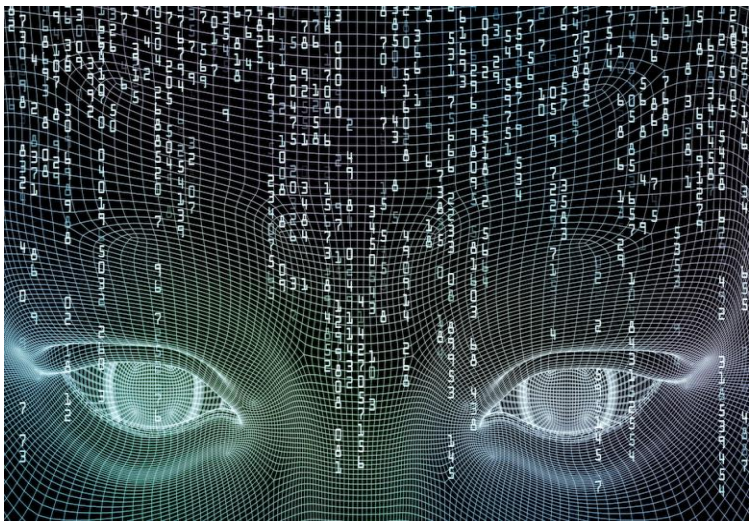
A quest for order amid cyber insecurity



Context:

- The digital revolution has sped up the emergence of a global digital space.
- This digital space, the "**cyberspace**", is the communication space made of network infrastructure (such as servers and cables), devices (like computers and smartphones), software (both human-machine and machine-to-machine interfaces) and data carried over the network.

What is the significance of cyberspace?

- Cyberspace has been growing at an exponential rate. The world is adopting new ways of digital interaction and more of our critical infrastructure is going digital.
- Cyberspace provides major **opportunities for innovation, economic progress, cultural development and access to information**. Its **increasing accessibility and affordability** have proved hugely useful for many human activities.
- The **cyberspace market has grown exponentially**. Apple, Amazon and Microsoft together have added more than a trillion dollars in market value, since the start of 2020.

What are the challenges?

Cyber insecurity:

- **Cyberattacks have grown in sophistication, intensity and frequency**. Cyberinsecurity of individuals, organisations and states has been expanding even amidst the COVID-19 crisis.

- New and dangerous practices are developing in cyberspace: **cybercrime, information manipulation, political or economic espionage, attacks on critical infrastructure or individuals,** theft of personal information or confidential data, compromise of information and communications systems used by citizens, companies and agencies.

Non-state actors:

- There has been a substantial increase in cyberattacks during the pandemic crisis. In just one week of April 2020, there were over 18 million daily **malware and phishing emails** related to COVID-19 monitored by a single email provider. Also, more than 240 million COVID-19-related daily spam messages were reported.
- The cyberattack on the Twitter platform targeting high profile twitter accounts was able to dupe people of around $120,000.
- The **ransomware attack** on California University leading COVID-19 research had resulted in the university paying around $1 million.

State actors:

- Australia has blamed state-backed cyber attacks on its cyber infrastructure.
- **China has been accused of hacking healthcare institutions in the United States working on the novel coronavirus treatment.**
- The United Kingdom has warned of hackers backed by the Russian state targeting pharmaceutical companies conducting COVID-19 vaccine research.
- **India recently banned 59 Chinese Apps, on grounds of protecting security, sovereignty and privacy.**

What is the need for global collaboration?

- Since the cyberattacks respect no borders, it is thus essential to bring the international community together to ensure peace and security in the digital space. In such a scenario, **shared rules and norms become imperative**.
- *Current cyberspace architecture:* The article argues that, against popular perception, cyberspace is not borderless and the connectivity across national boundaries hasn't been nurtured and hence, it cannot be equated to a global commons.

- The Internet which depends on physical infrastructure under national control remains subject to border controls with each state applying its own laws to national networks, consistent with its international commitments.
- Also, **cyberspace has multiple other stakeholders with the non-state actors playing key roles.** There are also many private networks.
- Nevertheless, states alone have the right of oversight. **States remain responsible for cybersecurity, enforcement of laws and protection of public good**.

What are previous International efforts?

- In 1998, Russia for the first time raised the issue of information and communications technologies (ICTs) in international security at the UN.
- **Six Group of Governmental Experts (GGE)** with two-year terms and limited membership have functioned at the United Nations with the aim of **drafting norms for responsible state behaviour in cyberspace**. India has had representatives on five of the six GGEs.
- An **Open-Ended Working Group (OEWG)** with a broader membership has been working on the issue of ICT since 2019. India has actively participated in the OEWG.
- UN Secretary-General António Guterres's recent report, **"Roadmap for Digital Cooperation",** also calls for action on the issue of cyberspace.
- Many regional organizations, like the Shanghai Cooperation Organisation, have voiced support for a cyber code of conduct.
- **The Christchurch Call** brings together countries and companies in an effort to stop the use of social media for promoting terrorism and violent extremism. India has been part of these efforts.

What are limitations?

- Like all other technologies, the growth of cyberspace technology has been way ahead of the development of associated norms and institutions.
- **There has been slow progress in the GGEs and the OEWG.** And the discussions have been **narrowly focused.** Issues such as Internet governance, development, espionage, and digital privacy have been kept out. While

terrorism and crime are acknowledged as important, discussion on these has not been focused on.

- The net result of the UN exercise has been an acceptance that international law and the UN Charter are applicable in cyberspace and subsequently a set of voluntary norms of responsible state behaviour was agreed to in 2015. However, there continues some uncertainty as to what aspects of international law and in what circumstances will it be applicable.
- There seems to be very little hope that the current processes would lead to any substantial cyberspace architecture in the current geopolitical circumstances.

Way forward:

- **For the world:** There is a need for **rules and norms that provide clarity on acceptable behaviour and deter subversive behaviour from nefarious actors.**
- The next phase of global collaboration in an increasingly contested and fragmenting cyberspace domain requires better arrangements and more intense partnerships with more safeguards.
- **India specific:** Given the fact that the next billion new smartphone users will include a significant number from India, India has high stakes in this issue.

Balancing the competing needs:

- India needs to evolve an approach, in tune with its economic, social and political objectives. The approach will have to balance the competing demands of national sovereignty and transnational connectivity and the twin needs of **national security and economic growth**.
- India's disinclination to support unfettered data flows across borders is propelled by the 'data sovereignty principle'. However, the emphasis to nationalise data could pose problems for entrepreneurs and start-ups who prefer relaxed data-sharing rules to foster innovation and product development.

Shaping cybernorms and rules:

- Globally, India's passivity in influencing global tech rules must end and India needs to play a key role in shaping cybernorms and rules.

- Engagement in multi-stakeholder orientations such as the **Paris Call (for trust and security in cyberspace)** could be helpful.
- India could consider acceding to the **Budapest Convention, or Convention on Cybercrime of the Council of Europe.**
- The sheer volume of data generated by citizens at home makes India an essential destination for foreign technology firms enabling India to exercise its authority in shaping global trade rules. This allows India to shape, influence and constrain global technology rules that serve its strategic interests. It can and must significantly shape the making of the digital world.
- *Domestic data protection regime:* Domestically, there is a need for the adoption of a **robust data protection regime**.
- *Involving the stakeholders:* There is the need to **encourage the private sector** to get involved more in industry-focused processes in the domain of cyberspace such as the Microsoft-initiated Cybersecurity Tech Accord and the Siemens-led Charter of Trust.
- There is also the need for a **deeper public understanding of the various dimensions of cyberspace.** Addressing the current digital divide will help in this direction.