ForumIAS

(Don't Write anything in this Area

GS Advanced Program 2023

Generic Booklet

Test Name/Code/No. : .....

Name			
Email ID.			
Roll No.			
Mobile No.		Date	

Allotted Time : 60 Minutes

Instructions to Candidates -

- There are 7 Questions in this Question paper.
- All Questions are Compulsory.
- For all updates, please visit the noticeboard – https://noticeboard.forumias.com/gsap-2023/

Important -

- Answers must be attempted in the QCA Booklet only.
- To upload the Answer Copies please visit to "My Course" section on – https://academy.forumias.com/
- Only those copies will be evaluated which will be submitted before the next class.

Q. No.	*Grade/Score*
1	
2	
3	
4	
5	
6	
7	
Overall Grade/Score	

Start Writing Here

Q.1) Cyber security refers to preventing any unauthorized or malafide access to ICT infrastructure.

Different elements

Elements	Related to Security of
1) Application Security	Software applications
2) Information Security	Data of company, customers, vendors etc
3) Disaster Recovery	Preventing malware attack + Recovery
4) Network Security	Physical Network Ex:- Firewall
5) Enduser Security	Devices of users + users themselves
6) Operational Security	End to End operation

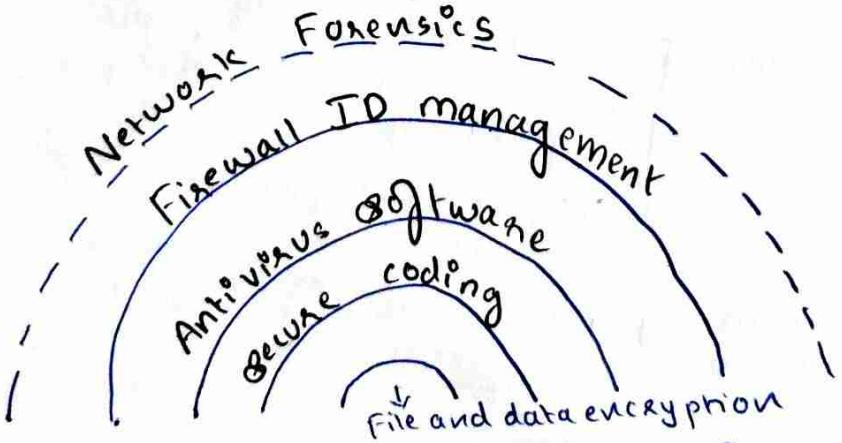


Fig: Elements / Tools of Cyber Security

Challenges to cyber security

1) Few cases reported
   - Digital illiteracy
   - Fear of reputation and credibility loss of companies.

2) Hardware & Software
   - Hardware imported from China
   - Rampant use of unlicenced and underpaid licence softwares.

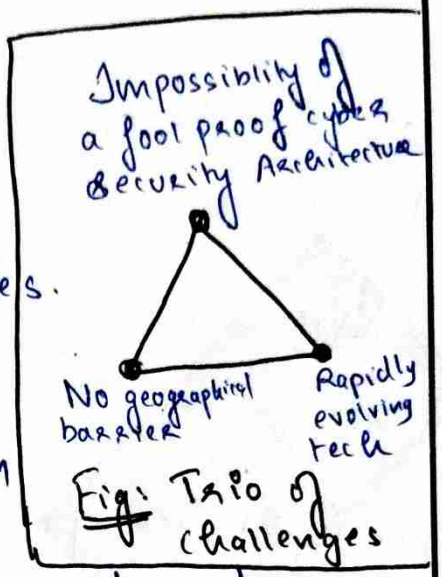


Fig: Trio of challenges

3) Lack of adaption of new technology
   - Ex Banks still use magnetic strip for card → Easy to clone!

4) Policy Issues
   - Single IT act inadequate for multiple cyber crimes
   - Multiple coordinating bodies [CERT-IN, NCCC etc]

5) Talent Issues
   - Few Indian companies make cyber security products
   - 30000+ cyber security vacancies

With growing presence of cyber ecosystem, cyber security becomes imperative

Overall Grading (√)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

Q.2) India is the 5th most vulnerable country in terms of cyber security breaches. As per CERT IN India saw atleast 1 cyber security crime every 10 minutes during 1st half of 2019 as per CERT-IN. This shows the increasing need for securing cyber space

Need for Securing Cyber Space

1) Economy Needs
- ▷ National Cybee Security Coordinator Rajesh Pant → Cybee Attacks' cost India ₹1.25 trillion loss in 2019
- ▷ Growing fintech & ICT startups in India.
- ▷ MNC presence in India. Ex Ransomware attack on Cognizant.

2) Hosility with China :→ china is a world leader in IT.

Ex Red Echo, a chinese Racker group targeted India's critical infrastructure

Ex Recent cyber attack on AIIMS ⇒ alleged to be done by china

3) Polity
↳ Government now favouring e-government services
Ex Aadhar, MyGov etc
↳ Digital Sovereignty :- Large amount of Indian user data stored in servers outside India ⇒ Data Colonization

4) Citizens
↳ Right to Privacy (Puttuswamy case)
↳ India ranks 3rd in terms of internet users after US & China.

Government Initiatives	International Initiatives
1) Cyber Surakshit Bharat → Awareness campaign	1) International telecommunication union
2) National cyber security coordination center	2) Budapest Convention on cyber crime.
3) Cyber Swachta Kendra.	3) Paris call on cyber crime.
4) CERT-N	
5) IT Act 2000	

Overall Grading (√)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

Q.3) With increasing use of cyber space by state and non state actors as a mode of warfare - cyberspace is being increasingly considered as 5th arena of warfare.

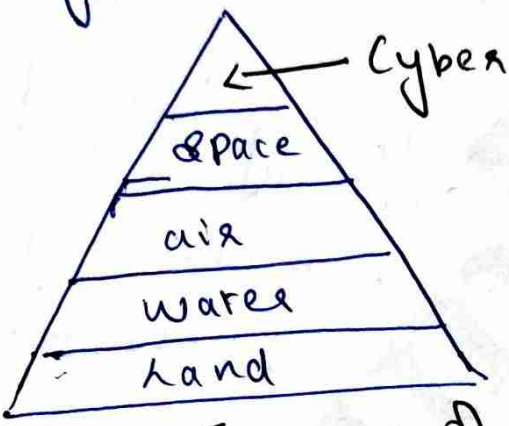


Fig: 5 arenas of warfare.

Cyber warfare is defined as organized effort by a nation state to conduct operations in the cyber space against foreign nations.

Ex Stuxnet attack:- US + Israel → attacked Irans Nuclear facility.

Ex DDos Attack in Ukraine (2014) - allegedly by Russian government

Ex Cybercriminals backed by chinese State accused of breaching The US office of personnel Management (2015)

(Don't w
anything in

4)

Countries Preferring Cyberwar

1) Borderless + Anonymous → Difficult to get caught + Escape from repurcussions

2) Less costly → Minimum setup cost
Ex North Korea (small GDP) → Massive cyber attack against Sony

3) Financial Gains → Hacking banks & financial institutions

4) Assymetric + Covert + No loss of lives

5) Increasing relaince on technology by all countries ⇒ Data is the new oil'

6) Attack on Critical Infrastructure → Massive loss to target state
Ex Iran's attack on Saudi Aramco - State owned oil & gas company.

Even non state actors like ISIS are moving to cyber warfare → End goal to build a United Cyber Caliphate

Overall Grading (√)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

Q.4) National Cyber Security policy 2013 aims to protect national cyberspace, strengthen regulatory framework and to develop suitable domestic technologies.

Though National Cyber Security policy 2013 had highly ambitious goals, its implementation is difficult due to the massive changes in cyberspace in the recent past; as shown below :-

(1) Technology → IOT, Cloud computing, Blockchain etc.

(2) Social Media explosion

(3) New Threats → Cyberwarfare, Denial of Service etc.

(4) Services → e-commerce, e-healthcare etc.

(5) Aspirations → Data Sovereignity, data localisation etc.

National cyber security falls short of keeping in pace with the above changes.

(Don't w... anything in...

Changes Required

1) A 'Digital Armed force' → with offensive & defensive capabilities against cyber warfare

2) Create a single Apex body

As of now ⇒

CERT (MeITY)	Defence Cyber research (Min of Defence)
NATGRID (Home Ministry)	CCTNS (Home ministry)

3) Focus on building 'Digital Army' → Ethical hackers, white hat ~~hackers~~, cyber lawyers etc

4) Legislation → Data protection law, Amendment to IT Act to deal with other cyber crimes.

5) Build more synergies between government & private → local, national, global.

India needs to bring in a new cyber policy encompassing all the new age changes.

Overall Grading (√)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

Q.5) Cyberwarfare is one of the different type of cyber-threats to which India is vulnerable. As per CERT IN, India saw atleast one cyber threat attack every 10 minutes during the first half of 2019

Types of Cyber Threat

1) Cyberwarfare – Organized attack by a foreign state or non state actor

Ex ISIS hacking 2000 Indian websites from Far East → End goal to build a united cyber caliphate

Ex DTrack virus attack on Kudankulam by Lazarus – a cyber arm of North Korean government

2) Cyber Espionage – Illegal access to confidential information

Ex Email infrastructure of Secy. of MeITY compromised twice in 2021 to have access to confidential information.

3) Cyber Crime / Attack

↳ Ransomware → Ex Recent attack on Delhi AIIMS

↳ Hacking → Ex Air India servers hacked in 2021 → compromising confidential information of passengers

↳ Phishing attack

83% organizations in India saw rise in phishing attack during pandemic

[Source: 'Phishing Insights 2021']

↳ Spyware attack – Through imported hardware from China or unlicenced software

Other cybercrimes like digital forgery, sale of illegal articles through dark web, is also a threat to India

India needs to adopt the 4D principle – Deter, Detect, Destroy & document to deal with these cyber crimes.

Q.6) Money laundering refers to the conversion of money which has been illegally obtained in such a way that it appears to be legally obtained

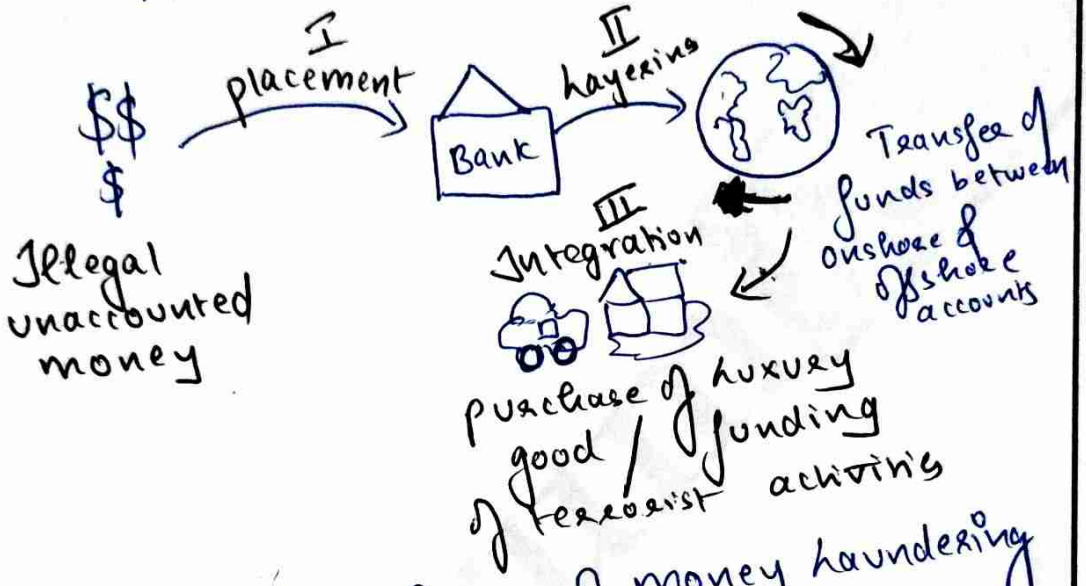
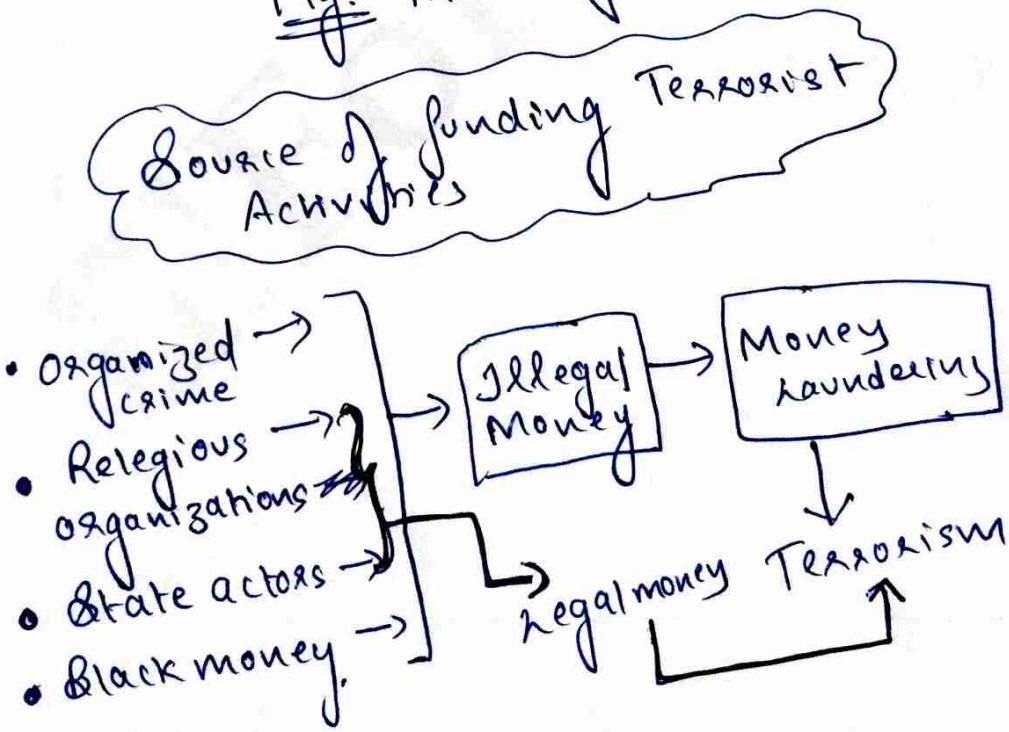


Fig: Process of money laundering



Money Laundering → Terrorism

1) **Shell companies:-** Enable terrorist groups like **Hezbollah** to hide their profits from crime [Report by Open Society Foundation]

2) **Formation of Trust & NGOs**

Black money contributed as charity → Terror funding

Ex ~~Recent~~ NIA raid in NGOs of Kashmir in connection with Terror funding.

3) **Hawala** → Funds transferred across global borders for terrorism

4) **Tax Havens** → Confidentiality + Secrecy + Opaque system → large parking of Black money → Terrorist financing

Thus Money Laundering has emerged as the financing arm of terrorism

Way forward

1. More legitimacy & power to FATF
2. Effective Implementation of UAPA
3. Effective coordination of Terror funding + Financial Intelligence cell (of NIA) unit (Min of Finance)
   + FICN coordination group (of Min of Home affairs)

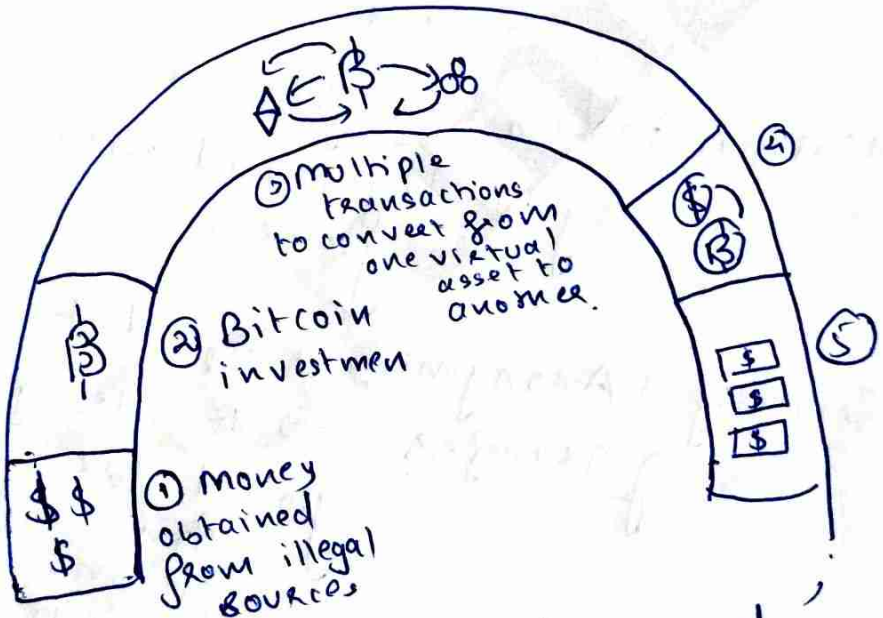
Cryptocu... curren...

Overall Grading (√)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

Q.7) Cryptocurrency refers to digital currency secured by cryptography and NFTs are a unique digital identifier that is recorded in a blockchain.

Emerged as methods to launder money and fund illicit activity



④ → Send the cleaned bitcoins to service provider that converts assets into fiat money

⑤ → Fiat money invested in banks or spend.

Why Cryptocurrency & NFT preferred

1) Easy to take Ransom payments
   Ex 2017 Wannacry ransomware attack → victims paid hackers in bitcoin
2) No government oversight
3) Blooming of Crypto service providers
   → Easier to convert laundered money to cash
4) Minimal transaction fees → Easy to layer and move across the globe.
5) Security + Anonymity + Speed + Ease of Transfer → Breeding ground for illicit activity funding.

Way forward

1) Countries to adopt FATF virtual asset guidelines

ForumIAS

2) Make KYC mandatory for crypto investment

3) Bring crypto currency & NFT to regulatory ~~plate~~ arena

Ex Government of India to tax income from crypto currency from FY 22-23.

Overall Grading (√)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9