Enhancing Global Cybersecurity Cooperation: European and Indian Perspectives

Cormac Callanan • Basu Chandola
Hannes Ebert • Caitriona Heinl • Anirban Sarma

ORF

ESIWA
ENHANCING SECURITY
COOPERATION
IN AND WITH ASIA

Co-funded and implemented by
the European Union

Attribution: Cormac Callanan, et al., *Enhancing Global Cybersecurity Cooperation: European and Indian Perspectives,* October 2022, Observer Research Foundation and ESIWA.

ORF (Observer Research Foundation) is a non-partisan, independent think tank based in India. It seeks to lead and aid policymaking toward building a strong and prosperous India in a fair and equitable world. It helps inform India's choices, and carries Indian voices and ideas to forums that aim to shape global debates. ORF's research and other engagements cover a range of policy issues that include critical and emerging technologies, the impact of technology on national and international security, cyber security, Internet governance, and the interaction of tech policy and geopolitics.

ESIWA (Enhancing Security Cooperation in and with Asia) is a project funded by the European Union, and supported by the German Federal Foreign Office and the French Ministry for Europe and Foreign Affairs. The project is designed to support deeper and more operational security dialogues with partner countries (India, Indonesia, Japan, Republic of Korea, Singapore, and Vietnam); promote greater convergence between the policies and practices of the EU and these partner countries in the field of security; and contribute to increasing international awareness and acknowledgment of the EU as a security provider.

Cover image from Getty Images/Yuichiro Chino

Disclaimer: The contents of this publication are the sole responsibility of the authors and do not necessarily reflect the views of the EU, Indian government officials, or any other commissioning parties.

CONTENTS

Executive Summary

Background

The European Union (EU) and India share a long tradition of bilateral cooperation in the domain of cybersecurity. Since the early 2000s, both parties have on numerous occasions affirmed their commitment to stronger cyber-cooperation and greater global cyber resilience, and initiated joint strategies and actions in this regard. Both parties also interact across various groups and dialogues such as the India-EU Joint ICT Working Group, the Counter-Terrorism Dialogue that tackles the use of cyberspace by terrorists, and the India-EU Cyber Dialogue.

Besides these bilateral activities, the EU and India engage with and through various international cooperation mechanisms for advancing responsible state behaviour in cyberspace. These include the UN Group of Governmental Experts, the UN Open-Ended Working Group, the recently proposed Programme of Action, and coordinated multi-country efforts like the International Counter Ransomware Initiative.

Framing the Challenge

The last few years have seen a sharp rise in the incidence of cyber-attacks in various parts of the world, signalling a renewed need to focus on efforts to strengthen cybersecurity. Partly as a result of the COVID-19 outbreak that forced a shift to digitisation of economic, social and other activities, the year 2020 broke records in the number of criminal cyber-attacks on companies, governments, and individuals, and the volume of data lost in breaches. Cybersecurity firm McAfee estimated that as of December 2020, incidents of cybercrime had cost the world economy over US$ 1 trillion, up by 150 percent from a 2018 estimate of US$ 600 billion.

The increase in malicious cyber incidents has continued. In 2021, India experienced the third highest number of data breaches in the world, with over 86.3 million breaches occurring in the first 11 months of the year. Similarly, the *Internet Organised Crime Threat Assessment 2021* found that the EU was witnessing a spike in ransomware affiliate programmes, mobile malware, and online fraud.

Convening Stakeholders in New Delhi

ESIWA and ORF convened a high-level, closed-door roundtable in New Delhi on the sidelines of the Raisina Dialogue 2022 in March to discuss and examine European and Indian positions on these cybersecurity issues. The roundtable featured more than 30 high-level European and Indian stakeholders, including senior government officials, think tank analysts, and industry representatives. The event was the first in a series of six roundtables that ESIWA and ORF will host in 2022-23 in order to advance track 1.5 cyber-dialogues between the EU and India. The deliberations were guided by three principal questions:

- How can EU and Indian diplomatic officials in-charge of cyber issues cooperate bilaterally and multilaterally to increase adherence to cyber norms and implementation of cyber confidence-building measures?
- How can EU and Indian private sector stakeholders be best involved in implementing the normative framework for responsible state behaviour in cyberspace?
- How can the EU and India jointly, on a bilateral and multilateral basis, address the rise of increasingly lucrative and organised forms of cybercrime such as ransomware?

Recommendations

Based on the roundtable discussions, the authors have developed seven core recommendations to help policymakers in Brussels and New Delhi elevate EU-India cyber-cooperation, and continue evolving newer ways of promoting cybersecurity and countering cyber-threats.

SEVEN WAYS TO STRENGTHEN EU-INDIA CYBER COOPERATION

1

Build upon and expand EU-India cyber interactions.

2

Promote multistakeholder engagement at various levels.

3

Jointly undertake capacity building exercises and confidence-building measures.

4

Explore the implications and possible benefits of the Programme of Action.

5

Work towards crafting new standards for data governance and data sharing.

6

Work towards developing global standards in selected domains.

7

Continue to build trust through increased cooperation.

Introduction

India and the European Union (EU) share common values of democracy and rule of law, and both recognise the need to protect the rules-based order and enhance structures for sustainable development. They have expanded their security cooperation in the last few years, and today engage in naval exercises[1] and various forms of defence collaboration.[2] Most recently, in April 2022, the two sides established the EU-India Trade and Tech Council to "tackle challenges at the nexus of trade, trusted technology and security."[3]

This report outlines ongoing joint initiatives by the EU and India in promoting cybersecurity. It gives an overview of the current landscape of cyber-threats facing the two regions, and offers specific, actionable recommendations to strengthen their cyber-cooperation.

For both India and the EU, the imperative is to promote an open, free, secure and accessible cyberspace that enables growth and innovation—an aim which they reiterated during their most recent cyber dialogue in December 2020.[4] Earlier, at the 15th EU-India Summit in July 2020, government leaders agreed on a roadmap to guide joint actions and strengthen their partnership in a range of issues including promoting cybersecurity and combating cybercrime.[5] Other bilateral initiatives where both committed to cybersecurity include a number of EU-India Summits, the EU-India Joint Declaration on International Terrorism, the EU-India Connectivity Partnership, the Joint Statement on the India-EU Leaders' Meeting, and the India-EU Joint ICT Working Group whose most recent meeting was in 2021.[6,7]

The EU and India have acknowledged both the significant benefits of cyberspace, and its continuously evolving challenges. It is important to improve the capabilities of state and non-state actors to arrest the incidence of malicious cyber activities, which have increased in frequency amidst the COVID-19 pandemic and the Russian invasion of Ukraine.

It is against this backdrop that ESIWA and ORF are hosting a series of track 1.5 dialogues between the EU and India in the form of six roundtable events in 2022–23. The roundtable series aims to build on the tradition of cyber-cooperation between the EU and India, and foster dialogue and collaboration in order to strengthen cybersecurity and fight cybercrime. Participants will exchange information and discuss respective European and Indian positions on key cybersecurity issues of concern. The conclusions of the roundtable discussions will be put forward for consideration during the formal EU–India Cybersecurity Dialogue meetings.

The first ESIWA–ORF roundtable was held in New Delhi on 27 April 2022 on the sidelines of the Raisina Dialogue 2022. It addressed the theme, 'Enhancing Global Cybersecurity Cooperation: European and Indian Perspectives'.

> "The capabilities of state and non-state actors must be improved to arrest the incidence of malicious cyber activities, which have increased in frequency amidst the COVID-19 pandemic and the Russian invasion of Ukraine."

The Current Threat Landcsape

Partly as a result of the COVID-19 outbreak and the consequent increase in remote work, the year 2020 witnessed high numbers of criminal cyber-attacks on companies, governments, and individuals, and the volume of data lost in breaches. According to cybersecurity firm McAfee, as of December 2020, incidents of cybercrime had cost the world economy over US$ 1 trillion, up by 50 percent from a 2018 global report that pegged cybercrime-induced economic losses at US$ 600 billion.[8]

In Europe, the European Union Agency for Cybersecurity (ENISA) reported 304 malicious attacks against critical sectors[a] in 2020, double the number from the previous year.[9] Meanwhile, in India, the National Crime Records Bureau recorded a rise of 11.8 percent in cybercrime in 2020;[10] and over 1.15 million incidents of cyber-attacks were reported to the country's Computer Emergency Response Team (CERT-In) in the same year.[11]

In 2021, the Microsoft Threat Intelligence Center and the Digital Security Unit observed that most nation state actors focused operations and attacks on government agencies, intergovernmental organisations, nongovernmental organisations, and think tanks for traditional espionage or surveillance objectives.[12] During 2019–21, Microsoft delivered over 20,500 Nation State Notifications (NSNs) when customers were targeted or compromised by nation state activities.

In 2021, India ranked third in the world (after the US and Iran) in the number of reported data breaches, with 86.3 million incidents in the first 11 months of the year.[13] Overall, as data from CERT-In shows, instances of cybercrime in India have increased fivefold between 2018 and 2021.[14] Similarly, the *Internet Organised Crime Threat Assessment 2021* reported that the EU had witnessed a sharp rise in ransomware affiliate programs, mobile malware and online fraud. Indeed, the number of ransom payments across the EU increased by over 300 percent between 2019 and 2020.[15]

[a] Critical infrastructure sectors that were affected include healthcare, transportation, and energy.

A Brief History of EU–India Cyber Cooperation

The very nature of a cybercrime makes it difficult to address: it occurs in the borderless realm of cyberspace, and both the criminal and the victim could be located in multiple national jurisdictions. This underscores the need for flexible frameworks of international cooperation to enhance cybersecurity. As the United Nations Office of Drugs and Crime (UNODC) has observed, these mechanisms could include harmonised national cybercrime laws, or bilateral, regional and multilateral cybercrime treaties or arrangements.[16]

The focus of EU-India cyber-cooperation is still primarily on bilateral summits, joint agreements, partnerships, and working groups. Both parties also engage with and through several international cooperation mechanisms for advancing responsible state behaviour in cyberspace. Such initiatives include the India-EU Joint ICT Working Group, India-EU Connectivity Partnership, and the Indian-EU Cyber Dialogue.

India-EU Bilateral Cooperation on Cybersecurity

India and the EU have cooperated on cybersecurity since the early 2000s. They both have, on several occasions, reaffirmed their commitment to "an open, free, secure, stable, peaceful and accessible cyberspace that enables economic growth and innovation." The following table outlines the highlights of EU-India engagements over the years in the cyber domain.

Year	Forum or Platform	Outcome
2003	4th India-EU Summit	India and EU agreed to enhance cooperation in the area of data protection and cybersecurity in the information society sector.[17]
2010	India EU Joint Declaration on International Terrorism	India and EU agreed to enhance mutual assistance in the area of cybersecurity.[18]
2016	13th India-EU Summit	India and EU reaffirmed the need to strengthen cyber-cooperation.[19]
2017	14th India-EU Summit	
2020	15th India-EU Summit	India and EU underlined the need to increase global cyber resilience, including in the health sector.[20] Both sides also agreed to increase joint efforts on cybersecurity through the India-EU Connectivity Partnership.
2020	India-EU Connectivity Partnership and the Joint Statement on the India-EU Leaders' Meeting	India and EU agreed to increase joint efforts on cybersecurity through the India-EU Connectivity Partnership and the Joint Statement on the India-EU Leaders' Meeting. [21]
2020	India-EU Strategic Partnership: A Roadmap to 2025	India and EU agreed to strengthen cooperation, work towards tangible outcomes on cybersecurity, and continue to expand existing cooperative efforts.[22]
2020	India-EU Counter-Terrorism Dialogue	The most recent Dialogue where the use of cyberspace by terrorists was discussed.[23]
2020	India-EU Cyber Dialogue	The most recent Dialogue, which was held virtually.[24]
2021	India-EU Joint ICT Working Group	The most recent meeting of the Working Group. [25]

The India-EU Joint ICT Working Group is part of the EU's commitment of working with like-minded partners in "achieving common global objective: a green, digital, just and resilient future for the next generation"[26]. The Working Group works on a wide-range of subjects including artificial intelligence, digital platforms, data governance, cybersecurity and networks. Meanwhile, the India-EU Cyber Dialogue focuses on areas of cooperation in cyberspace including internet governance, cyber diplomacy at UN activities, regional cooperation, capacity-building, and emerging cyber-related technologies.

International Mechanisms for Promoting Cybersecurity

Various international cooperation mechanisms exist for advancing responsible state behaviour in cyberspace: the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention; and three UN First Committee state processes, namely, (a) the Group of Governmental Experts (GGE); (b) the Open-Ended Working Group (OEWG); and (c) the recently proposed Programme of Action (PoA) that seeks to end the dual-track discussions (GGE / OEWG) and in their place establish a permanent UN forum on cyberspace. Of these mechanisms, the EU (or individual EU Member States) and India have engaged chiefly on and through the GGE and OEWG. The UN third committee is responsible for the work on the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

The Budapest Convention

The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention was opened for signature in Budapest in November 2001 and came into force in July 2004 as the first international instrument on cybercrime. It is currently the only binding international instrument on cybercrime[27] and seeks to pursue "a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation." Although it is a Council of Europe (COE) instrument, the Convention permits states that are not members of the Council of Europe to accede to the Convention, subject to the unanimous consent of all parties.[28] As of July 2022, there are 66 parties to the Convention.[29]

Overall, the Convention deals with offences such as computer-related fraud, illegal access, misuse of devices, and child pornography. Its principal aims are to: (1) Harmonise domestic laws on cybercrime; (2) Support the investigation and prosecution of cybercrimes; and (3) Facilitate international cooperation on cybercrime. Since 2006, the first Additional Protocol to the Convention that criminalises *'acts of a racist and xenophobic nature committed through computer systems'* has been in effect.[30] A recently approved Second Additional Protocol on *'enhanced cooperation and disclosure of electronic evidence'* opened for signature by states in May 2022.[31]

EU and Indian positions on the Budapest Convention

The EU continues to support third countries that wish to accede to the Budapest Convention, and to work towards improving international cooperation between law enforcement agencies, judicial authorities, and service providers, in which the European Commission participates in negotiations on the EU's behalf. The EU also engages in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms, through inclusiveness, transparency, and by leveraging available expertise, with the goal of delivering value for all.

India has refrained from acceding to the Budapest Convention. While India has not released any official statements regarding the matter,[32] information in the public domain suggests a few possible reasons for its hesitancy.[33] First, as the Convention allows for trans-border access to data, it might be seen as infringing on India's national sovereignty. Second, as India was not involved in the original drafting process, there could be a perception that its priorities are not adequately reflected in the Convention. Finally, the perceived lack of effectiveness of the Convention's Mutual Legal Assistance (MLA) regime could be a disincentive for accession.

In January 2020, the UN General Assembly (UNGA), on the basis of the report of the Third Committee (A/74/401), via a resolution established an open-ended ad hoc intergovernmental committee to draft an international convention on cybercrime (2019-2020). India voted in favour of the resolution.[34]

The UN Group of Governmental Experts (GGE)

The UN First Committee on International Security and Disarmament is where states exchange views on issues related to international peace and security, including those related to cyberspace. These discussions take place through the Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace, and the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications.

The UNGA established the first GGE in 2004 to explore the impact of developments in ICT on international peace and security. Six GGEs have convened to date, with each Group comprising individual experts representing interested UN Member States, including the five permanent members of the UN Security Council. The mandate of the GGEs has been to examine threats in cyberspace along with possible cooperative measures, and to maintain an open, secure, peaceful and accessible ICT environment. Towards this end, discussions have focused on existing and emerging cyber-threats; cyber norms, rules and principles for states; confidence-building measures (CBMs); the application of international law to the use of ICTs; and international cooperation and cyber capacity building (CCB).[35]

The report of the sixth GGE to the UN General Assembly in 2021 identified a distinct set of norms for promoting responsible behaviour among states; reaffirmed that international law is the basis for preventing conflict and promoting a peaceful ICT environment; reiterated the importance of CBMs to strengthen cybersecurity; and underscored the importance of cooperation related to ICT security.[36] With the completion of the sixth GGE's work in May 2021, no immediate plans have been issued to renew the GGE format. In retrospect, the GGE's two key achievements have been to outline a global cybersecurity agenda; and to introduce the principle that international law applies to cyberspace.[37]

EU and Indian positions on the UN GGE

While the EU itself is not a member of the GGEs, many individual EU member states have held expert positions on past GGEs. It is the EU's position though that it continues to work with international partners to advance and promote an open, stable and secure cyberspace where international law, particularly the UN Charter, is respected, and the voluntary non-binding norms, rules and principles of responsible state behaviour are adhered to. The EU's Cybersecurity Strategy (2020) indicates a clear need for the EU and its member states to take a more proactive stance in discussions at the UN and other relevant international fora. It further states that the EU is best placed to advance, coordinate and consolidate EU member states' positions in international fora, and should develop an EU position on the application of international law in cyberspace.

India was an active member of the fifth (2016-17) and sixth (2019-21) GGEs. While it was not a member of the third GGE for 2014–15, it responded to the Group's deliberations by initiating a national study for examining the norms for cooperation proposed by the GGE and designing a set of national cyber norms.[38,39] In 2021, India endorsed the long-standing GGE view that the application of international law to cyberspace is critical for building a secure and peaceful ICT environment. India has also expressed its hope that discussions at the UN and other multilateral forums will continue to focus on cooperative measures, CBMs, and cyber norms.[40] In June 2021, India reiterated the importance of a collaborative rules-based approach in cyberspace, and of leveraging the positive momentum generated by the GGE and the OEWG in order to "find further common ground and improve upon the already agreed cyber norms and rules."[41]

The UN Open-Ended Working Group (OEWG)

In 2019, the UNGA set up the Open-Ended Working Group (OEWG) to provide a "democratic, transparent and inclusive platform"[42] for UN member states to participate in the process of determining the rules for ICTs and international security. The OEWG's mandate is to develop rules, norms and principles of responsible behaviour of States; devise ways to implement these rules; identify CBMs and capacity-building measures; and study cyber threats and the application of international law to cyberspace.

The first OEWG of 2019-20 conducted substantive sessions and consultative meetings, allowing UN member states to participate along with other stakeholders such as the academia, industry, and non-government organisations. Its final report, adopted on 12 March 2021, included a set of recommendations on "Rules, Norms and Principles for Responsible State Behaviour, International Law, Confidence-building Measures, Cyber Capacity-building and Regular Institutional Dialogue".[43] The UN General Assembly has since established a new OEWG (2021-25) on security of and in the use of ICTs.[44] The second OEWG aims to build on the work of the GGEs and the previous OEWG and held its first organisational session in June 2021.

EU and Indian positions on the UN OEWG

The EU participated in the first OEWG, contributing interventions and submissions on behalf of EU member states throughout the deliberations. Since the second OEWG began its deliberations, the EU has made submissions to the second OEWG substantive session in 2022 on each of the topics under discussion, namely: organisational matters; existing and potential threats; further developing and implementing the rules, norms and principles of responsible state behaviour; how international law applies to states' use of ICTs; CBMs; capacity-building and regular institutional dialogue.

India actively participated in the first OEWG and contributed substantively towards its final report. In its statement at the June 2019 Organisational Session of the first OEWG, India stated that a *"common understanding on how international law is applicable to State's use of ICTs is important for promoting an open, secure, stable, accessible, interoperable and peaceful ICT environment."*[45] It assured full support to the OEWG, and also provided comments on the initial pre-draft of the OEWG's report[46] and on the zero draft of the OEWG's final substantive report. As mentioned in Section 3.2.1 of this report, in 2021 India lauded the outcomes of the OEWG, and noted the need to build further on its deliberations and the points of consensus achieved.

The Proposed Programme of Action (PoA)

In October 2020, over 40 countries (including EU member states) proposed the establishment of a Programme of Action (PoA) for advancing responsible state behaviour in cyberspace. The PoA seeks to end the dual-track discussions of the GGE and OEWG, and to establish a permanent UN forum to consider the use of ICTs by states in the context of international security. It is envisaged as a single, long-term, inclusive and progress-oriented platforms.[47]

The PoA is expected to offer UN member states newer opportunities to create a framework and political commitment based on recommendations, norms and principles already agreed; have regular, implementation-focused working-level meetings; step up cooperation and capacity building; conduct regular review conferences to ensure the PoA's relevance; and conduct multistakeholder consultations on cyber-related issues.

EU and Indian positions on the PoA

The proposed PoA has met with a mixed response. The EU, through the High Representative together with its member states, aims to take forward their inclusive and consensus-based proposal for a political commitment on the PoA in the UN. The EU's Cybersecurity Strategy specifies that building on the existing acquis as endorsed by the UN General Assembly, the PoA offers a platform for cooperation and exchange of best practices within the UN, and a possible mechanism to implement the norms of responsible state behaviour and promote capacity development.

Some stakeholders believe that the PoA could indeed act as an effective way forward by combining the best of the GGE and OEWG; and eliminating the redundancies and duplications of having two bodies dealing with similar issues and being more inclusive, action-oriented and impactful.[48] India and several other states, however, see a possibility of future discussions on ICTs and cybersecurity continuing within the framework of the OEWG 2021–25.[49] In February 2022, in response to a Parliament Question about the Indian stance on the PoA, the Ministry of External Affairs (MEA) simply noted that "India has been participating in UN-mandated cyber processes and consultations".[50]

Actionable Recommendations

The March 2022 roundtable in New Delhi on enhancing global cybersecurity cooperation served as a curtain-raiser for the ESIWA–ORF roundtable series. Existing cyber efforts between the EU and India were highlighted, and a concise description of international processes for cyber cooperation was provided. The deliberations were guided by three questions:

- How can EU and Indian diplomatic officials in charge of cyber issues cooperate bilaterally and multilaterally to increase adherence to cyber norms and implementation of cyber confidence-building measures?

- How can EU and Indian private sector stakeholders be best involved in implementing the normative framework for responsible state behaviour in cyberspace?

- How can the EU and India jointly address, on a bilateral and multilateral basis, the rise in increasingly lucrative and organised forms of cybercrime such as ransomware?

Based on the roundtable discussions, the authors of this report have drafted seven actionable recommendations. These will be put forward for formal discussions between the EU and India, and eventually will be submitted for consideration during the EU-India Cybersecurity Dialogue meetings.

Recommendation 1: Build upon and expand EU-India cyber interactions.

The EU and India could build upon existing cyber interactions by exchanging best practices and lessons learned on the implementation of cyber norms. Both parties could work towards enforcing and promoting responsible behaviour through diplomatic means; engage in discussions on the drafting and implementation of relevant international standards for new technologies such as 5G; and undertake joint efforts to advance global cyber resilience. The Indian government has expressed interest in having points of contact among agencies through which it can share information transnationally. Dedicated EU and Indian points of contact at the policy and technical levels could therefore be appointed to provide guidance for determining cyber roles and responsibilities, coordination functions, and readiness requirements.

Recommendation 2: Promote multistakeholder engagement at various levels.

The EU and India agree that multistakeholder initiatives have a valuable contribution to make towards governmental policy positions. However, non-governmental stakeholders sometimes confirm that it is difficult to have their perspectives heard at intergovernmental forums. The EU and India could forge a joint agreement on how they could advance multistakeholder engagement both domestically and internationally, with clearly formulated guidelines for interaction.

Private sector inputs are deemed crucial for international processes, and there is a need to ensure that the latter encourage companies to become involved. As a first step, specialised working groups or bodies in the EU and India that include representatives of both government agencies and industry must be encouraged. These groups could then come together, ideally through regular initiatives of the groups' chairs. Such approaches could be crucial for building public-private consensus and partnerships and could foster a more inclusive ecosystem for cyber cooperation. Relevant subjects for public-private collaboration could include protecting the core stability of the Internet; supply chain security; security-by-design; committing not to hack-back; and commitments not to cyber-attack citizens.

Recommendation 3: Jointly undertake capacity-building exercises and confidence-building measures.

The EU and India agree that undertaking joint capacity building exercises and confidence building measures (through training, and the sharing of knowledge and best practices) is necessary, and that private sector and academic stakeholders should be involved, particularly in areas such as promoting cybersecurity, strengthening encryption standards, and developing the capacity of cyber professionals. It is believed that the limited engagement of several Member States with UN processes on cybersecurity could be because of a lack of capacities. The EU and India could therefore cooperate to help close capacity gaps in third countries[b] with respect to cyber diplomacy and cybercrime. European and Indian experiences and mechanisms related to cybersecurity could act as a valuable guide for other nations to bolster their cyber-capabilities. Support to third countries could also be strategic, focusing on issues such as helping eradicate the safe havens for cybercriminals operating out of these countries; or facilitating cooperation among third countries from an enforcement perspective.

The Indo-Pacific region presents a potential new theatre for activities directed at enhancing global cybersecurity. India is already a key actor in the region, and with the EU's adoption of its Indo-Pacific strategy in September 2021, the region could present new opportunities for EU-India-supported capacity development and confidence-building exercises.[51] Strengthening capabilities to counter ransomware in particular could be an important area of intervention.[c]

Finally, cybercrime prevention and awareness-raising efforts ought to be a critical component of all capacity-building initiatives as the weakest link is sometimes the person(s) handling the computer. Evolving a joint approach to awareness raising among citizens, bilaterally and multilaterally, would thus be valuable.

[b] For instance, the EU Global Gateway initiative is planning to build data centres in several countries, including in Africa. Capacity building initiatives could be combined in various ways.

[c] The EU and India are already part of the International Counter Ransomware Initiative (ICRI) established by the United States to fight ransomware. Of the several panels set up by the ICRI, India and Lithuania chair the panel on resilience; Australia chairs the panel on disrupting ransomware; the UK chairs the panel on countering the illicit use of cryptocurrency; and Germany chairs the cyber diplomacy panel. The Initiative is a public-private partnership, and most EU Member States are already members.

Recommendation 4: Explore the implications and possible benefits of the Programme of Action.

Supporters of the proposed Programme of Action (PoA), including the EU, see it as a possible action-oriented UN forum that could help further the practical implementation of cyber-tools, promote joint efforts for capacity building, and operationalise cyber norms and principles through multistakeholder engagement. India is closely following developments regarding the PoA and is keen to better understand how it will be shaped, while remaining interested in its possible evolution as a forum for action. It is important therefore that the implications and potential benefits of the PoA are more closely explored, discussed and understood by both sides. The PoA's possible potential for adopting approaches of common interest – such as taking a regional approach to understand and address the needs of individual Member States – could also be examined by the EU and India in greater detail.

Recommendation 5: Work towards crafting new standards for data governance and data sharing.

From a non-governmental perspective, the EU and India could work towards showcasing to the world a new approach for creating standards in two areas, namely how data governance can be conducted and how data can be shared swiftly (with or without MLAT requirements). Given that most platforms tend to come from the United States or China, there is a perceived need for a third non-aligned platform. The EU and India could jointly identify (a) what data can be shared and how, and (b) the common standards required for the data and infrastructure layers in question. Both parties could then aim to work towards creating a common joint platform which sets standards in a non-aligned manner. Political dialogue between both parties and a shared normative framework could advance mutual trust and the agenda on data.

Recommendation 6: Work towards developing global standards in selected domains.

With a view towards building open, secure public digital infrastructure, the EU and India could work towards developing global standards in domains such as cryptocurrency regulation, anonymity, and counter ransomware. Other immediate areas for cooperation could include setting standards to enhance the security of software and of digital supply chains.

Recommendation 7: Continue to build trust through increased cooperation.

The EU and India could achieve much through continued bilateral and multilateral cooperation, and building mutual trust should a key focus of future cyber efforts. Towards this end, sustained interactions should be undertaken at European cybercrime platforms and conferences, and at the new UN Cybercrime Ad Hoc Committee (which is still at a nascent stage of its negotiations and thus presents an opportunity for the EU and India to coordinate on key issues of mutual interest). There is also a need to conduct exchanges on a possible future Convention in the UN Third Committee, and to build upon the deliberations of the existing UN Intergovernmental Expert Group on Cyber Crime. Finally, it is important to ensure that crime does not pay. The EU and India could therefore collaborate to strengthen mechanisms for facilitating cybercrime investigations across borders, along with freezing and confiscations measures directed against perpetrators of cybercrime and cross-border restitution measures for victims.

Conclusion

The EU and India share many common interests and face a range of shared concerns in the domain of cybersecurity. Both parties support an open, free and secure cyberspace and acknowledge that this can be achieved through the promotion of international law and standards.

The present ESIWA-ORF project will complement the official EU-India interactions on cybersecurity. Several points made during the first roundtable have drawn attention to areas where further emphasis, interventions, and support would be beneficial, such as joint cyber capacity building, cooperating to counter ransomware and cybercrime, raising citizens' awareness about confronting and preventing cybercrime, and participating in joint table-top exercises. These issues will be incorporated into formal bilateral discussions, and will be put forward for further consideration at EU-India Cybersecurity Dialogue meetings.

Future ESIWA-ORF roundtables will identify related areas for possible cooperation and joint activity. These could include: defending against data breaches and cyber-attacks; using emerging technologies to fight cybercrime; exploring measures that states could take to ensure a balance between cybersecurity and free speech; and deliberating upon the ongoing process of drafting a comprehensive UN cybercrime treaty. As recommended, a multistakeholder approach involving governments, civil society organisations, and the private sector will be adopted across efforts to enhance cybersecurity cooperation.

About the Authors

Cormac Callanan is Thematic Coordinator for Cybersecurity of the ESIWA project.

Basu Chandola is Associate Fellow at ORF.

Hannes Ebert is Head of the Cyber Programme (Digital Conflict Department) at the Centre for Humanitarian Dialogue.

Caitriona Heinl is Executive Director at The Azure Forum for Contemporary Security Strategy.

Anirban Sarma is Senior Fellow at ORF's Centre for New Economic Diplomacy.

Acknowledgments

This publication was produced with the financial support of the European Union, the German Federal Foreign Office and the French Ministry for Europe and Foreign Affairs.

Endnotes

1. Ministry of Defence, Government of India, “EU-India Joint Naval Exercise”, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1729021

2. “India, EU hold first-ever security, defence consultations”, *The Economic Times*, June 12, 2022, https://economictimes.indiatimes.com/news/defence/india-eu-hold-first-ever-security-defence-consultations/articleshow/92165767.cms

3. EEAS, “India-EU: Joint press release on launching the Trade and Technology Council’, https://www.eeas.europa.eu/eeas/india-eu-joint-press-release-launching-trade-and-technology-council_en

4. Ministry of External Affairs, Government of India, “6th India-EU Cyber Dialogue”, https://www.mea.gov.in/press-releases.htm?dtl/33308/6th_IndiaEU_Cyber_Dialogue

5. Ministry of External Affairs, Government of India, “Joint Statement of the 15th India-EU Summit”, https://www.mea.gov.in/bilateral-documents.htm?dtl/32827/Joint_Statement_of_the_15th_IndiaEU_Summit_July_15_2020

6. Gateway House: Indian Council on Global Relations, *Moving forward the EU-India Security Dialogue: Traditional and emerging issues*, EU-India Think Tank Twinning Initiative, 2016, https://www.gatewayhouse.in/wp-content/uploads/2016/12/EU-India-Security-Dialogue-Cyber-Security.pdf

7. European Commission, “India-EU Working Group advances joint commitment for digital collaboration”, https://digital-strategy.ec.europa.eu/en/news/india-eu-working-group-advances-joint-commitment-digital-collaboration

8. “McAfee report says cybercrime to cost world economy over $1 trillion”, *Business Standard*, December 7, 2020, https://www.business-standard.com/article/technology/mcafee-report-says-cybercrime-to-cost-world-economy-over-1-trillion-120120700249_1.html

9. Nick Paton Walsh, “Serious cyberattacks in Europe doubled in the past year, new figures reveal, as criminals exploited the pandemic”, *CNN*, June 10, 202, https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html

10. “11% jump in cyber crime in 2020, NCRB data in Home Panel report”, *Business Standard*, February 11, 2022, https://www.business-standard.com/article/current-affairs/11-jump-in-cyber-crime-in-2020-ncrb-data-in-home-panel-report-122021100189_1.html#

11. “1.55 million cyber security incidents in 2019, 2020: Govt tells Lok Sabha”, *Business Standard*, March 23, 2021, https://www.business-standard.com/article/current-affairs/1-55-million-cyber-security-incidents-in-2019-2020-govt-tells-lok-sabha-121032300712_1.html

12. *Microsoft Digital Defense Report*, 2021, Microsoft, https://aka.ms/microsoftdigitaldefensereport

13. "India ranks third in global data breaches in 2021: Report", *Business Today*, December 15, 2021, https://www.businesstoday.in/latest/trends/story/india-ranks-third-in-global-data-breaches-in-2021-report-315750-2021-12-15

14. "Cybercrime cases recorded a fivefold jump in 3 years: Govt", *Hindustan Times*, April 08, 2022, https://www.hindustantimes.com/india-news/cybercrime-cases-recorded-a-fivefold-jump-in-3-years-govt-101649357021073.html

15. Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021*, Publications Office of the European Union, 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

16. UNODC, *Comprehensive Study on Cybercrime*, UN, 2013, https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

17. Ministry of External Affairs, Government of India, "4th India-EU Summit - Joint Press Statement", https://mea.gov.in/bilateral-documents.htm?dtl/7700/4th_IndiaEU_Summit__Joint_Press_Statement

18. Ministry of External Affairs, Government of India, "India-EU Joint Declaration on International Terrorism", https://mea.gov.in/bilateral-documents.htm?dtl/5247/IndiaEU_Joint_Declaration_on_International_Terrorism

19. Ministry of External Affairs, Government of India, "India-EU Joint Statement on the 13th India-EU Summit", https://mea.gov.in/bilateral-documents.htm?dtl/26576/IndiaEU_Joint_Statement_on_the_13th_IndiaEU_Summit_Brussels; Ministry of External Affairs, Government of India, "India – EU Joint Statement during 14th India-EU Summit", https://mea.gov.in/bilateral-documents.htm?dtl/29011/India__EU_Joint_Statement_during_14th_IndiaEU_Summit_New_Delhi_October_06_2017

20. Ministry of External Affairs, Government of India, "Joint Statement of the 15th India-EU Summit", https://mea.gov.in/bilateral-documents.htm?dtl/32827/Joint_Statement_of_the_15th_IndiaEU_Summit_July_15_2020

21. Ministry of External Affairs, Government of India, "India-EU Connectivity Partnership", https://mea.gov.in/bilateral-documents.htm?dtl/33854/IndiaEU_Connectivity_Partnership and Ministry of External Affairs, Government of India, "Joint Statement on India-EU Leaders' Meeting", https://mea.gov.in/bilateral-documents.htm?dtl/33853/Joint_Statement_on_IndiaEU_Leaders_Meeting_May_08_2021.

22. Ministry of External Affairs, Government of India, "India-EU Strategic Partnership: A Roadmap to 2025", https://mea.gov.in/bilateral-documents.htm?dtl/32828/IndiaEU_Strategic_Partnership_A_Roadmap_to_2025

23. Ministry of External Affairs, Government of India, "Joint Press Release of the 12th India-European Union Counter Terrorism Dialogue", https://mea.gov.in/press-releases.htm?dtl/33217/Joint_Press_Release_of_the_12th_IndiaEuropean_Union_Counter_Terrorism_Dialogue

24. Ministry of External Affairs, Government of India, “6th India-EU Cyber Dialogue”

25. “India-EU Working Group advances joint commitment for digital collaboration”, *EC*, April 23,2021, https://digital-strategy.ec.europa.eu/en/news/india-eu-working-group-advances-joint-commitment-digital-collaboration

26. “India-EU Working Group advances joint commitment for digital collaboration”, *EC*, April 23, 2021, https://digital-strategy.ec.europa.eu/en/news/india-eu-working-group-advances-joint-commitment-digital-collaboration

27. Jose de Arimatéia da Cruz, “The Legislative Framework of the European Union (EU) Convention on Cybercrime”, in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, ed. T Holt and A Bossler (London: Palgrave Macmillan, 2020)

28. U.S. Government Publishing Office, “Senate Executive Report 109-6 on Council of Europe Convention on Cybercrime” https://www.govinfo.gov/content/pkg/CRPT-109erpt6/html/CRPT-109erpt6.htm.

29. Council of Europe, “Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY”, https://www.coe.int/en/web/cybercrime/parties-observers

30. Council of Europe, “Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems”, https://rm.coe.int/168008160f

31. Council of Europe, “Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems”, https://rm.coe.int/168008160f

32. Deepak Parashar, “Budapest Convention On Cybercrime: Assessment Of India’s Concerns”, ILI Law Review II, 2019 126, https://www.ili.ac.in/pdf/dpa.pdf

33. Deepak Parashar, “Budapest Convention On Cybercrime: Assessment Of India’s Concerns”; See also Joyce Hakmeh, “Building a Stronger International Legal Framework on Cybercrime”, *Chatham House*, June 6, 2017, https://www.chathamhouse.org/2017/06/building-stronger-international-legal-framework-cybercrime; Alexander Seger, “India and the Budapest Convention: Why Not?” *ORF*, October 20, 2016, https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/; Anja Kovacs, “India and the Budapest Convention: To sign or not? Considerations for Indian stakeholders”, *Internet Democracy Project*, March 31, 2016, https://internetdemocracy.in/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders.

34. "Countering the use of information and communications technologies for criminal purposes : resolution / adopted by the General Assembly", *UN Digital Library*, https://digitallibrary.un.org/record/3841023?ln=en

35. "The UN Group of Governmental Experts (GGE)", *DigWatch*, https://dig.watch/processes/un-gge#Past-processes

36. UNGA, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, July 14, 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

37. "UN OEWG and GGE", *DigWatch*, https://dig.watch/processes/un-gge

38. Ministry of External Affairs, Government of India, "Question No. 1735: Cyber Security Policy", https://www.mea.gov.in/lok-sabha.htm?dtl/34851/QUESTION_NO1735_CYBER_SECURITY_POLICY

39. Asoke Mukerji, "International Cooperation on Cyberspace: India's Role", *Distinguished Lectures*, Ministry of External Affairs, April 04, 2018, https://mea.gov.in/distinguished-lectures-detail.htm?743

40. "Statement delivered by India at the Organisational Session of the OEWG", Permanent Mission of India to the Conference on Disarmament, Geneva, June 3, 2019, https://meaindia.nic.in/cdgeneva/?8251?000

41. "Statement delivered by India at the Organisational Session of the OEWG", Permanent Mission of India to the Conference on Disarmament, Geneva

42. Open-ended working group on developments in the field of information and telecommunications in the context of international security, "Final Substantive Report", https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

43. Open-ended working group on developments in the field of information and telecommunications in the context of international security, "Final Substantive Report"

44. "UN OEWG and GGE", *DigWatch*

45. "Statement delivered by India at the Organisational Session of the Open-Ended Working Group (OEWG) on 'Developments in the field of Information and Telecommunications in the context of International Security' in New York on June 3, 2019" https://eoi.gov.in/eoisearch/MyPrint.php?8251?001/0002 .

46. Permanent Mission of India to the Conference on Disarmament, Geneva, "Statement delivered by India at the Organisational Session of the OEWG".

47. "The future of discussions on ICTs and cyberspace at the UN", October 8, 2020, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

48. "A statement on the Programme of Action: A standing UN body to uphold international expectations is the best hope for stability in cyberspace", *Cybersecurity Tech Accord*, October 18, 2021, https://cybertechaccord.org/a-statement-on-the-programme-of-action-a-standing-un-body-to-uphold-international-expectations-is-the-best-hope-for-stability-in-cyberspace/

49. Pavlina Ittelson, "What's new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis", *Diplo*, March 19, 2021, https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis/

50. Ministry of External Affairs, Government of India, "Question No. 1735: Cyber Security Policy", https://www.mea.gov.in/lok-sabha.htm?dtl/34851/QUESTION+NO1735+CYBER+SECURITY+POLICY

51. Garima Mohan, "Where Does Europe Fit in India's Indo-Pacific Policy?", *Sasakawa USA*, https://spfusa.org/wp-content/uploads/2022/03/Dr.-Garima-Mohan-Paper_PDF.pdf

OBSERVER
RESEARCH
FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org