EU-INDIA CYBER CONSULTATIONS

EU CYBER DIRECT

Managing crisis in cyberspace

27-28 October 2020

This year's rapid proliferation of the coronavirus exposed the strengths and deficits in various public governance systems, including in states' cyber resilience. Criminals and state-sponsored groups have exploited the pandemic as an opportunity to target computers and networks of home offices and hospitals for financial gain and espionage purposes, and disinformation campaigns on COVID-19 have been employed to deter culpability for the pandemic's outbreak and undermine public trust in democratic institutions. In the post-pandemic order, the rollout of 5G and the emergent cross-sectoral application of AI will likely further increase systemic cyber vulnerabilities and accentuate the need to strengthen the global framework for responsible state behaviour and existing mechanisms for global cooperation on cyber crime.

The European Union (EU) and India have made significant legislative, policy and strategic adjustments in their respective jurisdictions and intensified their cyber diplomacy efforts to address these challenges, including through bilateral cooperation. Already in 2000, Brussels and New Delhi established a Joint ICT Working Group that helped kick-starting joint ICT research and innovation initiatives and exchanging best practices on data and internet governance between governments and industry communities. In 2011, both sides met for the first cyber policy consultation, which was upgraded to a strategic Cyber Dialogue within the framework of their bilateral Security Dialogue in 2015. This expanded dialogue addressed issues ranging from enhancing stability in cyberspace through norms of responsible state behaviour, confidence-building measures (CBMs) and capacity building and efforts to tackle cyber crime to scaling up cyber security skills training in India and democratically governing data. The Cyber Dialogue has also facilitated operational cooperation between EU-CERT and CERT-IN. In addition, assessments on the use of ICT by terrorist groups were exchanged in the EU-India Counter-terrorism Dialogue. Finally, India and around half of the EU's member states also entered bilateral arrangements to enhance cyber security-related cooperation.

In 2020, the conversation can build on this existing institutional setting to achieve tangible, targeted results for greater resilience and trust in cyberspace. To this end, the EU Cyber Direct project and the Observer Research Foundation join forces to organize a second edition of the Track 1.5 EU-India Cyber Consultations. The consultations seek to create a trusted, informal space to (1) enhance mutual understanding of the evolving cyber diplomacy postures in the EU and India with regard to critical information infrastructure protection, CBMs, disinformation and cyber crime, (2) identify convergences in the diplomatic positions on future negotiations on an open, free, and secure cyberspace, and (3) build bridges between multiple stakeholders in European and Indian cyber diplomacy by including non-governmental voices in the governmental norms-building processes. The consultations offer an opportunity to exchange views on how to best create a sustainable and inclusive dialogue on how to best reinforce resilience, prevent conflict escalation, tackle disinformation and combat crime in cyberspace at the bilateral, regional and global levels.

This event is co-organised with

ORF

Implementing organisations

ISS 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.

Draft Agenda (as of 26 October 2020)

27 October 2020

09:00-09:30 [CET]
13:30-14.00 [IST]

Welcome Remarks

Gustav LINDSTROM
Director, European Union Institute for Security Studies

Ugo ASTUTO
Ambassador of the European Union to India and Bhutan

Opening Remarks: Visions for Peace in Cyberspace

Joanneke BALFOORT
Director, Security and Defence Policy, European External Action Service

Shashi THAROOR
Member of Parliament and Chairman of the Parliamentary Standing Committee on Information Technology, India

09:30-11:00 [CET]
14:00-15:30 [IST]

Panel 1: Conflict Prevention and Confidence-building in Cyberspace

Foremost driven by initiatives of regional organizations, confidence-building measures (CBMs) tailored to prevent conflict escalation in cyberspace have become one of the three pillars of the global framework for responsible state behaviour in cyberspace developed in consecutive United Nations Group of Governmental Experts (GGE) meetings and further advanced by the recent Open-Ended Working Group (OEWG). Supported by adequate cybersecurity capacity building, these CBMs help states to observe agreed upon norms by increasing transparency and predictability, facilitating crisis cooperation, and incentivizing restraint. In this panel, experts will discuss how Europe and India tailor CBMs, ranging from the identification of points of contact at the policy and technical levels to regular information exchange on cybersecurity threats and policies, to their specific contexts and use them to prevent conflict escalation or to de-escalate tensions. Panellists will also explore how Brussels and New Delhi can translate their experience with building confidence in cyberspace into concrete actions implementable by all states.

Chair

Camino KAVANAGH
Member, Advisory Support Team, UN OEWG and GGE

Speakers

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

Asoke MUKERJI
Distinguished Fellow, Vivekananda International Foundation, former Permanent Representative to the United Nations, India

Patryk PAWLAK
Brussels Executive Officer, European Union Institute for Security Studies

11:30-13:00 [CET]
16:00-17:30 [IST]

Panel 2: Building Resilient Infrastructures and Societies

The attack against India's largest nuclear power plant in 2019 and healthcare, railway, communication and shipping systems during the WannaCry and NotPetya attacks in 2017 and the COVID pandemic in 2020 have underscored the urgency to protect critical information infrastructure (CII) against cyber attacks. As a result, CII protection has become a priority of national and global cyber norms and capacity building efforts. India's new national security strategy and the EU's Cybersecurity Act outline measures to protect CII in their respective jurisdictions. This panel will discuss CII-related threat perceptions and best-practices building institutional, political, regulatory and technical capacity. Panellists will also address how the EU and India can integrate cybersecurity capacity building into broader national and regional development and digital transformation strategies to ensure greater resilience at the societal level.

Chair

Latha REDDY
Co-chair, Global Commission on the Stability of Cyberspace, and former Deputy National Security Advisor, India

Speakers

Lt. Gen. Rajesh PANT
National Cyber Security Coordinator, India

Regine GRIENBERGER
Special Representative for Cyber Foreign Policy and Cyber Security, Federal Foreign Office, Germany

Pukhraj SINGH
Cyber threat intelligence analyst, India

Ian WALLACE
Senior Fellow, The German Marshall Fund of the United States

28 October 2020

09:00-09:30 [CET]
13:30-14:00 [IST]

Welcome Remarks

Rajeswari RAJAGOPALAN
Distinguished Fellow, Observer Research Foundation

Santosh JHA
Ambassador of India to Belgium, Luxembourg and the European Union

Opening Remarks: Visions for a Free and Secure Cyberspace

Amitabh KANT
CEO, NITI Aayog

Miguel GONZALES-SANCHO
Head of Unit, Cybersecurity technology and capacity building, DG Communications Networks, Content and Technology, European Commission

09:30-11:00 [CET]
14:00-15:30 [IST]

Panel 3: Defending Democracies against Digital Disinformation

COVID-19-related digitized disinformation campaigns have proliferated in Europe and India in 2020. State and non-state actors have spread disinformation to deflect the blame for the pandemic's mismanagement or undermine trust in public democratic institutions, threatening public health. Domestic political parties and proxies leveraged social media technology to empower propaganda and incubate aggressive speech and polarization, tilting elections but also escalating caste, communal, ethnic or religious discrimination and violence. Panellists will discuss public and private, legislative, policy and technological responses to the various forms of disinformation, and explore how stakeholders from Europe and India can jointly exploit new technologies' democratic and economic benefits while mitigating their risks.

Chair

Govindraj ETHIRAJ
Founder, BOOM and FactChecker

Speakers

Lutz GUELLNER
Head of Strategic Communications Division, EEAS

Amber SINHA
Executive Director, Center for Internet and Society

Päivi TAMPERE
Head of Communications, European Centre of Excellence for Countering Hybrid Threats, Finland

11:30-13:00 [CET]
16:00-17:30 [IST]

Panel 4: Combatting Cybercrime

Reports about cyber criminals targeting hospitals during the pandemic constituted yet another wake-up call for collective global action. However, challenges in global cooperation to combat cyber crime remain a severe impediment to effective law enforcement. This panel will address how the EU and India can help jointly fill this gap. How can Brussels and Delhi bilaterally coordinate efforts to enhance capacity and training of law enforcement agencies and judicial authorities and to establish standards and procedures for cross-border data access? How can both maintain coherence, effectiveness and legitimacy of the multilateral cyber crime governance order?

Chair	**Anna Maria OSULA** Tallinn University of Technology, Estonia
Speakers	**Sanjay BAHL** Director-General, CERT-In
	Michele SOCCO Policy Officer, Directorate-General Migration and Home Affairs, European Commission
	Gulshan RAI Distinguished Fellow, Observer Research Foundation, India
	Tatiana TROPINA Assistant Professor, Leiden University
13:00-13:15 [CET] 17:30-17:45 [IST]	Conclusions **Samir SARAN** President, Observer Research Foundation
	Hannes EBERT Senior Advisor, The German Marshall Fund

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.

About Observer Research Foundation

The Observer Research Foundation (ORF) is a non-partisan, independent think tank based in India. The mission of ORF is to lead and aid policy thinking towards building a strong and prosperous India in a fair and equitable world. ORF's aim is to encourage voices from all quarters, geographies and gender, both those that fall in and those that question dominant narratives. It is this plurality of thought and voice — in a country of over a billion individuals — that ORF seeks to carry abroad, while simultaneously bringing contemporary global debates to India. ORF provides independent, well-researched analyses and inputs to diverse decision-makers in governments, business communities, and academia and to civil society around the world.