1. What are the threats to the financial sector emanating from the cyber space? Examine.

Introduction

The Indian government has embarked on a programme to turn the country into a digital economy. It has unveiled a series of initiatives—from introducing Aadhaar, MyGov, Government e-Market, DigiLocker, Bharat Net, Startup India, Skill India and Smart Cities to propel India towards technological competence and transformation.
The move towards a digital economy is likely to help trigger a fresh wave of economic growth, attract more investment, and create new jobs, across multiple sectors. However, it also poses a big challenge, that of Cyber Security.

Body

Threats to the financial sector emanating from the cyber space

- Amount of data held by financial services companies makes them prime targets for "cyberthreat actor
- According to NITI Aayog report
  - 24 % of cyber breaches affected financial organizations.
  - 73% of all of breaches were financially motivated
  - Denial of Services, Web Application Attacks and Payment Card skimming represent 88 % of all security incidents within financial services.
- Ransomware attacks (Ransomware is a type of software that threatens to publish a person's data or block it unless a ransom is paid) increasingly affected businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails.
- Huge consolidation has happened in the banking industry in the last several years. Bank are also willing to pay up when held hostage by a ransomware attack

Conclusion

Institutions such as the National Cybersecurity Coordinator (NCC), National Technical Research Organisation, Computer Emergency Response Team and the National Cyber Security Coordinator Centre are all doing a reasonable job.

2. We live an era of data driven governance. What are the threats to the data ecosystem? What would be the implications of a big data breach? Examine.

Introduction

Data-driven governance is a new approach to governance, one where data is used to drive policy decisions, set goals, measure performance, and increase government transparency.

Body

Data ecosystem includes infrastructure, analytics, and applications used to capture and analyze data. Increase in use of data in governance has also brought certain threats and challenges to data ecosystem:-

- **Hardware –** by impregnating ICs and chip-sets for spying.
- **Software –** virus, malware, Trojan software and worm attacks being a regular issue. eg – WannaCry, Petya.
- **Apps –** like Tiktok, Snapchat, Tumblr have been used for data mining.
- **Network –** Attacks on networks can slowdown entire system. In October 2019, India announced that North Korean malware designed for data extraction had been identified in the networks of a nuclear power plant.
- **Websites –** Following an attack on Indian military forces in Kashmir, Pakistani hackers targeted almost 100 Indian government websites and critical systems.
- **Storage –** Data breach of sensitive information is most feared at present times.

These threats sometimes take more ugly form such as big data breach. Under such conditions there is release of secure or private/confidential information to an untrusted environment. This would have several implications:-

- **Data Privacy –** The meta-data would affect the privacy of individual. This was one of the fear expressed in Justice K. S. Puttaswamy (Aadhar case**)**
- **Demographic data –** breach of demographic data which can be mined by foreign companies/governments so as to use it for their narrow vested interest
- **Economic implication –** In the past six years, the global average cost of a data breach has grown by 12%, totaling $3.92 million per breach in 2019.
- **Political Manipulation –** Data collected by foreign governments (Ex: Russia, China) can be misused to influence political narrative and elections. Ex: 2016 US Presidential elections
- **Diminish Trust –** A data breach can put citizens and customer trust at risk.
- **Legal implication –** Data breaches may also impose legal liabilities and penalties upon the affected organisation along with the loss of intellectual property.

Conclusion

Need of the hour is strict data protection framework. This could be done by compiling to Justice BN Srikrishna Committee's recommendations, and E.U's General Data Protection Regulation.

3. How is black economy an internal security threat? Analyse. What are the measures in place to tackle black economy? Discuss.

Introduction

Black economy is based on the unaccounted money of the people and is also known as the 'Parallel economy'. It is a great menace to the Indian economy. Black money is nothing but money generated in transactions which are hidden from Government in order to avoid tax. This is usually done in cash because cash transactions do not reveal the identity of the person carrying out the transaction. It's elimination will help the society in more than one way..

Body

Black economy an internal security threat
Black economy is the main source of resources for all the major internal security issues of India.

- **Economic terrorism**

  The country has to contend with Economic terrorism. Pakistan has been flooding the country with counterfeit currency with a view to subverting its economy and funding terrorist activities in different parts of the country.

  It is estimated that Pakistan pumped in 16 billion worth of FICN into India in 2010, a figure that rose to 20 billion in 2011 and 25 billion in 2012.

- **Organised crime**

  Organised crimes in India especially in metro cities such as Mumbai and Delhi are rising due to flourishing parallel economy. Such organised criminals also fund for radicalisation of youth and terrorist attacks.

- **Religious or ideological extremism**

  Parallel economy is greatest source of financial help to extremists. Financial incentives lure unemployed youth towards antinational activities in the name of particular religion or ideology.

- **Cybercrime**

  Crypto-currency and unrecorded cash transaction in e-commerce are also emerging means to supply resources to hostile elements in the country.

- **Armed violence**

  Armed violence which was hitherto legacy of Maoists or insurgencies is now taking a new form throughout India especially in the form of right wing extremism. Recently there has been reports of seizure of illegal weapons and public firing by individuals. Black money is easy source of illegal arms trade in India.

Measures taken by Government to contain parallel economy

- Voluntary income declaration schemes, such as Gareeb Kalyan Yojana
- Demonetisation
- Tax reforms; GST
- The Benami Transactions (Prohibition) Act
- Prevention of Money Laundering Act
- Financial Action Task force; for international cooperation in case of terror funding
- Reviewing of Double Taxation Avoidance Agreements
- Formalization of economy
- Banking reforms
- Promotion of cash less economy: Digitisation of economy

Conclusion

Though we have taken many measures to contain the parallel economy but success is far below the potential. Political will to curb corruption and organised crime, and poverty alleviation along with social will to remove the cancer of black economy from society can only lead to elimination of parallel economy and subsequently control over internal security of the country.

4. Has demonetisation been able to make a dent in terrorist funding? Critically examine.

Introduction

The central government had demonetised the high-value denomination notes in 2016 with objectives to eliminate black money, curb infusion and circulation of fake notes, create deterrence to the funding of terror and left-wing extremism, facilitate the transition of the non-formal economy into a formal economy and boost digitalisation.

Body

- The finance of terrorism in India follows a hybrid model, which includes terror funding from within and beyond the country's borders. Terrorists have employed a variety of formal and informal channels to fund their activities.
- Since illegally held cash forms the major chunk of terrorist funding, after the Demonetisation, most of the cash held with the terrorists turned worthless. Demonetisation also led to instant extinguishment of Pak-printed high quality fake Indian currency notes. It also adversely affected the hawala operators.
- While hawala cash transfers to terrorists and separatist elements based in Kashmir, which were mostly in denomination of Rs 500 and Rs 1,000, have come to an abrupt halt, Maoist groups, particularly in states like Bihar and Jharkhand, are at pains to "convert" the extortion money that has been stocked as piles of cash.
- The bigger casualty in terms of sheer volume of funds, however, is Left-wing extremism. Intercepts of recent conversations among CPI(Maoist) leaders based in Bihar and Jharkhand show them discussing the fear of losing their piles of cash collected through extortion and 'levy'.
- The financial hit likely to be taken by a terrorist group is closely linked with its cash reserves, the ability to retain liquidity in a business where terror groups choose to invest and the ease of reconverting these assets into liquid money.
- Groups in Northeast India and the CPI (Maoist) operating in the Naxal affected areas of the country are likely to be hit the most, as a large proportion of their financial reserves are more likely to have been held as cash. Further, investments in property will become relatively difficult to liquidate in order to recreate funds for organisational support mechanisms.
- In contrast, Pakistan and J&K based terror groups, while impacted, will be able to recuperate faster, as they are financed by the Pakistani state, rich donors in West Asia, voluntary collections in Pakistan, FICN or drug money.
- None of these can be impacted in the long term and to the extent that terror organisations are unable to sustain themselves. However, the impact will certainly be felt in the immediate and midterm future, wherein, the cash available for sustaining activities like civil disobedience in Kashmir Valley, will be sucked out of the terror economy.
- Two of the most vulnerable sectors that have traditionally been exploited for parking crime proceeds and black money is the property, and gems and jewellery market. These sectors have also been used for the temporary investment of terror funds. Unless transactions are made transparent and reflect real market value, black money and terror funds will continue to find their way into these businesses.
- The objective of Demonetisation is linked with removing unaccounted wealth (black money), criminal proceeds (which is different from black money), as well as FICN and Indian currency hoarded and distributed by terrorist groups.

There are different estimates of the percentage of cash within the overall share of each of these three categories. However, irrespective of the percentage of cash, it is certain that removing a major portion of cash alone will not resolve any of these challenges.

- There is a need to take interlinked steps and it is only the sum of these individual initiatives that can impact the larger fight against the financing of terrorism.

Conclusion

Demonetisation was an important step in the fight against the finance of terrorism. However, it should neither be the first nor the last, if the interlinked threats of corruption, crime and the finance of terrorism have to be controlled. These must also not be addressed simply within departmental and ministerial silos. Instead, an all-of government approach is imperative if each of these challenges is to be met.

5. Critically evaluate the institutional framework established to thwart cyber security threats in India.

Introduction

The digital economy today comprises 14-15% of India's total economy, and is targeted to reach 20% by 2024. India has more than 120 recognised 'data centres' and clouds. These factors clearly necessitate a robust institutional framework to thwart cyber security threats and secure the national cyber space.

Body

- With more inclusion of artificial intelligence (AI), machine learning (ML), data analytics, cloud computing and Internet of Things (IoT), cyberspace will become a complex domain, giving rise to issues of a techno-legal nature. Sectors such as healthcare, retail trade, energy and media face advanced persistent threats (APTs).
- Further, incidents relating to data leakage, ransomware, ATM/credit cards denial of service, diversion of network traffic intrusion in IT systems and networks using malware are also on rise. Attacks on embedded systems and IoT have also registered a sharp increase of late.
- Currently, the Information Act, 2000 is the primary law for dealing with cybercrime and digital commerce in the country. The Act was first formulated in 2000, and then was revised in 2008 and came into force a year late. The Information Technology (Amendment) Bill, 2008 amended a number of sections that were related to digital data, electronic devices and cybercrimes.
- In this regard, the Government has taken several steps to prevent and mitigate cyber security incidents. These measures and their analysis include:

- Establishment of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. Inadequate cybersecurity professionals available to partner with NCIIPC to cover the whole sector is one of the major drawbacks.
- All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously. More coherence is needed in CERT operations for greater effectivity.
- Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes. The reach of this initiative has been an issue which needs to be tackled expeditiously.
- Issue of guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
- Provision for audit of the government websites and applications prior to their hosting, and thereafter at regular intervals. Such measures need to be regularised and institutionalised.
- Empanelment of security auditing organisations to support and audit implementation of Information Security Best Practices.
- Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.
- Conducting regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.
- Further, the Government has launched the online cybercrime reporting portal, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content.
- Also, The Central Government has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

The concept of 'active cyber defence' is generally being adopted to address the new challenges. Examples of this are EU's General Data Protection Regulation (GDPR). The global multi-stakeholder model of internet governance is showing cracks. In this regard, following step can be considered in India-

- One, a concise 'National Cybersecurity Strategy' that sets clear, top-down directions to enhance the cyber resilience for the ecosystem that includes government, public and private sectors, the citizenry, and also addresses international cyber issues.
- Two, a separate 'Cybersecurity Policy' based on principles laid down in 'strategy'. It must be outcome-based, practical and globally relevant, as well

as based on risk assessment and understanding of cyberthreats and vulnerabilities.

Conclusion

According to the National Cyber Security Coordinator, India is at number 23 of the UN Global Cybersecurity Index (GCI) 2017. Thus, an accountable national cybersecurity apparatus must provide clear mandates and be empowered adequately. It must be able to supervise and enforce policies across India, including policies regulated by independent regulators.