EU-INDIA THINK TANKS TWINNING INITIATIVE 2022-2023 CALL FOR INDIVIDUAL RESEARCH PAPERS ON EU-INDIA RELATIONS

Selected papers

Title: When the Outsourcer meets the Standards Setting Power: Assessing the Achievements and Challenges of EU-India Cybersecurity Cooperation
Author(s): Tobias Scholz and Sameer Patil

Funded by the European Union

This paper was written in the framework of the Call for Individual Research Papers on EU-India Relations under the EU India Think Tanks Twinning Initiative 2022-2023, aimed at connecting research institutions in Europe and India. This publication is funded by the European Union. Its contents are the sole responsibility of the corresponding author or authors and do not necessarily reflect the views of the European Union.

When the Outsourcer meets the Standards Setting Power

Assessing the Achievements and Challenges of EU-India Cybersecurity Cooperation

By Tobias Scholz & Sameer Patil

Abstract

The European Union's (EU) and India's paths towards becoming "cyber powers" could hardly be more different. The EU has a long tradition of protecting personal privacy rights and patents, while urging to enhance multilateral norms on cyberspace. India's thinking on cybersecurity has continuously been boosted by the cyber threats emerging from China and Pakistan. It has further been shaped by India's domestic Information Technology industry, which seeks to extend its market power beyond India. The different motivations and domestic capacities provide opportunities and challenges for the future of EU-India cybersecurity cooperation. This research paper analyses the evolution of EU-India cybersecurity relations in the context of both partners' different domestic policy ecosystems. It also proposes two promising areas for expanding bilateral cooperation, tackling cybercrime and expanding cyber hygiene efforts, to reinforce both partners' cyber resilience.

Executive summary

- Despite their shared threat landscape and common security concerns, EU and India have been unable to make substantive progress on cybersecurity cooperation, beyond the regular annual dialogue. The two sides have fundamentally different strategic cultures, and varying understandings that inform their cybersecurity thinking, such as on data governance and application of human rights.
- By building on their distinct domestic perspectives, both partners can explore some specific areas of cooperation in the domain of cybercrime and cyber hygiene. This potential partnership builds on their expanding cooperation in other related domains of technology, as evident from the establishment of the India – EU Trade and Technology Council.

- The growing challenge of cybercrime and proliferation of ransomware for EU and India provides an urgent imperative to advance collaboration. They can realize this by establishing a dedicated Working Group for cyber forensics and information-sharing. Supplementing this can also be the potential collaboration to tackle darknet marketplaces.
- Cyber hygiene is another promising area of cooperation, where both sides can shape and share best practices and training platforms and mechanisms. The EU can hereby draw on its own and the experiences of its member-states.

Introduction

At the center of the European Union's (EU) and India's strategic partnership stands the puzzling contrast between growing geoeconomic and geopolitical convergences and fundamentally different strategic cultures. The cybersecurity relations between the EU and India are exemplary of the relationship's disconnect. This essay seeks to contribute to the understanding of EU-India cybersecurity relations by emphasizing how domestic experiences have shaped attitudes and priorities of both partners differently over time. We ascertain, that by considering the distinct domestic perspectives of both partners on cybersecurity, this brief arrives at sensible recommendations for future advancements in the partnership.

This brief consists of four sections. To get a more profound understanding of the varying understandings that inform cybersecurity thinking, the first section introduces the origins of cybersecurity awareness in the EU and India. The second section traces the convergence of ideas, interests, and institutions within the evolving partnership to identify the key advancements and well as the uniting and dividing factors in EU-India cybersecurity relations. The third part assesses the achievements of EU-India cybersecurity relations on cybercrime, and cyber hygiene.

The discussion of this paper aims at contributing to a more profound understanding of the challenges and opportunities in the EU-India cybersecurity partnership. Illustrating the different roots of cybersecurity thinking, varying normative standpoints, and strategic convergence, we seek to provide a realistic assessment of where the EU and India can leverage their strengths to advance the partnership. As we identify the most significant convergence on cybersecurity interests in increasingly aligning strategic interests rather than similar normative values, this brief explicitly focuses on the strategic angle. This perspective allows locating appropriate areas for future cooperation more realistically.

Origins of Cybersecurity Thinking in the EU and India

The EU's early to approach cybersecurity has initially been informed by the member states' experiences in the United Nations (UN) debates. In 1998, the Russian Federation had pitched General Assembly Resolution 53/70, followed by annual multilateral debates which ultimately resulted in the creation of the UN Group of Governmental Experts. A central diving line quickly emerged, in which EU countries, alongside the United States, debated against authoritarian governments from China, Iran, and Russia who sought greater sovereign control over the Internet. In line with its international normative aspirations as well as with the economic advantages of a global and interconnected Internet, the EU stood for a relatively free and open information space. While the EU aligned with the U.S. in many ways, it began focusing on cyber norms in the fields of international trade and security to influence the scope of free speech online, the applicability of international law in cyberspace, and dispute resolution mechanisms.

In the case of India, the formation of cybersecurity priorities was shaped by two lines of thought. The first relates to India's developmental aspirations. From the beginnings of an international cyberspace, India perceived the Internet and cyberspace as tools for enabling economic development and employment creation. In the early 1990s, the expansion of the Internet led to the development of the Information Technology (IT)-enabled services, making India an IT hub. Simultaneously, the Indian

government too gradually adopted IT and expanded citizens' access to basic government services. These development aspirations contributed to India's digital transformation.

The second significant realization came through the changing needs of the private sector, considering new international cybersecurity standards. After India's first liberalization efforts in the early 1990s, market growth and exports of Indian IT and IT Enabled Services companies contributed greatly to India's overall economic growth. With increasing success on the U.S. market, India's exporting companies had to comply increasingly to new sets of cybersecurity norms and standards that American legislations introduced. Emulating technical cyber norms and harmonizing its standards (or at least not adopting conflicting standards) became a priority for the Indian companies. It was hence Indian companies like Infosys or Wipro which took the lead in developing IT security products and subsequently forayed into the cybersecurity domain.

The evolution of cooperation

When the EU and India started discussing cybersecurity, they could already build on diplomatic interactions in domains related to their cybersecurity efforts. These building blocks include the Agreement for scientific and technological cooperation in 2001, in which both partners first recognized the growing technological capabilities and the need to converge on Research and Development (R&D) as well as on intellectual property rights. More in the context of a digital and developmental partnership, the two partners in the same year began the Information and Communication Technologies (ICT) Working Group.

The relationship was further affected by the ongoing international discussion on Internet governance. At the beginning of the 21st century, countries around the world were debating on whether the ownership of the International Corporation of Assigning Names and Numbers (ICANN) should be transferred from being a private contractor of the U.S. Department of Commerce to a UN body. Funded by the European Commission, the bilateral ecosystem fostering public-private partnerships and ICT Research was initiated by a cooperation forum on the information society in 2004. The forum's

name referenced the then ongoing World Summit on the Information Society, in which Internet governance was discussed. India and the EU stood on different sides of the table when nation states debated over a future governance model for the Internet. That both partners started a bilateral track on the information society in the same year illustrates the severity of an appropriate Internet governance model for both countries' at the time. Technically, not a security conflict, the debate on Internet governance foreshadowed the normative standpoints of both partners in future international controversies. While the EU supported the US, India urged to view the Internet as a space which requires greater law enforcement capacity for nation states.

The 2005 Joint Action Plan, which specified the goals of the EU-India Strategic Partnership, marked the first comprehensive assessment of steps to be taken to advance cooperation on ICTs. The Action Plan mostly emphasized ICTs in their developmental context by pointing out the "powerful effect on economic and social development". The only significant security matter that both countries explicitly put forward as a field of cooperation was the problem of "spamming". An in-depth look at the Joint Action Plan further exposes a lack of comprehensive strategic considerations on cybersecurity. For instance, the document lists issues like e-commerce and digital health, where cooperation should be increased. The Joint Action Plan does not, however, mention the significance of the need to aligning legal concepts like privacy and data protection, which could have nurtured a better normative understanding between the two partners.

This first episode of EU-India cooperation on issues relating to cyber illustrates how the awareness of the new domain was initially only growing within separate policy tracks. Towards the end of the 21st century's first decade, both partners' policy elites experienced severe political crises. Within the EU, it was Estonia which was hit the hardest by coordinated Denial of Service attacks emanating from Russia in 2007.[1] As a consequence, Estonia, which belonged to the early adopters of public digital

[1] Russia's attacks took place as a retaliation towards the Estonian government's decision to relocate a Soviet era bronze statue. Estonia's decision to critically distance itself from the Soviet past had previously met diplomatic aggression by the Russian Federation.

infrastructures, pushed towards stronger international cooperation on cyber norms, capacity building, and hygiene. In India, on the other hand, the 2008 Mumbai terror attacks initiated a debate in New Delhi on the rights of executive agencies to access and control personal communications on the Internet. After the terrorists had used satellite phone networks and Voice over Internet Protocol technology to plan and coordinate the attacks, the federal political consensus in India shifted towards a greater emphasis of state control. As cybersecurity threats grew, the EU and India could draw on the already existent dialogue formats and agreements to formalize cybersecurity relations.

Growing cyber threats and first major convergences

India and the EU began to upgrade their cooperation significantly in 2010 following a growing cyber threat landscape. In the context of the India-EU Joint Declaration on International Terrorism, cooperation on cybersecurity was mentioned by the two countries for the first time in an official document. In the declaration, both partners committed to leveraging their efforts towards information sharing. This was particularly in India's interest. Not in alliance with any major cyber power and further not a party to the Budapest Convention on Cybercrime[2], India viewed bilateral information sharing agreements as the only efficient measure to seek support for transnational criminal prosecution. The situation further became increasingly worrisome for India's law enforcement agencies, as much of the inquired information was stored on servers of social media companies and tech platforms that were not located in India. That the first exclusive conversation on cybersecurity took place as a debate within the wider counter-terrorism efforts marks a success for India's political agenda, which lays a greater emphasis on information security. The mutual proclamations, however, could not end up forging a significant cybercrime partnership going much beyond regular diplomatic statements. Particularly, a lack of institutionalised cooperation between the respective computer emergency response teams, CERT-In and CERT-EU, became a missed opportunity.

[2] The Budapest Convention is the world's sole body of international law regulating international cybercrime.

The early 2010s were marked by the emergence of great scale cyberattacks affecting the critical infrastructure and, in response, a realization that cybersecurity belonged at the center of diplomatic efforts. India was the third most affected country by the Stuxnet virus targeting Iran's nuclear enrichment facilities, and its public sector became the target of an increasing number of cyberattacks from China. Just shortly after, EU countries were greatly impacted by Duqu, a similar virus targeting Industrial Control Systems.

In 2015, the two parties established their first Cyber Dialogue as part of the existing Security Dialogue framework. This marked the first time in which both partners committed publicly to "work together to maintain an open, secure and resilient cyberspace". Since then, the EU and India have met annually to discuss national and international cybersecurity challenges alongside counter-piracy, non-proliferation, and counter-terrorism. The dialogue brought together from the EU side representatives of the European External Action Service and EUROPOL and from the Indian side, representatives from the Ministry of External Affairs, Ministry of Electronics and Information Technology, the National Security Council Secretariat, National Critical Information Infrastructure Protection Centre, as well as security agencies like the Central Bureau of Investigation (CBI) and National Investigation Agency (NIA). This wide-ranging participation notwithstanding, the existing Track 1 dialogues produced mixed results. In terms of strategic cooperation between the EU and India the outcome of the annual dialogues was underwhelming as they have not resulted in any major effect on the overall bilateral security relationship. However, dialogue formats have recognised the economic potentials, particularly by considering standardisation, technology development, and by advancing B2B programmes. While the economic relations between both partners were just heading off, the strategic element was still amiss. This was changing with the growing assertiveness of China and Russia.

Forging strategic depth

Lately, definite divergences as well as new strategic convergences between the EU and India characterized the cybersecurity relations. Data governance, for instance, illustrates a policy issue in which the EU's and India's varying legal understandings continue to thwart further economic

integration. Similarly, two sides differ considerably on the application of human rights in the management of cyberspace. Therefore, expanding bilateral cybersecurity cooperation will necessarily encounter trust issues. This requires both sides to explore cooperation on other related domains. The formation of the India – EU Trade and Technology Council (TTC) in 2022 is one effort towards this. The TTC, in its first meeting in May 2023, agreed to work together on issues like semiconductors, Quantum and High-Performance Computing and Digital Public Infrastructure. Instead of elaborating on the detailed evolution of cooperation between India and the EU between 2015 and 2023, the following chapter provides insights into two particular policy issues. Taking such a focused perspective helps to consider more clearly the challenges and opportunities for the partnership.

Assessing success and failure

In the following sections, we critically review the success in two contemporary and pressing areas of cooperation between the EU and India. For two decades, progress on cybercrime cooperation between the two countries has been low due to the partners' different stance towards the Budapest Convention. Much untapped potential lays in cyber hygiene efforts, that have only been a minor component of the EU-India cyber partnership.

Cybercrime

The growing sophistication of cybercrime through customized malware and advanced ransomware poses a significant cybersecurity challenge the world over. Proliferation of generative Artificial Intelligence tools has also helped cybercriminal syndicates to ramp up their criminal activities on the Internet.

In India, as per the National Crime Records Bureau, there has been an unparalleled spurt in cases of cybercrime in the country. However, the conviction rate remains low at just 42.5 percent in 2021, highlighting the inadequacy of Indian law enforcement agencies' cyber forensic capabilities. Ransomware has emerged as a major threat whereby cybercriminal syndicates are targeting not just major corporations, but also small and medium sector enterprises, which do not necessarily have

adequate guardrails to protect themselves from these malicious activities. According to one study, 73% of organizations surveyed in India had become victims of ransomware attacks. Moreover, there is a drop in ransoms being paid for data recovery, with organizations refusing to follow cybercriminals' diktats. Yet, this is also increasing the risk of data leaks, particularly on darknet marketplaces, which have flourished by selling stolen personal and financial data. The criminal use of cryptocurrencies on these websites also poses an additional challenge for Indian agencies.

A similar trend is evident in Europe where, according to the European Union Agency for Cybersecurity (ENISA), cybercriminals have shown an increased level of collaboration and professionalization. It also adds that the threat of ransomware persists, with 60 percent of the organizations complying with ransom demands. While Russia's invasion of Ukraine has displaced various known cybercriminal syndicates, some of them adapted and are now exploiting the situation to perpetuate payment frauds. EUROPOL also highlights the critical role played by phishing, anonymization tools and criminal abuse of cryptocurrencies as cross-cutting crime enablers, that complicate the European cybercrime landscape.

Despite the pressing nature of the cybercrime threat, India-EU cooperation on cybercrime front has not achieved its full potential. The issue has regularly featured in the annual India-EU Cyber Dialogue. Yet, as noted in previous paragraphs, it appears that these conversations have not materialized in concrete action. Divergent positions on cross-border data flows, and the Budapest Convention, continue to be stumbling blocks in advancing the collaboration.

The surging sophistication of cybercrime and the menace of ransomware provide an urgent imperative for both sides to leave old disagreements on multilateral norms and treaties behind them. Instead, the two partners must advance their collaboration by putting forward concrete measures. In particular, they can work together on cyber forensics and information-sharing – two areas which India's Ministry of Home Affairs (MHA) has pursued with greater focus in recent years, after establishing the Indian Cybercrime Coordination Centre. The Ministry is in the midst of establishing cyber forensic

laboratories all over India. An India-EU cooperation on information-sharing and on forensics for cybercriminal investigations will only reinforce mutual resilience. Supplementing this can also be the potential collaboration to tackle darknet marketplaces that draw upon EUROPOL's extensive experience in disrupting this illicit activity. Such collaboration will also be beneficial for EUROPOL, particularly in tackling the sale of narcotic substances emanating from India's neighborhood.

The EU and India can operationalize cooperation on these aspects by establishing a dedicated Working Group on Cybercrime, Darknet and Cryptocurrencies. This group should ideally involve the Indian MHA and security agencies like the CBI, NIA and EUROPOL along with the respective Financial Intelligence Units and CERTs. This Working Group can serve as a platform to not only share intelligence on the activities of cybercriminal syndicates and darknet marketplaces, but also keep track of encryption and cryptographic tools used by them. Through this Working Group, EUROPOL can further engage the Indian law enforcement agencies for training in cybercriminal investigations, examining digital evidence, and involving them in darknet marketplace takedowns.

At the normative-macro level, the EU can work with India to review and revisit the Indian position on the Budapest Convention. As the only functional international mechanism to tackle cybercrime, the Indian government too has internally deliberated on reconsidering India's opposition to the Budapest Convention.

Cyber hygiene

New and emerging criminal methods in an interconnected cyberspace mandate adoption of cyber hygiene practices for protecting critical infrastructure and personal data. Cyber hygiene is generally associated with the practices and precautions users take with the aim of keeping sensitive data organized, safe, and secure from theft or unauthorized access. According to a survey conducted by ENISA in 2016, cyber hygiene was still a low priority for businesses operating in the EU.

Consequently, the EU has extensively emphasized on cyber hygiene in its efforts to boost European cyberspace resilience, including through its Digital Single Market Strategy, launched in 2015. The

ENISA also implements the annual 'European Cybersecurity Month' campaign to raise awareness among EU citizens and organizations. Cyber hygiene has also figured in cyber diplomacy with other countries, for instance, with the United States.

The issue of cyber hygiene assumes all the more significance for India which has the world's second-largest Internet user base with 780 million users. Many of these are first-generation users who generally lack awareness to protect themselves in cyberspace. The Covid-19 pandemic has only exacerbated cyber hygiene concerns as it fostered dependence on the Internet due to extended lockdowns, online learning and 'work from home' modes. Aspiring to become a leader in private and public digital infrastructure solutions, Digital India's success also rests on the success of its citizens' ability to adapt secure behaviors when using the Internet.

India and the EU can shape and share best practices and training platforms and mechanisms on cyber hygiene that not only foster resilience but also contribute to the overall cybersecurity capacity of both partners. Results from these processes can be leveraged in trilateral developmental programs. Besides ENISA's own work in this domain, the EU can particularly draw on the experience of its member-states like Estonia, which has widely disseminated cyber hygiene training and practices to its citizens, businesses, and government officials.

EU-India cybersecurity cooperation: A success story waiting for the big deliverables

Two sets of interests create greater policy convergence between the EU and India. On the one hand, rising threat levels due to malicious state- and non-state actor activities urge the EU and India to align their political efforts closer with each other. This includes a shared interest in countering revisionist and imperialist projects in their region by increasing cyber resilience and capacity. It also includes a potential for higher multilateral cooperation to shape norms that make it easier to work against rogue cyber actors and to work towards more attribution mechanisms. On the other hand, there is a strong economic imperative. Whether specifically considering the cybersecurity- and privacy sectors, or more

generally the IT & ITES industries, the EU, and India are demanded to increase interoperability as well as common norms and standards.

Focusing on cybercrime and cyber hygiene as two relevant contemporary cases illustrates that the EU-India cybersecurity partnership requires greater strategic depth. First steps to accomplish this goal can include more agency-level cooperation, more dialogue on multilateral cyber norms, as well as joint capacity building efforts. Thinking one step beyond, the evolving cybersecurity partnership can even benefit other partners. Trilateral cybersecurity capacity building development partnerships or joint cybersecurity exercises with third countries could be a promising way how the EU and India could leverage their partnership to higher levels of cybersecurity globally.

Authors:

Tobias Scholz is a doctoral candidate at King's College London and the National University of Singapore and a non-resident fellow with the Global Public Policy Institute (GPPi). His dissertation investigates continuity and change in India's foreign and security policy in the context of its cyber diplomacy. His research interests further include geopolitical challenges in the Indo-Pacific region, Germany-India and EU-India relations, as well as international cybersecurity governance.

Sameer Patil is Senior Fellow, at the Observer Research Foundation's (ORF) Centre for Security, Strategy and Technology and Deputy Director, at ORF's Mumbai centre. His work focuses on the intersection of technology and national security, including cybersecurity. He also serves as India Commissioner for the Global Tech Security Commission, set up by the Krach Institute for Tech Diplomacy at Purdue and the Atlantic Council.