ForumIAS

(Don't Write anything in this Area

GS Advanced Program 2023

Generic Booklet

Test Name/Code/No. : ....19.....

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) What are the different elements of cyber security? Keeping in view, what are the challenges to cyber security. Examine?

Cyber security is the technique of protecting computers, networks, programs & data from unauthorised access or attacks.

Elements of Cybersecurity :-

1. Application security :- Use of hardware software to protect applications.
2. Information security :- tools for securing digital information.
3. Network security – protecting networks.
4. Operational security – classification & control required to protect information assets.

(Don't Write anything in this Area

(5) Disaster recovery plan
(6) End user education

Challenges to cybersecurity :—

(1) High no. of users - due to increased penetration of mobile & internet.
eg:- rural population are not aware about cybersecurity practices.

(2) Inadequate legal & policy frameworks
eg:- Single IT Act.

(3) lack of cybersecurity specialists.
eg:- Nasscom projected India would need 1 million cyber security experts by 2020.

While coming of New Digital India, India need comprehensive & strict cyber laws to prevent cyber attacks.

Overall Grading (√)

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

Q.2) Discuss the need for securing the cyber space especially in the recent context of China. What has been the Government and international initiatives to tighten the cyber security of India?

Ans According to Recorded future (US based cybersecurity firm) revealed targeted intrusions against India's from Chinese state-sponsored groups.

Need for securing cyberspace:—

1. China as a threat:—
   - 1.1) China targeted at least 10 Indian power sector organisations ~~their~~ & 2 Indian ports.
   - 1.2) Mumbai- power outages is alleged to be carried out by Chinese state-sponsored group Red Echo.
2. Cyberspace has become 5th arena of war.
3. To secure digital payment platforms
4. According to CERT IN: India experienced cyber attack every 10 minutes in 2019.

(Don't Write anything in this Area)

Govt. & international initiatives to tighten the cyber security of India:-

(1) Information Technology Act, 2000:-
Regulates computers, computer systems, networks, data and info in digital format.

(2) IT Act (Amd) 2008:- includes provision to deal with data protection.

(3) National cyber security policy 2013

(4) USA has a seperate cyber command center - to counter all adverse cyber activities.

(5) Israel Defence force has created two elite units for cyber warfare viz. C4I and military intelligence.

On the lines of global practices, India should also establish a dedicated cyber command to ~~deal~~ secure the cyber space.

Overall Grading (√)

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

Q.3) Why is the Cyber-space has been termed as 5th arena of warfare. What are the most probable reasons for countries preferring cyber war?

Ans Cyber-space has been termed as 5th arena of warfare after land, air water & space.

Increased relevance for becoming 5th arena of warfare because:-

① Rise of IT - in the global economy and connected people & markets

② 'Data' has become the 'new oil' - the most precious commodity.

③ Emerging economies has weak cyber laws - which becomes a soft target for hackers.

④ No comprehensive global rules on cyberspace.

(Don't Write anything in this Area)

Reason's for countries preferring cyber ware :-

① Cyberspace allows for groups to remain anonymous.

② Very low cost, compared to traditional warfare.

③ Economic gains - by compromising the digital economic platforms & transactions

④ Geopolitical interest - spying and stealing confidential information.

⑤ Due to fast changing & complexity of cyber attacks - it is preferred.

The world need a comprehensive global rules which should be borderless - to prevent cyber attacks

Overall Grading (√)

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

.4) Considering the threats cyberspace poses for the country, India needs a 'Digital Armed force' to prevent crimes. Critically evaluate the National cyber security policy 2013 outlining the challenges perceived in its effective implementation.

Cyberspace has become the 5th Arena of war due to rise in global IT. India needs a 'Digital armed force' for cyberspace to tackle the increased cyber attacks.

National cyber security policy, 2013 is a policy framework to create a secure cyberspace ecosystem & strengthen the regulatory framework. Also compliance to global security standards to create assurance framework.

(Don't Write anything in this Area)

Challenges to National cyber security policy, 2013 :-

① Did not specify what comes under the 'critical information infrastructure'.

② lacks detailed implementation guidelines and plan of action.

③ Too much of government intervention could undermine business innovation, making it uncompetitive.

④ Policy needed deeper analysis based on experiences of other ~~et~~ countries.

⑤ No specific strategy to safeguard the privacy of citizens.

Various cybersecurity firms and groups should come together under an umbrella for effective implementation of cyberlaws.

Overall Grading (√)

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

Q.5) Cyberwarfare is considered by some defence analysts to be a larger threat than even Al-Qaeda or terrorism. Outline the different types of cyber-threats to which India is vulnerable with recent examples?

Cyber warfare includes the actions by a nation-state or its proxies to penetrate another nation's computers or networks for the purpose of espionage, causing damage or disruption.

Cyber warfare is considered more dangerous than terrorism because of :-

1. It allows the hacker to remain anonymous.
2. Low expenditure than traditional warfare.
3. There are multiple sources of cyber threats.

Different Types of Cyber threats:-

① Computer virus - program that attaches itself to application & runs along with it.

② Malware - inserted into system covertly, to compromise confidentiality.

③ logic bomb - destroys data.

④ Spoofing - to fool biometric sensor.

⑤ Phishing - targets are lured by mails to provide sensitive information.

Recent Cyber threats to India:-

① Pegasus spyware - ability to stealthily enter a smartphone and gain access to everything including camera & microphone.

② ~~Botne~~ Mirai Botnet - to remotely controlled computers.

(Don't Write anything in this Area

③ Union Bank of India heist in 2016 – by phishing email sent to employee.

④ Wannacry ransomware – ransom of money was asked when computer was locked without owner's permission.

⑤ Data theft at Zomato in ~~January~~ 2018.

⑥ Hacking of Bihar education website.

Way forward:–

① Protection of data by privacy laws.
② Regular back of data by individuals.
③ Repository of IT professionals to deal with cyber security issues.
④ Security framework should be envisaged in PPP mode.

Gulshan Rai Committee has recomended to link NATGRID and CCTNS to deal with cybercrimes.

Overall Grading (√)

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

Q.6) Money laundering is an issue that has gained increasing significance following the events of 9/11. It has recognized it as a source of the funding of terrorist activities. Comment?

According to INTERPOL, Money laundering is concealing or disguising the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources.

The attack at 9/11 brought into attention the impact of Money laundering into funding terrorist activities.

Process of Money laundering :—

Placement → Layering → Integration

Placement: dirty money into financial system

Layering: multiple transfers of money

Integration: investments or purchase of items.

Impact of Money laundering :—

① Undermine the integrity of financial market - dampens foreign investments

② leads to volatility in exchange rates due to unanticipated transfers.

③ leads to inflation - effect felt by underpriviledge sections.

④ Revenue loss to the public exchequer

⑤ Increased criminality in society.

⑥ Drug trafficing, smuggling, corruption.

Government initiatives :—

① PMLA, 2002 :- legal framework to combat money laundering

② Fugitive Economic offenders Act, 2018 - to confiscate properties.

③ Directorate of Enforcement for enforcement, investigation of cases under FEMA, 1999.

④ Global efforts includes Financial Action Task force, DTAA, UN ~~Office~~ Global programme against Money laundering 1997.

Way forward :-

① Create special cells to deal with Money laundering with linkages to INTERPOL

② FATF Recommendations :-

2.1) identifying the risks.

2.2) developing policies & domestic coordination.

Mutual legal assistance should be provided between countries so as to effectively combat money laundring

Overall Grading (√)

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

(Don't Write anything in this Area

Q.7) New technologies like cryptocurrency and even NFT's have emerged as new methods to launder money and also are used to fund illicit activities. Analyse the statement?

Ans

According to IMF Global Money laundered is estimate to be between 2-5% of the world's GDP.

There are various mechanisms to launder money of which cryptocurrency and NFT's have emerged as new, due to increased digitalisation & rise in IT.

Methods ~~of~~ for Money laundering :—

① Smurfing - placement where cash is broken into smaller chunks and deposited into various bank accounts.

② Creation of shell companies.

(3) Bulk cash smuggling – cash is physically smuggled to another jurisdiction.

(4) Hawala Transactions – transferring money with the help of brokers.

(5) Keeping money in tax heavens to avoid taxes.

(6) Art & ~~other~~ Art works – buying & selling in auction.

(7) NFT – ~~to~~ conversion of any artwork into digital assets and trading.

(8) Cryptocurrency – is used ~~to~~ for laundring due to its highly decentralised and anonymous nature.

Challenges in preventing money laundering :–

(1) Non-fulfillment of KYC norms by ~~banks~~ banks.
(2) Tax heaven countries.
(3) Technological revolution –

(Don't Write anything in this Area

coming at new technologies like NFT & cryptocurrency.

(4) DTAA's - & have loopholes, which is used by groups for their advantage

(5) Nexus between criminals & politicians

Way forward:-

(1) Comprehensive IT laws including safeguard mechanism for data privacy

(2) Regulation of cryptocurrencies.

(3) Mutual legal assistance should be provided between countries

(4) ~~to~~

There should be continuous upgradation and dissemination of informations, so any aberration can be flagged within time.

Overall Grading (√)

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