Framework for the UK-India Cyber Relationship

1. Shared Principles

Cooperation on cyber issues is a key component of the bilateral relationship between India and the United Kingdom. The two countries have created a wide-ranging strategic partnership that reflects their shared values, democratic traditions, national security and economic interests, and common vision and principles for cyberspace. Consistent with their respective domestic laws and international obligations, shared principles for the UK-India cyber relationship include:

A commitment to a free, open, peaceful and secure cyberspace;

A commitment to maintaining the increasing economic and social benefits accruing from the growth in use of the Internet;

A recognition of the importance of bilateral, multilateral, and multi-stakeholder cooperation for combating cyber threats, promoting cyber security and recognising the threats posed to our prosperity and national security by malicious cyber acts from state and non-state actors;

A commitment to promoting the free flow of information across borders while respecting domestic and international legal frameworks for privacy, data protection and data access;

A commitment to promote international security and stability in cyberspace through a framework that recognises the applicability of international law to state behaviour, in particular the UN Charter as the foundation for state behaviour in cyberspace;

A commitment to operationalise mutually agreed voluntary norms of responsible state behaviour and promote confidence building measures that can build trust between responsible states;

A recognition of the importance of and a shared commitment to cooperate in capacity building;

A commitment to promote, protect, and respect human rights and fundamental freedoms online;

A commitment not to conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;

A commitment to the multi-stakeholder approach to Internet governance that is transparent and accountable to its stakeholders, including governments, civil society, the technical community, academia and the private sector, and promotes cooperation among them;

A recognition of the leading role for governments in cyber security with the cooperation of other stakeholders;

A desire to cooperate in strengthening the security and resilience of critical information infrastructure;

A commitment to support the development and use of mutually acceptable international standards and best practices for technology products and services;

A recognition of the importance of open and secure internet access as an enabler for achieving the Sustainable Development Goals;

A commitment to share knowledge on skills initiatives in cyber security;

A recognition that cyberspace can promote inclusiveness in the delivery of services offered through digital governance.

2. Main Areas of Cooperation

India and the United Kingdom seek to cooperate in the following main areas:

1) Exchanging information and strategies for effective cyber security incident management and threat response;
2) Exchanging, in a timely manner, information relating to cyber security incidents, exchanging analytical products on cyber security where possible and mutual response to cyber security incidents;
3) Promoting cooperation in the fields of cyber security-related research and development; cyber security standards and security testing, including accreditation process; and cyber security product development, including further consultations on such issues;
4) Elaborating and implementing practical measures that contribute to the security of ICT infrastructure on a voluntary and mutual basis;
5) Continuing to promote cooperation between law enforcement agencies to combat cybercrime including through enhancing dialogue and developing enabling processes and procedures, and setting up consultations as needed;
6) Promoting the applicability of international law, including the UN Charter, to responsible state behaviour in cyberspace and further exploring how it applies to state conduct in cyberspace;
7) Promoting voluntary norms of responsible state behaviour in peacetime, including the norms identified by the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security;
8) Developing a common and shared understanding of international cyber stability, and destabilising cyber activity;
9) Discussing and sharing strategies to promote the integrity of the supply chain to enhance user confidence in the security of ICT products and services;
10) Sharing experience of working to promote cyber security in the private sector;
11) Promoting and supporting industrial and academic cooperation on cyber security;
12) Promoting the multi-stakeholder approach to Internet governance;
13) Continuing our dialogue and engagement in Internet governance fora, including ICANN, IGF and other venues, and to support active participation by all the stakeholders of the two countries in these fora;
14) Pursuing cooperation in formal dialogue and coordination in international forums such as the ITU, CSTD and the CTO.

3. Main Forms and Mechanisms of Cooperation

(1) India and the United Kingdom intend to continue to meet and hold an annual Cyber Dialogue led by the Director for Cyber Affairs at the UK Foreign, Commonwealth & Development Office and the Joint Secretary for Cyber Diplomacy at the Ministry of External Affairs, India. This Cyber Dialogue is expected to review cooperation on cyber policy issues, including the implementation of this framework. This Cyber Dialogue will incorporate a broad range of relevant departments across both governments with a view to facilitating a more collaborative working process between relevant Ministries.

(2) The United Kingdom and India may designate Points of Contact in specific areas of cooperation provided for in this framework. Within 60 days after this framework becomes operative, the Participants intend to exchange information through diplomatic channels on their Authorised Agencies and Point of Contacts.

(3) The Participants intend to continue to promote incident management cooperation, including, but not necessarily limited to, through established mechanisms.

(4) The Participants intend to continue to promote and improve cybercrime cooperation, including through established mechanisms, and, in particular, the Treaty between the Government of the United Kingdom and the Government of the Republic of India on Mutual Legal Assistance in Criminal Matters.

4. Period of Framework

(1) This framework is expected to remain in place for a period of five years from the date of its signature.

(2) The Participants may modify this framework by reaching a mutual understanding. The Participants expect that such an understanding would be in written form.

(3) This framework may be discontinued by either Participant at any time in any manner, but preferably not earlier than 90 days after it becomes operative. The Participants expect the Participant discontinuing this framework to provide written notification, through diplomatic channels, to the other Participant of its intention to do so.

(4) If the framework is discontinued, the Participants intend to continue to protect information as well as to implement previously decided joint activities and projects carried out under this understanding and not completed upon discontinuation of this understanding.

In witness whereof, the following representatives duly authorized by their respective governments have signed this framework in two originals in the English language.

Signed by the Government of the United Kingdom and the Government of the Republic of India, April 2018