PLUTUS IAS
CURRENT AFFAIRS
Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

Date –21-April 2025

VICE PRESIDENT'S OFFICIAL VISIT TO INDIA: STRENGTHENING BILATERAL TIES

WHY IN THE NEWS?

U.S. Vice President J.D. Vance arrived in New Delhi on April 21, 2025, for an official visit, accompanied by his wife, Usha Chilukuri, their three children, and a high-level delegation of U.S. officials, including Ricky Gill, Senior Director for South and Central Asia at the U.S. National Security Council. Upon arrival, Mr. Vance was accorded an official guard of honour. He is scheduled to meet Prime Minister Narendra Modi and members of the Union Cabinet at a dinner hosted at the Prime Minister's residence. The visit is expected to witness the formal launch of the TRUST (Transforming Relationship Utilising Strategic Technology) partnership, which is a rebranded version of the previous Initiative on Critical and Emerging Technologies (iCET) initiated under the Biden administration. The visit has also drawn political attention, with the Congress questioning whether the Prime Minister will raise concerns about the treatment of Indian citizens abroad, and the farmer organisation AIKS announcing plans to protest the Vice President's presence. The visit is seen as a significant step in strengthening U.S.-India strategic and technological cooperation.

INDIA AND THE US: BILATERAL AREAS OF COOPERATION

1. Trade and Economic Relations: In 2024, bilateral goods trade reached $129.2 billion, with U.S. exports to India at $41.8 billion and imports at $87.4 billion. Both nations aim to increase this trade volume to $500 billion by 2030, under the "Mission 500" initiative.

2. Defence and Security: The U.S. and India have deepened their Major Defence Partnership, focusing on areas like space, artificial intelligence, and defence industrial collaboration.

3. Critical and Emerging Technologies (iCET): Launched in 2022, the iCET initiative enhances collaboration in fields such as semiconductors, AI, and quantum computing. Notably, the U.S. and India are jointly establishing a semiconductor fabrication plant in India, aimed at bolstering national security and technological capabilities.

4. Energy Cooperation: India is considering eliminating import taxes on U.S. ethane and liquefied petroleum gas (LPG) to strengthen energy ties and reduce its trade surplus.

5. Cybersecurity and Digital Infrastructure: Both countries are collaborating on enhancing cybersecurity measures, including threat information sharing and securing telecommunications networks.

6. Space Collaboration: India and the U.S. have reaffirmed their commitment to joint space exploration and research, building upon existing partnerships between their respective space agencies.

7. Health Sector: The two nations continue to collaborate on health initiatives, focusing on areas like disease surveillance, epidemiology, and research on various health conditions.

8. People-to-People Ties: The Indian American community, numbering over 3.5 million, plays a pivotal role in strengthening bilateral relations. Efforts like India's participation in the U.S. Global Entry Program facilitate easier travel and enhance cultural exchanges.

RECENT DEVELOPMENTS IN THE US POLICIES AND ITS IMPACT ON THE INDO-US RELATIONSHIP

1. Revival of Trade Talks: India and the U.S. have resumed comprehensive trade negotiations, targeting $500 billion in bilateral trade by 2030. India may cut tariffs on over $23 billion worth of U.S. goods, while the U.S. has paused tariff hikes for 90 days.

2. High-Level Diplomatic Visits: U.S. Vice President JD Vance's visit to India (April 2025) signals renewed political engagement. Meetings with PM Modi focus on resolving trade frictions and boosting bilateral cooperation.

3. Defence Partnership Upgrade: Both nations are set to sign a 10-year defence framework under the COMPACT initiative, covering military cooperation, technology, and joint exercises.

4. Strategic Tech & Nuclear Energy Cooperation: Under the TRUST initiative, both sides are working on AI infrastructure, semiconductor collaboration, and plans to build U.S.-designed nuclear reactors in India.

5. Space Collaboration Milestones: A NASA-ISRO partnership aims to send the first Indian astronaut to the ISS via AXIOM. The joint NISAR mission will be launched to track Earth changes using advanced radar.

6. Energy Trade Boost: India may remove duties on U.S. ethane and LPG, aligning with efforts to diversify energy imports and reduce its trade surplus with the U.S.

7. Digital Economy & IPR Concerns: The U.S. shift towards economic nationalism under Trump raises concerns over global IP regimes like TRIPS, with implications for tech transfer and pharmaceutical collaboration.

8. People-to-People & Diaspora Role: The 3.5 million-strong Indian-American community remains a bridge for stronger ties. VP Vance's cultural engagements in India highlight the soft power dimension of the relationship.

INDIA'S COURSE OF ACTION TO TACKLE CHANGES IN THE INDIA-US RELATIONSHIP

1. Strengthening Defence and Strategic Ties: India will deepen defence cooperation with the U.S., focusing on joint exercises, technology sharing, and a strategic defence partnership under the COMPACT initiative.

2. Expanding Trade Partnerships: India will address trade frictions through negotiations and seek diversification by strengthening ties with other global partners to offset potential disruptions.

3. Advancing Energy and Renewable Cooperation: India will continue collaborating with the U.S. on clean energy and nuclear technologies, aligning its policies with U.S. standards for investment in renewable energy and natural gas.

4. Driving Innovation and Tech Collaboration: India will boost its digital economy by working with the U.S. on AI, data privacy, and space technologies, and attract U.S. investments in emerging sectors like biotech and electric vehicles.

5. Enhancing Regional Engagement: India will intensify its role in the Indo-Pacific alongside the U.S. and deepen cooperation in the Quad to counter China's influence and promote regional security.

6. Leveraging People-to-People Ties: India will harness the Indian-American diaspora and expand educational and cultural exchanges to strengthen bilateral ties.

7. Collaborating on Climate Change: India will continue climate cooperation with the U.S. on clean energy, carbon reduction, and technology sharing, in line with the Paris Agreement.

8. Balancing Geopolitical Relations: India will carefully navigate its relations with both the U.S. and China, ensuring its global diplomatic and economic interests remain aligned while managing regional challenges.

CONCLUSION

The India-U.S. relationship is undergoing a dynamic phase of expansion, with strengthened cooperation in defence, trade, technology, energy, and regional security. Recent policy shifts in the U.S., especially with the launch of the TRUST initiative, signal a renewed commitment to deepening ties in strategic sectors. India's proactive response includes enhancing defence collaboration, addressing trade frictions, advancing energy cooperation, and focusing on technological innovation. The growing Indian-American diaspora continues to play a crucial role in bridging cultural and economic gaps, reinforcing the people-to-people connections. As both nations move forward, India's balancing act between its relationship with the U.S. and its regional challenges, particularly with China, will define the future trajectory of their partnership. With both nations committed to fostering strategic, economic, and technological ties, the India-U.S. relationship is poised for long-term success, contributing significantly to global stability and growth.

PRELIMS QUESTIONS

Q. With reference to the Malabar Naval Exercise, which of the following statements is/are correct?

1. It began as a bilateral exercise between India and the United States in 1992.

2. Japan and Australia have been permanent members of the exercise since its inception.

Select the correct answer using the code given below:

A. 1 only

B. 2 only

C. Both 1 and 2

D. Neither 1 nor 2

Answer: A

MAINS QUESTIONS

Q. Discuss the significance of the TRUST initiative in strengthening the strategic relationship between India and the U.S., with a focus on technology and defence cooperation.

(250 words, 15 marks)

INDIAN CYBER CRIME COORDINATION CENTRE (I4C): SAFEGUARDING INDIA'S CYBERSPACE

WHY IN THE NEWS?

The Indian Cyber Crime Coordination Centre (I4C) was in the news recently for celebrating its first Foundation Day on 10th September 2024 at Vigyan Bhavan, New Delhi. Union Home Minister Amit Shah launched four major initiatives to strengthen India's fight against cybercrime. These include the Cyber Fraud Mitigation Centre (CFMC), the Samanvay Platform for joint investigations, the Cyber Commandos program to train 5,000 digital specialists, and a National Suspect Registry. He emphasized that cybersecurity is now a core aspect of national security and requires coordinated action by all stakeholders. The new criminal laws also contain stronger provisions for tackling cybercrime. A new logo, vision, and mission for I4C were also unveiled. These efforts mark a significant step in India's pursuit of a safer digital ecosystem.

PLUTUS IAS
UPSC/ PCS
Indian Cyber Crime Coordination Centre
सहवीर्य करवावहै • Working Together With Vigour

WHAT IS I4C

The Indian Cyber Crime Coordination Centre (I4C) was conceptualized and launched by the Ministry of Home Affairs (MHA) in January 2020. The core objective is to create an effective mechanism for detecting, preventing, investigating, and prosecuting cybercrimes in a coordinated manner across the country. With the rapid increase in cybercrime incidents and the growing complexity of digital threats, a centralized system became essential. I4C is headquartered in New Delhi and works on a seven-pronged framework to ensure a robust, proactive, and multi-stakeholder approach. These pillars are:

1. **Threat Analytics Unit (TAU)** – For detecting new cyber threats.
2. **Joint Cybercrime Investigation Platform** – To enable collaborative investigations.
3. **Cyber Forensic Lab Ecosystem** – For digital evidence collection and analysis.
4. **Cybercrime Ecosystem Management** – Connecting stakeholders from law, tech, and finance.
5. **Cybercrime Reporting Portal** – User-friendly interface for victims.
6. **Capacity Building Unit** – For training police and judiciary.
7. **R&D in Cybercrime Technologies** – To stay ahead in the cyber arms race.

The Centre also encourages innovation in detecting digital frauds and promotes the development of indigenous tools and forensic technologies.

FUNCTIONS OF I4C

I4C performs a wide variety of critical functions aimed at strengthening India's cybercrime management capabilities.

1. Central Coordination: It acts as the nodal point for communication and coordination between central agencies, state police, and international law enforcement bodies. This ensures that cross-border and multi-jurisdictional cybercrime cases are dealt with effectively.

2. Reporting Infrastructure: Through the National Cybercrime Reporting Portal (cybercrime.gov.in), it provides a one-stop platform where individuals can report online financial frauds, cyberbullying, child pornography, and other offences. The portal categorizes cases and routes them to respective state units.

3. Data Analytics and Threat Mapping: I4C uses advanced analytics and AI-driven tools to analyze complaint data, identify hotspots, and detect emerging cybercrime patterns. This enables faster preventive actions.

4. Capacity Building: I4C has trained over 35,000 officers so far through classroom and e-learning modes. It develops modular training programs based on the latest cybercrime trends, tools, and tactics.

5. Technological Support: It supports state police with digital forensic kits, investigation tools, and real-time intelligence. It also runs workshops and simulation exercises to test preparedness.

6. Public Awareness and Outreach: It coordinates awareness campaigns like "Cyber Jaagrookta Diwas," broadcasts public messages, and distributes educational content to schools and colleges.

POWERS OF I4C

Though I4C does not possess direct investigative or law enforcement powers like a police agency, its influence and authority in shaping India's cyber security framework are substantial.

1. Strategic Authority: I4C acts as the strategic apex body for cybercrime management in India. It develops national-level guidelines and helps in the formulation of cybercrime policies and protocols.

2. Technical Expertise: It provides technical support to law enforcement by offering tools for digital forensics, real-time surveillance, and data analysis. The Centre helps bridge the tech gap for states lacking cyber capabilities.

3. Policy Advisory Role: I4C advises the government on amending existing laws and formulating new rules to tackle modern threats like ransomware, AI misuse, and dark web activities.

4. Inter-Agency Linkage: It liaises with CERT-In, RBI, telecom companies, and foreign cyber agencies to exchange information. It plays a critical role in coordinating responses during widespread cyberattacks or data breaches.

5. Cyber Forensic Infrastructure: I4C has helped set up specialized labs in Hyderabad, Pune, and other cities where digital evidence is collected, preserved, and analyzed using cutting-edge tools.

FINANCIAL FRAUDS IN RECENT TIMES

Digital financial fraud has emerged as one of the most common and damaging forms of cybercrime in India. From UPI frauds to crypto scams, the landscape of financial cybercrime has rapidly evolved.

Year	Reported Cases	Amount Involved (INR Crore)	Top Methods
2021	51,000	560	Phishing, Fake KYC, Loan scams
2022	84,000	980	UPI frauds, Ponzi schemes, investment scams
2023	1,25,000	1,500	Vishing, job frauds, romance scams
2024	1,95,000	2,200	Remote Access scams, crypto frauds
2025 (Till Apr)	62,000	680	OTP scams, AI-generated voice impersonation

These figures reflect only reported cases; many go unreported due to lack of awareness or stigma. The shift toward AI-generated voice and video frauds is a worrying trend, where even well-informed users are deceived.

FINANCIAL FRAUD AS A CYBER CRIME

Financial fraud is among the most damaging forms of cybercrime because it directly impacts the livelihood of individuals and businesses. With digital payments becoming the norm, vulnerabilities have also increased.

1. Fraudsters commonly impersonate bank officials or tech support agents to trick people into sharing OTPs or clicking malicious links. The rise of social engineering has made cybercrime more psychological than technical.
2. E-commerce platforms are often misused to commit fake sales, bogus refunds, and payment diversions. Fraudsters also use social media ads to lure users into investing in fake schemes.
3. Fraud through QR codes, fake payment apps, and phishing links continues to rise. Criminals also exploit crypto platforms and create fake trading apps that appear genuine but are designed to siphon funds.
4. Law enforcement often faces challenges in tracing these frauds due to international routing of transactions, use of VPNs, and fake identities.

WHY MORE PREVALENCE IN INDIA?

Cyber financial frauds have found fertile ground in India due to several structural, social, and technological reasons:

1. Massive Digital Adoption: India is the world's fastest-growing digital economy, but with over 900 million internet users, digital hygiene is still poor. Many users are unaware of basic safety practices like not sharing OTPs or using two-factor authentication.

2. Lack of Digital Literacy: Especially in rural and semi-urban areas, people are prone to falling for job scams, lottery frauds, and phishing emails. Cyber education has not kept pace with digital penetration.

3. Smartphone Dependency: Financial services are now app-based, and mobile devices are more vulnerable than desktops. A single mistake—such as downloading a fake app—can compromise entire accounts.

4. Low Reporting and Prosecution: Victims often feel embarrassed and don't report incidents. Even when they do, police stations may lack the tech expertise to investigate, leading to poor conviction rates.

5. Language-Localized Scams: Fraudsters now operate in regional languages, making it easier to gain trust and deceive users. Scammers also impersonate known individuals using AI-generated voices.

6. Cheap Access to Technology for Criminals: With inexpensive smartphones, SIM cards, and easily available VPN services, even small-time criminals can execute sophisticated scams. The cost of entry into cybercrime is low, but the returns are often high.

7. Organized Cybercrime Networks: Many frauds are not isolated events but part of large-scale, well-organized scam call centers. These networks operate with trained agents, scripts, and fake digital identities, often across multiple states or countries.

8. Inadequate Cybersecurity Infrastructure: Many small businesses and institutions don't invest in robust cybersecurity measures. Their weak systems are easy targets for ransomware, phishing, and financial frauds.

GOVERNMENT INITIATIVES TO CONTAIN CYBER CRIMES

The Indian government has adopted a multi-layered strategy to address the rising tide of cybercrimes, especially financial frauds.

1. I4C Initiative: Centralizes cybercrime detection and response efforts across India, ensuring consistency and expertise in handling cases. It has already led to thousands of fraudsters being identified and tracked.

2. Cybercrime Reporting Portal: Offers victims a simple, quick way to report crimes, with multilingual support and categorized complaint types. It helps create a national database of cyber fraud patterns.

3. Capacity Building Programs: The government regularly organizes workshops, certifications, and simulations for police officers, prosecutors, and judges to improve their cybercrime handling skills.

4. Public Campaigns: Initiatives like "Stay Safe Online," "Cyber Swachhta Kendra," and "Digital Suraksha" aim to educate the public through media, infographics, and influencer campaigns.

5. Partnership with Private Sector: Collaborates with banks, payment companies, telecom providers, and social media firms to share threat intelligence and shut down fraudulent channels quickly.

6. Legislation: New rules under the IT Act, as well as the Digital Personal Data Protection Act, 2023, aim to strengthen privacy and accountability mechanisms.

WAY FORWARD / RECOMMENDATIONS

The future of India's fight against cybercrime hinges on sustained effort, cross-sector collaboration, and innovation.

1. Revise and Strengthen Laws: Cyber laws must be revised regularly to tackle new-age threats like deepfakes, AI-powered scams, and blockchain-based fraud.

2. Localized Cyber Literacy Campaigns: Governments and NGOs should work together to spread cybersecurity knowledge in local languages through schools, panchayats, and mobile vans.

3. Specialized Cybercrime Units: Every district police headquarters should have a well-equipped cyber cell with trained staff and access to forensic labs.

4. Faster Judicial Redress: Creation of dedicated cybercrime courts to reduce case backlogs and improve conviction rates. Victims deserve timely justice.

5. International Partnerships: Strengthen global cybercrime treaties and data-sharing agreements, especially with countries where scam centers operate.

6. Mandatory Cybersecurity Protocols: Organizations handling sensitive data should follow minimum standards and be penalized for negligence.

7. Cyber Insurance Ecosystem: Promote policies that help victims recover from financial losses and encourage more proactive protection measures.

CONCLUSION

The Indian Cyber Crime Coordination Centre (I4C) stands at the heart of India's cybersecurity strategy, helping to create a safe and secure digital environment. In the digital age, where every citizen is a potential target, I4C plays the dual role of protector and enabler. While the challenges are complex and ever-evolving, India's commitment to fighting cybercrime through innovation, legislation, and public participation remains strong. A safer digital India is not just the responsibility of the government, but a collective mission involving citizens, companies, and institutions.

PRELIMS QUESTIONS

Q. The Samanvay Platform is aimed at:

A. Promoting cyber education in schools

B. Facilitating joint cybercrime investigations

C. Regulating fintech applications

D. Tracking cryptocurrency usage

ANSWER: B

MAINS QUESTIONS

Q. Discuss the rising trend of financial frauds as a form of cybercrime in India. What are the key challenges in tackling these crimes, and how can the government address them?

(250 words, 15marks)