ForumIAS

(Don't Write anything in this Area

GS Advanced Program 2023

Generic Booklet

Test Name/Code/No. : 693031

Name			
Email ID.			
Roll No.			
Mobile No.		Date	

Allotted Time : 60 Minutes

Instructions to Candidates -

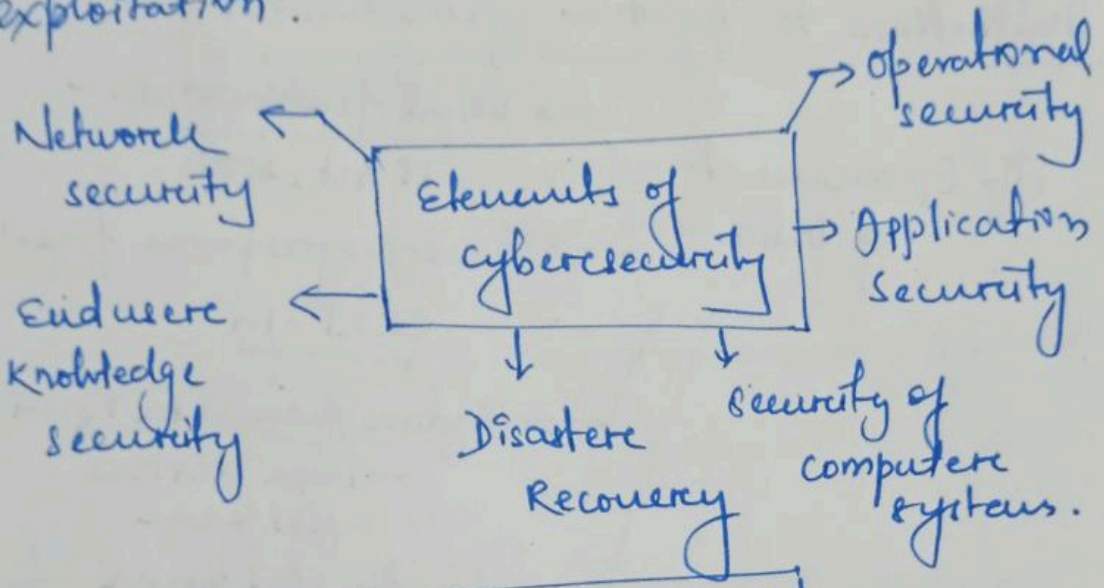
- There are 7 Questions in this Question paper.
- All Questions are Compulsory.
- For all updates, please visit the noticeboard – https://noticeboard.forumias.com/gsap-2023/

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	

Q.1) Cybersecurity refers to the techniques employed to protect computer systems, networks, critical information infrastructure etc. from unauthorized access aimed at exploitation.



Challenges to cybersecurity: —

① Governance :- 1.1) Outdated and inadequate laws – eg. ITAct, 2000

1.2) Data monopolisation by Big Tech

1.3) Lack of adequate infrastructure and trained professional

② Individuals → 2.1) Lack of digital literacy

2.2) Under-reporting of cyber attacks due to inability of system to solve cases

2.3) fears of a surveillance ~~Space~~ state

③. Technology → 3.1) >60% of hardware and software are imported from Chinese firms - Huawei and ZTE

3.2) Lack of adoption of new tech - eg. >50% debit & credit cards still have magnetic strips.

Therefore, India needs to invest in R&D to indigenize ~~IT~~ ICT and declare its public doctrine of cyber defense and warfare. This would built trust among citizens & allies & send clear signals to adversaries.

Q.2) Recently, India has been facing multiple cyber attacks from China. eg. vandalisation of AIIMS website, cyber attack on Indian vaccine manufacturer by StonePanda, etc. all have been linked to china

Need for securing cyberspace :-

① For Government :- 1.1) Increased digitization push like Aadhaar, UPI, etc.

1.2) Assert Data sovereignty with reise in data colonisation by BigTech

② For technology :- ~~+60% of hardware and softw~~ 4th Industrial revolution has led to adoption of IoT, thus, increasing vulnerabilities

③ · For individual – 3.1) Protect citizens' Informational privacy which is a fundamental right U/A-21.

Initiatives to tighten cybere security :-

① . Goverment of India → Legal framework :- IT Act, 2000

→ Emergency response force :- CERT-In

→ Cybere Swachhta Kendra - clean devices platforem

→ Sandes platforem - indigenous govt. instant messaging system

② . International → Budapest convention to harmonise national laws.

Thus, a secure cyberspace is necessary in the digital era for holistic national security.

Q.3) MeitY defines cyberspace as a complex environment involving interactions among people, software services backed by worldwide distribution of ICT.

It has emerged as 5th arena of warfare due to: ① increasing recourse to cyber attacks by state actors against enemy nations.

eg. Recent vandalising of AIIMS website has been linked to China.

② Rise in digitization and "data as new oil"

③ Increased interconnectedness due to globalisation

The reasons for countries preferring cyberwar over conventional war are:-

① Asymmetric nature – which doesn't require military prowess

② Low cost; high benefits involved

③ Anonymity – eg. CIA's UMBRAGE project's "false flag attack"

④ Involves no loss of lives

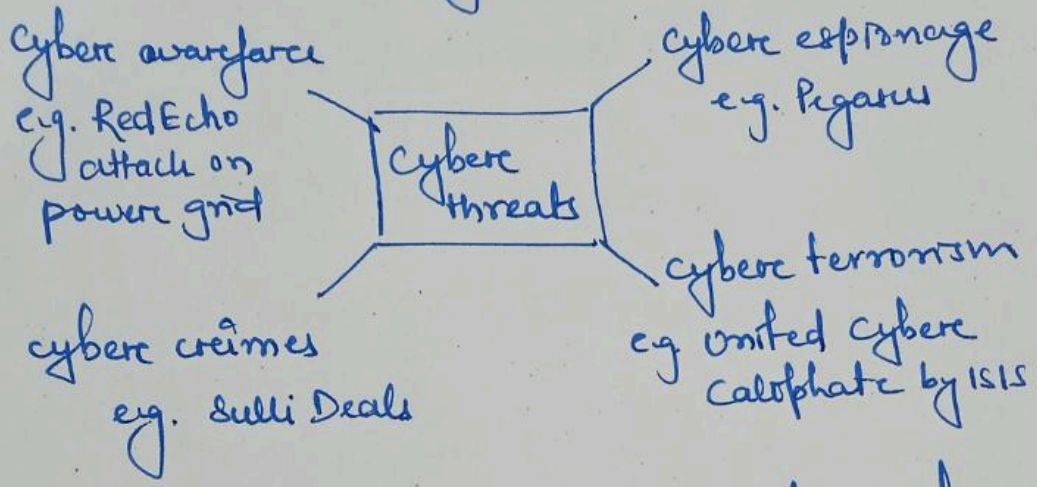
⑤ Ability to cripple economies and bring nation to standstill
eg. India's power blackout case.

Way forward:-

Experts recommend India to sign Budapest convention for global cooperation, built a team of skilled professionals, indigenize ITC sector and expedite adoption of National Cyber Security Strategy

Q.4)

India has been ranked as the 5th most vulnerable country to cybere threats. The threats faced by India are :-



Therefore, India has formed "Defense Cybere Agency" under Ministry of Defense as a tri-service command to deal with cybere threats.

Also, after the NSA spying case of 2013, India formulated the National Cybersecurity Policy 2013 with provisions like :-

1) Establishment of National Critical Information Infrastructure Protection Centre.

2) Train 5 lakh skilled professional in 5 years

3) tax benefits to businesses for adoption of security standards, etc.

However, the following challenges were faced in its implementation:

1) Governance → multiple agencies without clear demarcation of role
eg. NCIIPC, Defence cyber agency, etc.
→ Data colonisation by Big Tech

2) Technology → >60% of hardware & software are imported from chinese firm - Huawei / ZTE.

3) Individual → Digital illiteracy
→ fear of surveillance state.

Therefore, India must focus on indigenization of ICT and adopt a cyber security doctrine at the earliest.

Q.5) Cyberwarfare refers to one country employing techniques to disrupt / vandalise the computer systems, networks, critical information infrastructure in another country. Cyberspace has thus emerged as the 5th dimension of warfare.

for eg. Attack on Iranian nuclear facilities by STUXNET (joint act of US & Israel)

Defence analysts claim it to be a larger threat than Al Qaeda / terrorism because :-

① Asymmetric nature of war

↳ one doesn't need to raise huge defence infrastructure or standing army

(2). ~~Anonymity~~ - eg. US's CIA - UMBRAGE project which had "false flag attack" capability to misdirect investigation ~~agencies~~ agencies.

(3). Capacity to cripple economies -

eg. 2016 cyberattack on Bangladesh's Central Bank

(4). Internet firewalls as response to cyberwars could lead to "splinternet" and "deglobalisation"

(5). More frequent conflicts due to lowere threshold of attack.

India ~~face~~ has been ranked as the 5th most vulnerable country to cyber-attacks. The threats faced by India are:-

U.P.S.C.

Cyber terrorism

↳ use of cyber-space by terrorists

eg. cyber attack by United Cyber Caliphate (ISIS) from Malaysia and Indonesia

Cyber threats

→ Cyber warfare

↳ from state sponsored Acts

eg. Chinese firm RedEcho attack on power system of India

→ Cyber crimes like extortion, bullying etc.

eg. "Sulli Deals"

Cyber espionage ←

↳ attempt to obtain confidential information

eg. Pegasus case.

Way forward:-

India needs to focus on indigenisation of electronics and software through R&D, train skilled professional to deal with attacks, and expedite the implementation of a National Cybersecurity Strategy.

Q.6) Money laundering, as defined by Interpol, refers to concealing the source of illegal proceeds so that they appear to have originated from legitimate sources.

At the 'No Money for Terror' conference (2022), Indian Home minister said that criminal proceeds around the world launder $2-4 trillion annually, majority of which goes to terror financing. This link has been realised post 9/11 attacks.

The factors that facilitated the linkages are:-

1. End of cold war → state support to terror outfits ended → terrorists resorted to other criminal activities to sustain finances.

(2). Gllobalisation → provided seamless movement of capital and people
eg. David Headley

(3). Rise of digitisation

(4). Poore global coopercation and information sharing.

(5). Trans-national nature of money laundering, along with confidentiality in tax havens adds to the problem.

(6). In Indian case, being sandwiched between major drug producing regions - golden triangle and crescent - is a major challenge.

Money laundering and terrorism challenge the economic sovereignty, territorial integrity and unity of a nation. Therefore the following steps have been taken to tackle it :-

① By Indian govt. → PMLA
→ POEM rules for shell companies
→ e-RUPI
→ Amendments to FCRA

② Global efforts → FATF
→ Mutual Legal Assistance agreements

The 2030 Agenda for sustainable development under SDG-16 clearly asserts that - "There can be no sustainable development without peace and no peace without sustainable development". This calls for enhanced global cooperation.

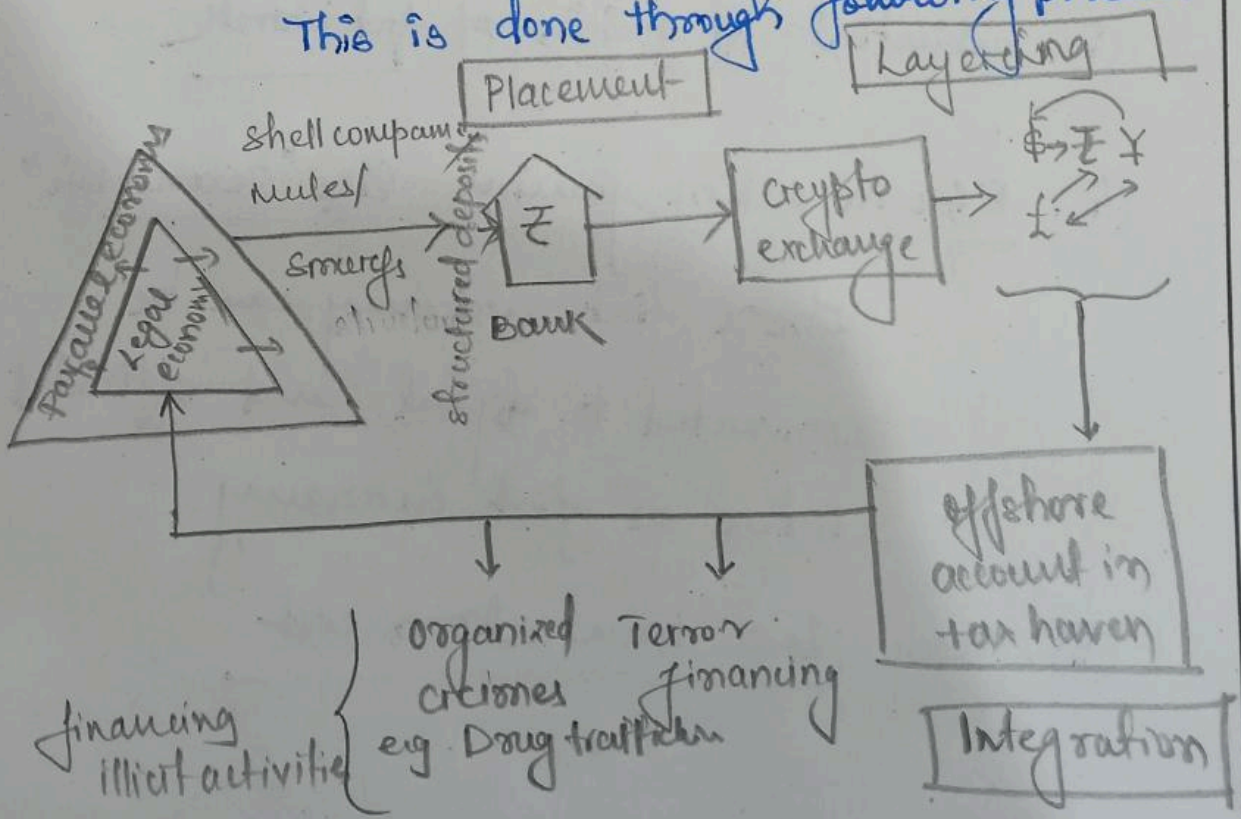
U.P.S.C.

7) Money laundering, as defined by Interpol, refers to concealing the source of illegally obtained proceeds so that they appear to have originated from legitimate source.

According to Crypto-currency Anti-Money Laundering Report, criminals laundered $2.8 billion in 2019 using bitcoin cryptocurrency.

Non-fungible tokens (which are unique digital identifiers based on blockchain) are used for money laundering through artwork.

This is done through following process:-



Cryptocurrency and NFTs are being preferred by criminals for money laundering because :-

1. Regulatory vacuum → They are not governed by Central Banks.

2. Anonymity → Art auction houses and crypto exchanges don't reveal identity of dealers.

3. Subjectivity in pricing of Art work

4. Rise in online gaming like "Second life" where fiat currency can be converted to digital and offloaded later as fiat currency.

5. Very low transaction cost

To deal with the menace, Indian government has taken steps like - taxing incomes through cryptocurrency; pilot project on Central Bank Digital currency; Bureau of Police R&D (BPRD) has issued SoP for investigations of crypto crimes, etc.