Fund of the United States

11:15-12.00 **Questions and Answers**

About EU Cyber Direct

The EU Cyber Direct project was established to broaden the European Union's dialogues on cyber resilience, norms and CBMs with strategic partners, including Brazil. The project conducts research and facilitates dialogues among governmental and non-governmental cyber experts by organizing workshops in Europe as well as partner countries. The goal is to discuss in a more informal setting effective ways to jointly build a free, open, and secure cyberspace. It also seeks to disseminate knowledge on the EU's cyber security and internet governance policies and build bridges across regions and sectors. The EU Cyber Direct project is funded by the European Commission under its Partnership Instrument Action *International Digital Cooperation – Trust and Security in Cyberspace*. It is jointly implemented by The German Marshall Fund, the European Union Institute for Security Studies and Stiftung Neue Verantwortung.