

Deepening cooperation can develop avenues for mutual learning and create complementary markets in cyber tools and technologies, boosting bilateral business and strategic commitments on both continents.

Western and media attention may be focused on the conflict between Russia and Ukraine, but countries have not taken their eye off the Indo-Pacific where there is clear evidence of the changing world order. This is manifest in the signing of the India-Australia Economic Cooperation and Trade Agreement in goods and services earlier this month.

The botched US withdrawal from Afghanistan followed by China taking a serious interest in creating new economic, military and political alliances, and the impending energy crisis demand that nations recalibrate their strategic as well as long-term interests. The India-Australia ECTA is a concrete example of the bilateral faith in common values, and understanding of threats and goals. A reflection of this is cooperation in cyber security.

The Russia-Ukraine conflict has shown how cyber threat actors, both state and non-state, have become significant players in hybrid or “unrestricted” warfare. Both countries have let loose malicious elements in the information as well as operational space, while non-state actors like the hacktivist group Anonymous claimed to have caused significant damage to critical Russian and Belarusian financial and military infrastructure.

China is accused of having amassed a large number of cyber weapons and has allegedly carried out sophisticated operations aimed at espionage, theft of intellectual property, and destructive attacks on internet resources of some countries. Australia and India have been at the receiving end of several such campaigns by the so-called Advanced Persistent Threat (APT) groups, supported by or assumed to be located in China.

At the June 2020 virtual bilateral summit, Prime Minister Narendra Modi and his Australian counterpart Scott Morrison elevated the bilateral relationship to a Comprehensive Strategic Partnership. The new cyber framework includes a five-year plan to work together on the digital economy, cybersecurity and critical and emerging technologies. This will be supported by a \$9.7 million fund for bilateral research to improve regional cyber resilience.

An annual Cyber Policy Dialogue, a new Joint Working Group on Cyber Security Cooperation and a joint working group on ICTs have been established. An annual India-Australia Foreign Ministers Cyber Framework Dialogue will be held. India will now be included in a core Australian initiative called the International Cyber Engagement Strategy — it began in 2017 to actively conduct capacity-building arrangements in Indonesia, Singapore and Thailand, and support similar activities in Malaysia, Vietnam and Cambodia. In 2021 Australia added critical technologies to the initiative, making it important to the bilateral partnership with India and to the Quad.

India has much to learn from Australia's low-key but smart cyber expertise. The Australian Cyber Security Centre (ACSC) in Canberra is the receptacle of the country's cybersecurity information, advice and assistance efforts. It draws expertise from national law enforcement, intelligence agencies, crime investigation, and national security bodies. ACSC has a partnership programme with the corporate world to facilitate intelligence-sharing on threats. AustCyber, another government effort, aims at establishing an internationally competitive domestic cybersecurity industry.

India has set up the office of the National Cybersecurity Coordinator, a national Computer Emergency Response Team (CERT-IN), a national Critical Information Infrastructure Protection Agency (NCIIPC), and made appropriate amendments to the Information Technology Act and Rules to enhance its cyber security posture. This has upped India's rank to 10th in the Global Cyber Security Index (GCI) 2020, from 47th just two years earlier. India has capable cybersecurity professionals.

In February, the foreign ministers of India and Australia recognised cooperation in cyber governance, cyber security, capacity building, innovation, digital economy, cyber and critical technologies as an essential pillar of the relations between the two countries. A joint Centre of Excellence for Critical and Emerging Technology Policy, to be located in Bengaluru, will be set up.

India and Australia share common concerns around 5G rollouts, threats by APT groups, cybercrime, information warfare and threats to a democratic order. Deepening cooperation can develop avenues for mutual learning and create complementary markets in cyber tools and technologies, boosting bilateral business and strategic commitments on both continents.

Committed To Excellence

GS World Team Input

IN THE NEWS

What is Cyber Security?

- Cyber security refers to a type of Internet security that protects you from malware, black hat hackers or any other kind of cyber-attacks.
- If you use the Internet for banking related activities, then you must install antivirus on your device keeping in mind the cyber security.

What is Cyber Crime?

- Cyber-crime is also called cyber-crime or computer crime. Cybercrime is a type of illegal activity, which is carried out with the help of internet or digital means. In general terms, any crime committed through digital or internet means is called cyber-crime.

Different forms of cyber crime

- Cybercrime refers to criminal activity involving the Internet, computers or any other inter-connected infrastructure. It covers crimes like a credit card fraud, illegal downloading, industrial espionage, child pornography scam, cyber terrorism, creation of viruses, distribution of spam and so on.

National Cyber Security Strategy 2020

- The National Cyber Security Strategy 2020 was drafted with an aim to improve cyber awareness and cyber security through rigorous audits. Under this policy, the empaneled cyber auditors will carefully monitor the security features of the organisations.

WORLD

Committed To Excellence

Expected Question (Prelims Exams)

Q. Consider the following statements:-

1. India was ranked 10th in the Global Cyber Security Index (GCI) 2020.
2. The Global Cyber Security Index (GCI) is released by the International Telecommunication Union (ITU).

Which of the above statement (s) is/are not correct?

- (a) 1 only
- (b) 2 only
- (c) Both 1 and 2
- (d) Neither 1 nor 2

Expected Question (Mains Exams)

Q. What is Cyber Threat? While mentioning different types of cyber-crimes, analyze the various steps taken by the government to prevent cyber-crimes. (250 Words)

World

Committed To Excellence

Note: - The question of the main examination given for practice is designed keeping in mind the upcoming UPSC main examination. Therefore, to get an answer to this question, you can take the help of this source as well as other sources related to this topic.