The 21st Century Cold War in "Cyberia"

Rajesh Pant

"Gutenberg's achievement created a new and wonderful earth, but at the same time also a new hell."

—Mark Twain

What Mark Twain said about the invention of the Printing Press by Gutenberg in the 19th century, may well apply today to the evolution of the Internet. In order to combat this, in 1998, the Russian Federation had first introduced a resolution in the United Nations (UN) First Committee on the threats posed by information and communication technologies (ICT) to international peace and security. Since then the UN has set up six Group of Governmental Experts (GGE) to study the nature of threats in cyberspace-mainly implications of ICT on national security and military affairs, and how to deal with them.[1] Subsequently, in December 2018, the UN General Assembly approved the establishment of two distinct groups, in order to further explore issues related to advancing 'responsible' state behaviour in cyberspace, namely: an Open-Ended Working Group (OEWG) and a new 6th UNGGE.

The virtual meeting of the 6th UNGGE on ICT security has somewhat widened the already existing fault lines in resolving the issue of acceptable

Lieutenant General (Dr.) **Rajesh Pant** (Retd) is the National Cyber Security Coordinator of India.

norms for good internet behaviour by nations across the world. This UNGGE was convened for a period of two years and it comprises 25 countries,[2] including India. The previous 5th UNGGE had failed to achieve a consensus and had ended in a deadlock. In fact, all that the previous meetings have been able to achieve is a list of eleven non-binding norms. These norms, though desirable, were always considered too idealistic, such as the norm that nation states will cooperate to exchange information, prosecute terrorists, and address threats. And that in case of ICT incidents, states should consider all information for attribution, or that states will intentionally not damage critical infrastructure. It is only wishful thinking that all nations would adopt these norms. However, the harsh reality is different. For one has to only witness the annual reports, as issued by the global internet security companies to realise the blatant disregard for these norms in the interconnected cyber world, called herein, as 'Cyberia'.

Why is this happening? Well, one of the main reasons is the lack of a coordinated international investigation and prosecution mechanism against the cyber criminals. While the UN Charter and law on use of force (*Jus Ad Bellum*) applies to activities conducted in cyber space, the International Humanitarian Law (*Jus In Bello*) applies to the conduct of cyber activities occurring within an international armed conflict. Since the attacks in Cyberia are taking place during 'peace' conditions, there is an ongoing debate on the applicability of the International Humanitarian Law. Furthermore, the Eastern and the Western lobbies are already at loggerheads over the perceived skewed governance of the internet as most of the 'root' servers, which control the last part of the Internet Protocol address, are located in the United States (US).

In such a turbulent atmosphere, the only happy entity is the cyber-criminal for he has no fear of attribution and any legal prosecution since the path of cybercrime spans across several national boundaries. To make matters easier for him, there is the 'Dark and Deep Web'—a vast network

of anonymised users and untraceable communication nodes. This is the dirty underbelly hosting dream markets that sell drugs, credit cards, firearms, pornography and state secrets to name a few. Payment is usually in cryptocurrencies supported again by untraceable blockchain technology. Besides, the international legal processes like the Mutual Legal Assistance Treaty and Letter of Rogatory are woefully time consuming and just not able to deliver justice.

In addition to the activities at the UN, there is also a rising tide for the 'Balkanisation of the Internet'. In order to overcome the American dominance of the internet root servers, the Chinese have now proposed a new internet protocol to the International Telecommunication Union (ITU). This appears to be a part of their strategy to create a new internet based on a new set of standards—to ensure that technical control is dominantly exercised by the Chinese in the future. This will lead to the establishment of two internets and it is likely that its usage by nations will be dictated by geopolitical affiliations. This will further exacerbate the original aim of creating a globally safe and secure interconnected network and will adversely affect social media as well as global business functions.

Cyberspace is heavily infected with a variety of computer viruses and bots and the recent spate in ransomware attacks and financial frauds, are an indicator of the increasing incidents of cybercrime. These fraudsters and criminal gangs have no morals and they exploit any and every opportunity to make money. In the ongoing COVID-19 crisis too there are reports of over 4,000 websites that have sprung up under the pretext of the coronavirus to carry out phishing attacks—leading to an exponential increase in cybercrime. In such a scenario, India ranks amongst the top three cyber-attacked nations in the world and lost 1.25 lakh crores of rupees to cybercrime in 2019.

There are many viruses already rampant in Cyberia, and what is required is a coordinated response by the international community such as that we are currently witnessing in the physical world against

the COVID-19 pandemic. Indian Prime Minister Narendra Modi too highlighted this issue in his address at the 75th UN General Assembly. India, with its non-aligned past and current strategic partnerships, has a great opportunity to lead the way in ensuring that the internet does not split. To which, India has already initiated certain measures in this direction in both regional and international forums. *Let us all resolve to strive towards a peaceful Cyberia!*

Notes

1. In 2004, the UN General Assembly established the GGE. Since then six GGEs have been convened – in 2004/2005 (A/RES/58/32), 2009/2010 (A/RES/60/45), 2012/2013 (A/RES/66/24), 2014/2015 (A/RES/68/243), 2016/2017 (A/RES/70/237), and 2019/2021 (A/RES/73/266). For details see, United Nations, "Group of Governmental Experts." Available online at https://www.un.org/disarmament/group-of-governmental-experts/, accessed on September 30, 2020.
2. UNGGE Members (2019-2021) include: Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States and Uruguay.