SPRING 2020 / ISSUE NO.16

$ 15.00 | € 10.00 | 1500 RSD

HORIZONS

JOURNAL OF INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

PANDEMICS & GEOPOLITICS
THE QUICKENING

UNLOCKING THE MIDDLE EAST

SUSTAINABLE CYBERSPACE

ISSN 2406-0402

ABDELAL • BREMMER • BROS • DAVUTOĞLU • DUCLOS • DURBIN
FAHMY • FEDOROV • FRIEDMAN • HEISTEIN • HOFMAN • KORTUNOV • KUMAR
MUKERJI • RUBIN • SACHS • SARIOLGHALAM • SINGH • TERZIC • YADLIN

cirsd.org

The Need for an International Convention on Cyberspace

Asoke Mukerji

OVER the past three decades, a convergence of information and communication technologies (ICTs), together with various governance policies, have created what we now call "cyberspace." Today cyberspace is a living reality, influencing all aspects of human behavior. The need to create a universal and transparent global framework to ensure the effective security and utilization of cyberspace "for the economic and social advancement of all peoples" has become paramount. How can this be achieved?

Governments addressed this issue more than two decades ago, when the UN General Assembly (UNGA) adopted its first resolution on ICTs in December 1998. Other stakeholders including businesses, academia, and civil society have become more articulate in seeking a supportive international framework for their activities in cyberspace. As the United Nations marks its Seventy-fifth anniversary this year, and notwithstanding the truly unpredictable effects of the COVID-19 pandemic, I believe the time has come to launch a broad-based multi-stakeholder process that can culminate in the adoption of an international convention on cyberspace.

Cyberspace and its Stakeholders

Emerging concepts related to the application of cyber technologies are propelling the world into the Fourth Industrial Revolution. The Internet of Things (IoT), artificial intelligence (AI), and robotics are expected to dominate cyberspace and redefine the role of human beings in this domain within just a few short years. While these phenomena are currently being tested and applied within a few countries, their impact will be felt globally due to the complex interlinkages of cyberspace. These interlinkages revolve around cyber technologies and infrastructure.

Photo: Pixabay

"Cyberspace is a living reality, influencing all aspects of human behavior."

A broad understanding of the internet incorporates cyber technologies such as wireless and fixed broadband, smartphones, the mobile internet, and cloud computing. Critical national infrastructures as well as social media platforms enable the flow of data across cyberspace, using a global network of fiber-optic cables and 13 primary root-servers that direct this data to its destination. The potential of cyberspace for the progress of mankind is immeasurable when it functions in a holistic manner. On the other hand, any fragmentation of this domain could have unfathomable ramifications.

The four main stakeholders in cyberspace acknowledged by the UNGA are governments, businesses, academia, and civil society. These stake-

Asoke Mukerji *was India's former Permanent Representative to the United Nations in New York and supervised India's participation in negotiations that resulted in the adoption of the UN 2030 Agenda for Sustainable Development. More recently, he chaired a multi-stakeholder Study Group under the National Security Council Secretariat of India to recommend cyber norms for the country.*

holders are active in varying degrees within most UN member states.

Of these four, governments have the primary responsibility for cyberspace policies, including cyber-security, and the application of cyber technologies for national governance objectives. Thus, governments have an obligation to ensure effective international cooperation in cyberspace to meet these objectives. Two broad areas where governments have taken the lead are in discussing and agreeing on norms for securing cyberspace, and in using ICTs for socio-economic development.

The time has come to launch a broad-based multi-stakeholder process that can culminate in the adoption of an international convention on cyberspace.

Businesses have a major impact on how governments formulate cyber policies nationally, and how they approach cooperation on cyber issues globally. Due to their focus on innovation, and the application of cyber technologies that they have patented or copyrighted, businesses see cyberspace as a new frontier for growth and profit. The emergence of a global trade framework for regulating e-commerce adds urgency to the interest of businesses for a predictable and effective international framework for cyberspace.

Academia plays a key role in research and development, innovation, and the conceptualization of theories regarding cyberspace to give them global relevance. Many of these theories are brought into the wider world through governments or businesses. As cyber activities increase across the world, the role of academia in creating essential building blocks of awareness about cyberspace, including imparting cyber skills and values through education, has become more significant.

Civil society focuses on the impact of the activities of governments, businesses, and academia in cyberspace with a special focus on the human dimension. Issues such as ease of access to new cyber platforms and technologies and the use of these for empowering the individual and society, bridging digital divides, and upholding fundamental human rights and freedoms in cyberspace are priorities for civil societies across the world.

All four stakeholders—governments, businesses, academia, and civil society—play a critical role in identifying the strengths and vulnerabilities of cyberspace. In varying degrees around the world, all four have expressed interest in creating the building blocks for a multi-stakeholder international framework for cyberspace.

The Global Conferences on Cyberspace

At the global level, issues in cyberspace that require effective international cooperation have been raised by the five multi-stakeholder Global Conferences on Cyber Space held so far, beginning with the London Conference in 2011.

The London Conference identified five broad themes for international cooperation in cyberspace. These were economic growth and development, social benefits, international security, tackling cybercrime and ensuring safe and reliable access to cyberspace.

Subsequently, similar global conferences have taken place Budapest in 2012, which highlighted the importance of capacity building in cyberspace, the linkage between internet security and internet rights, as well as the role of civil society in cyberspace policies; Seoul in 2013, which highlighted the need for universal access to cyberspace to accelerate development; and The Hague in 2015, which established a Global Forum on Cyber Expertise (GFCE) to promote capacity-building.

The Fifth Global Conference on Cyber Space was hosted by India in 2017, with a focus on "a secure and inclusive cyberspace for sustainable development." The intent of the conference was to promote the importance of inclusiveness and human rights in global cyber policy, to defend the status quo of an open, interoperable and unregimented cyberspace, to create political commitment for capacity building initiatives to address the digital divide and assist countries, and to develop security solutions in a balanced fashion that duly acknowledge the importance of the private sector and technical community.

Securing Cyberspace

Within the United Nations, governments have taken the initiative to address the potential and also the dangers of cyberspace. In 1998, they adopted a resolution in the UNGA that noted the use of ICTs for both civilian and military purposes and prioritized "civilian applications." The resolution mandated the definition of "basic notions related to information security," while "developing international principles" to enhance cyber-security.

The three broad areas that governments have taken up since 1998 to develop international cooperation in cyberspace relate to norms for cyber-security, measures to counter cybercrime, and agreeing on cyber policies for accelerating effective governance.

In 2002 the UNGA adopted a resolution to create a regulatory framework for securing cyberspace. Dealing with the "global culture of cyber-security," this resolution highlighted nine elements that could contribute to such a global culture. These elements included awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment.

Subsequently, in a resolution adopted by the UNGA in 2003, the UN Secretary-General was given the responsibility to seek the assistance of a Group of Governmental Experts (GGE) to develop norms for securing cyberspace. The GGE's mandate was very specific. It was asked to formulate recommendations in the context of "disarmament, global challenges and threats to peace that affect the international community…and challenges to the international security regime."

> *The three broad areas that governments have taken up since 1998 to develop international cooperation in cyberspace relate to norms for cyber-security, measures to counter cybercrime, and agreeing on cyber policies for accelerating effective governance.*

On the ground, the work of the GGE since its inception in 2004 has been deeply influenced by the way the UN Secretary-General has nominated governmental experts. In the absence of a roster of such experts in the United Nations, the Secretary-General has appointed individuals on the "basis of equitable geographical distribution and with the help of Member States in a position to render such assistance."

Despite this apparent concession to equitable representation, however, the Secretary-General has consistently nominated governmental representatives of the five permanent members of the UN Security Council (China, France, Russia, the United Kingdom, and the United States) to the various GGEs. In contrast, the Secretary-General has applied the principle of rotation for selecting experts from other member states.

The Secretary-General's approach has played into the growing polarization among the five permanent members of the UN Security Council, which is now reflected in the GGE process as well. One outcome has been to make the GGE dependent on the emerging interests and priorities (often not directly linked to cyberspace) of the five permanent members of the UN Security Council. In 2015, the GGE agreed to recommend norms for securing cyberspace, which were endorsed by the UNGA. An issue on which the five permanent members have confronted each other in the GGE is that of attributing attacks in cyberspace, and consequent counter measures. This has delayed implementing the agreed norms through transparent voluntary measures or a more robust legal framework.

To overcome the deadlock, the UNGA adopted a resolution in December 2018 to enhance "broad international cooperation." It decided to convene another GGE to focus on how international law applies to cyberspace and mandated the GGE to engage in multi-stakeholder consultations to generate greater acceptability for its eventual recommendations. The reconvened 25-member GGE mandated by the aforementioned resolution held its first meeting a full year later, in December 2019.

In the meetings of the current GGE held so far, new areas of discussion have included the emergence of new cyber technologies and platforms (like social media) for the application of such technologies. Apart from its core mandate for recommending norms for cyber-security, the GGE discussions encouraged the identification of voluntary confidence-building measures and capacity-building to enhance cyber-security. The outcome of this GGE is to be reported to the UNGA in 2021, which in the UN context translates into a demonstration of the increasing urgency being felt by governments for effective international cooperation in securing cyberspace.

In response to growing criticism that a majority of UN member states and other stakeholders in cyberspace were being excluded from contributing their perspectives to a global dialogue on cyber-security, the UNGA also adopted a resolution in December 2018 establishing an Open-Ended Working Group (OEWG) to make the discussions "more democratic, inclusive, and transparent." The OEWG established by the UNGA has met from June 2019 onwards. The OEWG is scheduled to hold its final substantive session in July 2020 in New York, although this may have to be pushed back due to the COVID-19 pandemic.

Besides governments, the OEWG discussions on cyber-security have brought in businesses, non-governmental organizations, and academia. The multi-stakeholder discussions held so far have revealed important gaps in securing cyberspace on the ground. These include "lack of data sharing and informed awareness of cyber threats" as well as "lack of will at the highest political levels." The discussions have noted that the GGE process had not fully considered the impact of new technological developments in cyberspace, which significantly enhanced cyber threats. Advocating a "holistic" approach to enhance cyber-security, participants have drawn attention to the linkages between economic security and cyber-security. Most significantly, discussions on cyber-security have emphasized, "a human-centric, rights-based approach that also emphasizes shared responsibility and accountability."

This is the broader context for the popular debates over new ICT technology like 5G, issues of ethics in applying AI to cyber activities, and assertions of sovereignty over the flow of data derived from traditional national jurisdictions ("data localization").

It is important to recognize the explicit incorporation by the UNGA of a "multi-stakeholder" approach. Such a multistakeholder approach can potentially integrate such issues into ongoing UNGA discussions on international cooperation in cyberspace—a point recently highlighted by the Chair of the OEWG.

Countering Cybercrime

The first major legal impetus for seeking inter-governmental cooperation in countering cybercrime came in November 2001 from the Council of Europe, which is comprised of 47 states and includes Russia but not the United States, China, and other non-European countries. The Council of Europe adopted the Budapest Convention on Cybercrime, emphasizing that an "effective fight against cybercrime requires increased, rapid, and well-functioning international cooperation in criminal matters."

Attempts to make the Budapest Convention universal in scope have been unsuccessful, so far. While the Council of Europe regulations provide for the accession of non-member states to the Budapest Convention, the procedures for enabling this include a requirement for a non-member state to make a written request for accession, and a scrutiny by Council experts on the "compatibility of the domestic law of the State concerned with the standards of the Council of Europe." In addition, non-member states would have to finance their participation in the Convention. These provisions act as a deterrent for sovereign states outside the Council of Europe, especially developing countries, from participating in the Convention on an equal basis.

The first major legal impetus for seeking inter-governmental cooperation in countering cybercrime came in November 2001 from the Council of Europe, which is comprised of 47 states and includes Russia but not the United States, China, and other non-European countries.

The Budapest Convention has issued guidance notes on countering 11 specific threats. These included threats to computer systems, botnets, trans-border access, identity theft, DDOS attacks, critical infrastructure attacks, malware, spam, subscriber information, terrorism, and election interference. The relevance of these issues for broadening universal international cooperation on countering cybercrime through the UNGA is obvious.

In December 2019, the UNGA adopted a resolution moved by Russia on countering "the use of information and communication technologies for criminal purposes." According to the Russian delegation, the next step would be for the UNGA to hold an "organizational session in New York in 2020," with negotiations on the text of "a comprehensive international convention on countering cybercrime" starting in 2021.

The aforementioned resolution sets the stage for the first inter-governmental negotiation in the UNGA on creating a legal framework to counter cybercrime. With its narrow focus on cybercrime, the proposed legal framework would be potentially falling short of the "holistic" approach towards securing cyberspace that is emerging as a template in international multi-stakeholder discussions.

Cyberspace and Sustainable Development

A holistic approach has characterized, so far, the UNGA's discussions on harnessing the impact of cyber technologies and platforms for sustainable development. The evolution of a supportive cyber environment for sustainable development, emphasizing a "people-centric" approach, has been cyclical.

The first cycle was launched by the UNGA in December 2001, when it adopted a resolution to hold a World Summit on the Information Society (WSIS) in two phases. In the first phase, which concluded in Geneva in 2003, agreement was reached on identifying principles and a plan of action to respond to the emergence of ICTs in socio-economic activities. In the second stage, which concluded in Tunis in 2005, UN member states committed their political support for these principles and activities.

Implementing the outcome of the Tunis meeting between 2005-2015 marked the second cycle of international attempts to support civilian priorities in cyberspace. An important dimension of the Tunis Agenda has been its focus on upholding the "respect for human rights and for fundamental freedoms for all" mentioned in the UN Charter. In its review of the Tunis Agenda in December 2015, the UNGA affirmed that "the same rights that people have offline must also be protected online."

The "Tunis Agenda" created an Internet Governance Forum (IGF) platform to enable multi-stakeholder discussions on how society should respond to the potential of cyberspace. The IGF witnessed a spirited debate between advocates of a business-driven model, whose policies would conform to the market-driven priorities set by the growing number of cyber technology corporations (often referred to as the "multi-stakeholder" model), and votaries of a more assertive role for government policies—i.e., both for law enforcement as well as for empowerment of societies, in order to bridge "digital divides" (referred to as the "multilateral" model). The fact that both approaches were convergent was finally acknowledged when the UNGA conducted its High-level Review of the implementation of the Tunis Agenda in December 2015.

The Review emphasized the importance of the need for effective international cooperation in cyberspace to achieve globally agreed goals of sustainable development. The review emphasized using cyber technologies to bridge the digital divides; equitable access to cyberspace; the creation of an enabling cyberspace environment for development; public-private partnerships in financing the growth of cyberspace; the online protection of human rights including the freedom of expression and privacy; and the management of the internet as a "multilateral, transparent, democratic, and multi-stakeholder" process. It extended the IGF by another 10 years.

Drawing upon extensive multi-stakeholder participation, the UNGA Review acknowledged that "the management of the internet as a global facility includes multilateral, transparent, democratic and multi-stakeholder processes, with the full involvement of Governments, the private sector, civil society, international organizations, technical and academic communities, and all other relevant stakeholders in accordance with their respective roles and responsibilities."

The third (and current) cycle of international multi-stakeholder activities attempting to regulate the use of ICTs for civilian activities began in September 2015, when the UNGA adopted the 2030 Agenda on Sustainable Development. The 2030 Agenda focuses on the 17 Sustainable Development Goals (SDGs) and the ambition is for all UN member states to fully achieve them all by 2030. In other words, the scope of the 2030 Agenda is ambitiously universal, applicable to both industrialized and developing countries. As the Preamble to the 2030 Agenda founding document asserts, there "can be no sustainable development without peace and no peace without sustainable development."

The targets for achieving each SDG have been set through multi-stakeholder negotiations in a ground-up approach. In the negotiations, it was agreed that technology would be prioritized to access the implementation of the SDGs under a Technology Facilitation Mechanism. The SDGs include poverty eradication; no hunger; good health and well-being; quality education; gender equality; clean water and sanitation; decent work and economic growth; industry, innovation, and infrastructure; reduced inequalities; sustainable cities and communities; responsible consumption and production; climate action; life below water; life on land; peace, justice, and strong institutions; and partnerships.

The outcome of this work in the UNGA has emphasized a "people-centered, inclusive, and development oriented" cyberspace, including for the application of cyber technologies to accelerate sustainable development.

> *The targets for achieving each SDG have been set through multi-stakeholder negotiations in a ground-up approach. In the negotiations, it was agreed that technology would be prioritized to access the implementation of the SDGs under a Technology Facilitation Mechanism.*

Businesses and Cyberspace

While governments have identified the key components for building a resilient international framework for cyberspace, major businesses have also realized the importance of such an international framework for their activities in cyberspace. Two such initiatives stand out.

Microsoft took the lead in February 2017 in proposing a framework for international cooperation in cyberspace through a "Digital Geneva Convention" to be adopted by governments. This idea was suggested by Microsoft to bring governments together to protect cyberspace, which it asserted "is owned and operated by the private sector." The objective of a "Digital Geneva Convention" would be for "the world's governments to pledge that they will not engage in cyberattacks on the private sector, that they will not target civilian infrastructure, whether it's of the electrical or the economic or the political variety." Microsoft has given the responsibility of creating such an international framework to governments.

At the Munich Security Conference in 2018, Siemens took the initiative to launch a Charter of Trust for enhancing cyber-security. Other major businesses associated with this initiative include AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, NXP, SGS, Total, TÜV Süd, and Japan's Mitsubishi Heavy Industries. The objective of the Charter is for the creation of "binding rules and standards to build trust in cyber-security and further advance digitalization," including for "the protection of data of individuals and businesses."

Such rules and standards would need to be integrated into an international framework applicable to businesses in cyberspace. Since 1995, the World Trade Organization (WTO) has been incrementally involved in cyber issues, from the negotiation of the Information Technology Agreement in 1996 and negotiations for ICTs' market access during its Telecoms Negotiations in 1997, to the adoption of a standstill agreement on not imposing customs duties on electronic transmissions in 1998 and the decisions of the WTO Dispute Settlement Body on many issues related to cyber products and processes involving businesses and governments.

Converging the WTO process with ongoing work in the UNGA will contribute to the resilience of efforts to create an international framework on cyberspace on the basis of international law. The opportunity to focus on such a convergence will be the next Ministerial Conference of the WTO, scheduled to be held in Kazakhstan in June 2020 (a delay is possible, again due to the COVID-19 pandemic).

High-level Panel on Digital Cooperation

As cyber technology transitions from the ICTs of the early twenty-first century to the digital world, the UN Secretary-General's initiative to convene a multi-stakeholder High-level Panel for identifying areas for Digital Cooperation provides a launching pad for the UNGA to create an appropriate international framework for cyberspace. The report of the Panel was presented to the UN Secretary-General in June 2019. It will form the basis for the process to coordinate multi-stakeholder discussions on cyberspace at the commemoration of the Seventy-fifth anniversary of the United Nations in September 2020.

Led by Melinda Gates of the Gates Foundation and Jack Ma of Alibaba, the Panel held nine months of consultations with governments, the private sector, civil society, international organizations, academia, and technical communities across the world. It made five specific recommendations for shaping a common future: building an inclusive digital economy and society; developing human and institutional capacity; protecting human rights and human agency; promoting digital trust, security, and stability; and fostering global digital cooperation.

The key conclusion of the Gates-Ma UN panel was to complement "multilateralism with multi-stakeholderism" in order to provide a strong foundation for international cooperation in cyberspace.

Towards an International Convention on Cyberspace

In November 1967, the UNGA had responded to a call for "an effective international regime over the seabed and the ocean floor beyond a clearly defined national jurisdiction." The outcome of that response was the discussion of "the freedom-of-the-seas doctrine with technological changes that had altered man's relationship with the ocean." This led to the Third UN Conference on the Law of the Sea in 1973, with the objective to negotiate a comprehensive treaty for the maritime domain. The outcome was achieved nine years later (in 1982) with the adoption of the United Nations Convention on the Law of the Sea (UNCLOS).

At its Seventy-fifth anniversary summit in September 2020, the UNGA will be faced with a similar choice. Taking into account the progress made in crystallizing international cooperation to secure cyberspace, counter cybercrime, maximize the use of cyber technologies for accelerating the objectives of sustainable development, and put people at the center of cyberspace, the UNGA must respond by convening a Conference on Cyberspace to negotiate and adopt an international multi-stakeholder framework for this unique domain.