ForumIAS

(Don't Write anything in this

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	

This Generic QCA booklet can be used to attempt all GS Advanced Program Tests.

Start Writing Here

1) Cyber security includes techniques of protecting computers, networks, programs and data from any threat, cyber terrorism, cyber espionage etc.

Elements of cyber security

① Application security :- while using application → it usage should be secure

eg: Anti virus softwares.

② Information security → as provided by social media giants eg: End-to-End encryption.

③ Network security - as provided in windows firewall for complete network security.

④ Operational security - captcha code provided in websites for login

(Don't write anything)

2)

(5) Disaster Recovery Plan → after hitting by cyber attack [eg:] IBM's cloud

Challenges to cyber security

(1) Data colonisation - servers are located outside India → sometimes disrupt political system [eg:] Cambridge Analytica.

(2) Widespread illiteracy (30%) → lack of awareness about cyber hygiene.

(3) Increasing cost - currently around 4bn USD → next 10 years - 20bn USD (WEF).

(4) Substandard devices - rampant use of unlicensed software.

(5) Dependence of import → majority of electronics imported china → increases country's vulnerability.

Government has come up with Cyber Suraksha shit scheme, National Policy of Cyber security 2020 are steps in right direction to curb these challenges.

Overall Grading (√)

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

This Generic QCA booklet can be used to attempt all GS Advanced Program Tests.

(Don't Write anything in this

2)

India suffers an average of nearly 2,00,000 threats every day as per US based cyber security firm - Norton.

Need for securing cyber space

① Data Sovereignty → with increased focus on data colonisation → need to secure cyber space.

② Secure Critical Infrastructure

↳ Health → recent attack on AIIMS - data breach of 3-4 crore patient.

↳ Power sector - Red echo attack on at least 10 Indian power sector.

↳ Vaccine development - Stone Panda attack (China).

③ Heavy dependence on chinese imports - [eg:] Huawei accused of privacy breach issues.

Government Initiatives

① Cyber Suraksit Bharat Initiative – spread awareness about cyber crime.

② National cyber security Strategy based on 3 pillars | secure → strengthen → synergize.

③ CERT-IN – Nodal agency to look into cyber crime cases.

④ Cyber Swachhta Kendra → users can wipe out malware

International Initiatives

① Budapest convention → address cyber crime

② Paris call for trust and security in Cyber space

③ Osaka Track – Japan proposed free movement of data.

Cyber space has been emerging as 5th Arena of warfare therefore, national and international collaboration is the need of the hour.

Overall Grading (√)

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

(Don't Write anything in this

3) PM Modi asserted that issues regarding cyber security are no longer limited to digital world alone. It has become a matter of National security.

Cyber-Space - 5th Arena of Warfare

① Threat to financial Institution

↳ Indian Bank System attacked - 3.2 million debit card data compromised.

② Social Infrastructure

↳ Education → Turkish attacker → Hacks Bihar Education website (2016)

↳ Health → Recently, AIIMS website attacked - Ransomware - $200 crore in bitcoin.

③ Energy security → In 2022 Oil India Limited attacked → disrupt energy supplies.

(Don't W anything

④ Security - Stuxnet - Attack of Iran's Nuclear programme.
↳ ISIS attack → 2000 Indian websites compromised.

Reasons for countries preferring cyber war

① Borderless and anonymity - Cimes → are borderless

② Low cost in comparison to conventional war. → low cost of set up.

③ Monetary benefit - attack on financial institutions and banks → money

Ex: Attack ~~on~~ Bo

④ Reliance on technology - advent of AI, Machine learning → difficult to cope up with changing technologies.

⑤ Policy → weak cyber security laws across countries.

As it is rightly said Data is a new oil - therefore robust cyber security law and greater awareness of cyber hygiene would eliminate challenges related to this 5th arena of warfare.

Overall Grading (√)

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

This Generic QCA booklet can be used to attempt all GS Advanced Program Tests.

4) India is the 5th most vulnerable country in the world in terms of cyber-security breaches. India saw at least 1 cybercrime in every 10 minutes as per CERT-IN

Need a "Digital Armed Force"

① Increased Internet users → India ranks 3rd in terms of net users → highly prone to cyber crimes.

② ~~Lyt~~ Widespread illiteracy - lack of awareness of cyber hygiene → exploited by cyber criminals. eg: Jamtara village has become cyber crime capital of India.

③ Increasing Online transactions - 1st half of 2020 saw - 70% of e-commerce transactions via mobile and online payments.

④ Borderless nature of crime → as 75% of crime is done - borderless.

National Cyber security Policy 2013

↳ Creation of secure cyber ecosystem
↳ Compliance of to global security standards
↳ Robust Infrastructure → ensure human capacity development (5 lakh).
↳ Creation of NCIIPC to protect critical Infrastructure - 24×7 operations.

Issues

↳ No specific strategy to safeguard privacy.
↳ Lacked detailed implementation guidelines and plan of action.
↳ Did not specify what come under critical infrastructure.
↳ Too much government intervention may undermine business ecosystem.

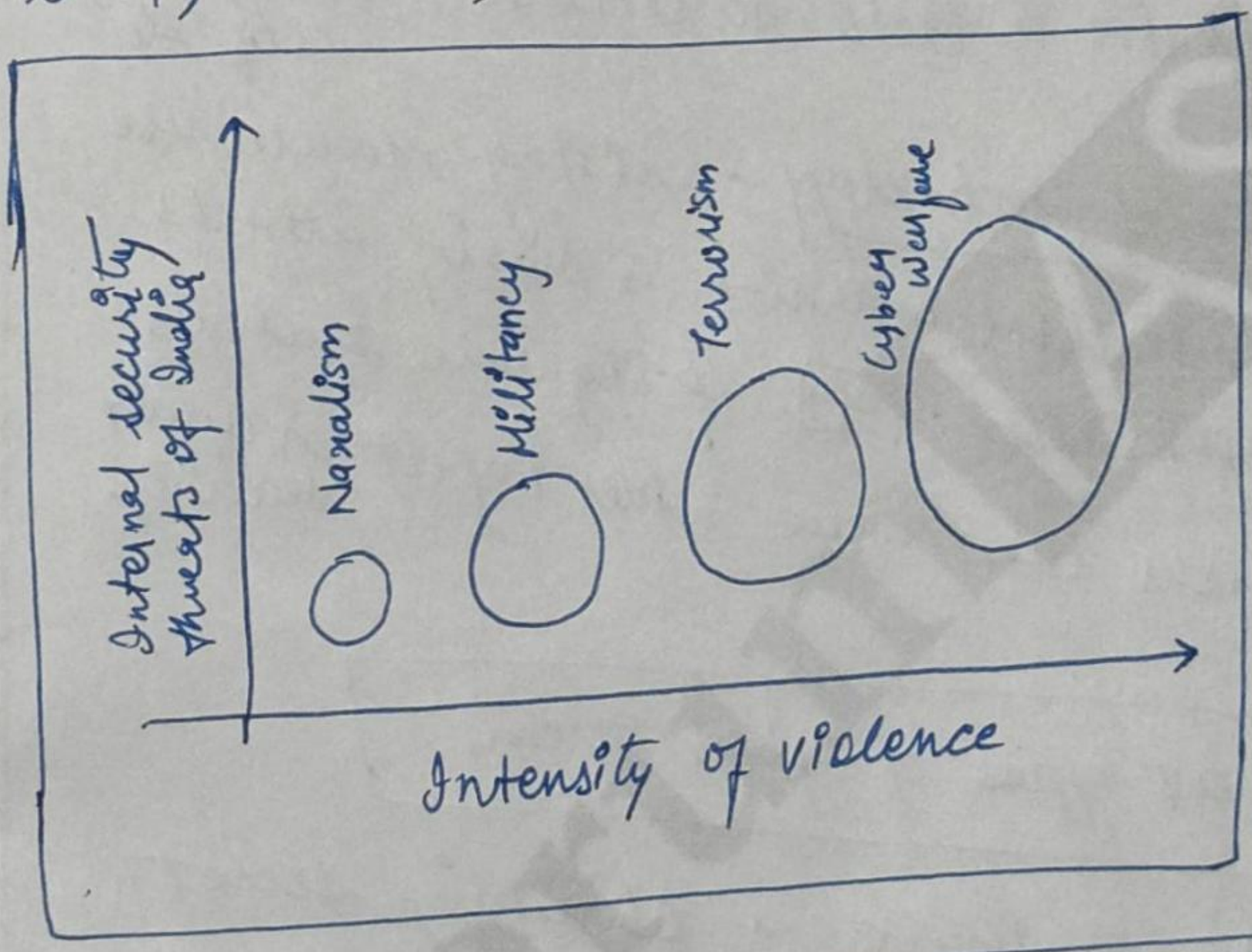
India was ranked 10th in Global security Index 2020. Though there has been significant improvement in comparison to previous ranks but dynamic nature of cyber crime still pose many challenges.

Overall Grading (√)

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

This Generic QCA booklet can be used to attempt all GS Advanced Program Tests.

.5) Cyber warfare is considered as the 5th arena of warfare after land, water, air and space.



Cyber warfare - larger threat than even Al-Qaeda

① Borderless Nature - No physical barriers attached → also it is anonymous → hardly identified.

② Low cost in comparison to conventional wars → low set up cost and committing it.

anything

(3) Wider impact - without impacting lives it jeopardises economic, political life of a person. eg: ISIS attack on 2000 Indian website → tactic to establish United Cyber Caliphate.

(4) Use of technology - using modern use of AI, Machine Learning → making attacks sophisticated. eg: Spyware such as Pegasus can have wider impact on cyber security.

Different types of cyber threats

(1) Cyber Espionage → obtaining secret information without taking permission.

eg: In 2021 → Ministry of Electronics, Information and Broadcasting's - email infrastructure compromised.

(2) Cyber attack - stealing of data, money using illegal methods.

eg: Indian Banking system - 3.2 millions debit card data compromised.

(3) Cyber Terrorism - convergence of terrorism and cyber space.

eg: True cyber army of Pakistan attacked websites of Kerala government, CBI, ECI and ASER.

(4) Cyber warfare - Action by nation state to penetrate another nation's computer for purpose of causing damage.

eg: In 2019 → Attack on Kudunkulam Nuclear Power Plant.

Measures to tackle

1. Greater Cyber Hygiene
2. Signing of Budapest convention
3. Data Protection Law should be brought up.

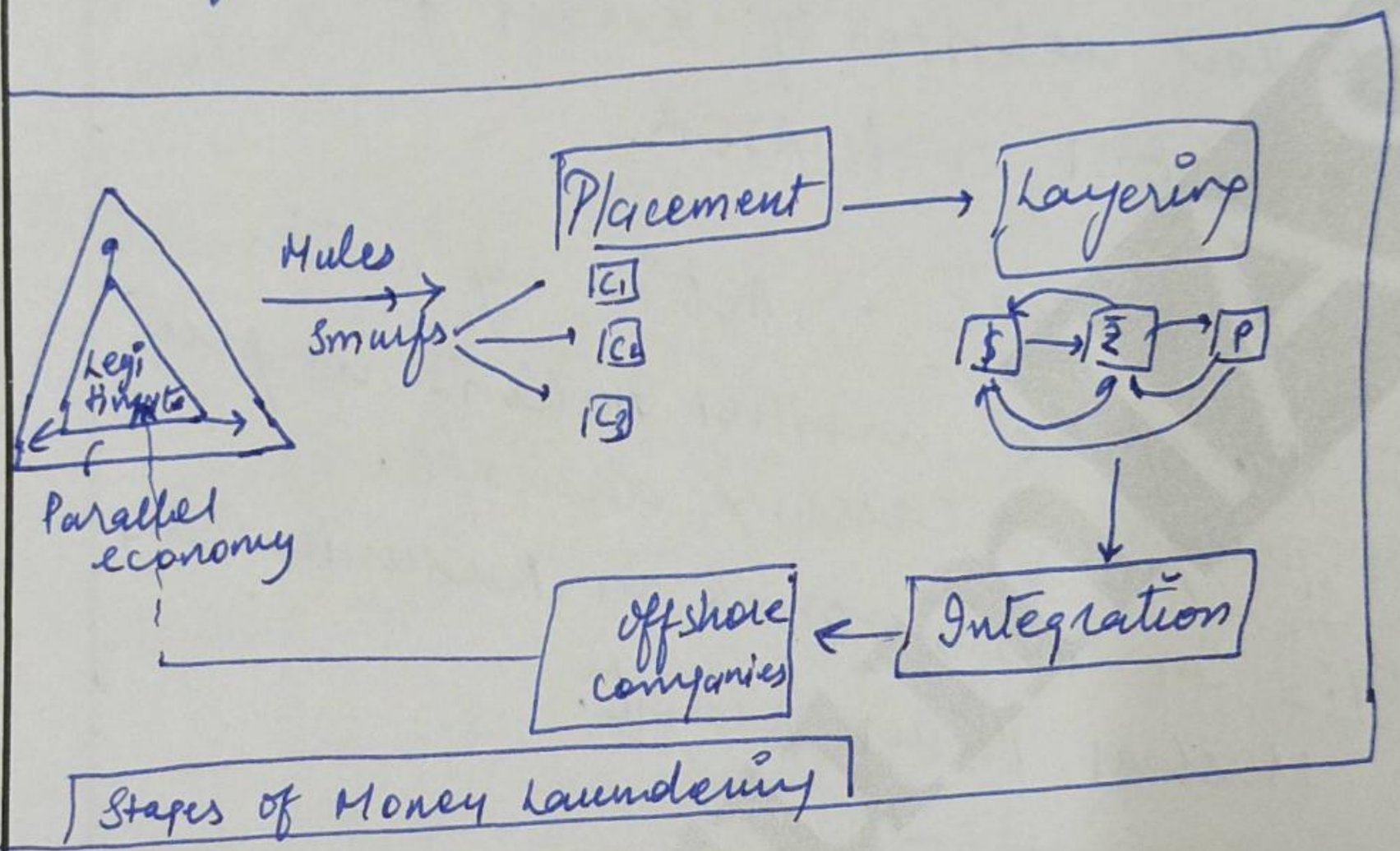
Cyber threats is a serious emerging challenge to nation across defence, economy, social etc. Digitization needs to be coupled with measures for personal and national security.

Overall Grading (√)

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

Q.6)

Money laundering is process of making illegitimate 'dirty money' appear as legitimate 'clean money'.



According to IMF - global money laundering is estimated to be between 2%-5% of the Global GDP and has gained significance:-

① Easier way to place black money to get unnoticed.

② Terrorist groups operate in different regions → money laundering helped them

to acquire arms and ammunitions.

(3) Hawala transactions charge comparatively less fees than conventional banking infra structure.

(4) No limit is attached for the amount of money to be laundered.

source of funding - terrorist activities

(1) Bulk cash smuggling - involving physical smuggling of cash to another jurisdiction.

(2) structural deposits - placement of cash in smaller chunks of money and deposited onto various bank accounts.

(3) Hawala routes - NIA investigations revealed that steady flow of funds through hawala in kashmir valley for terror financing.

④ Digital electronic money → convert from cash to crypto currency and vice versa.
↳ Help to main anonymity

⑤ Other sources → Bribery
↳ Kidnapping
↳ smuggling of drugs, poaching, narcotics

Government Initiatives to tackle the menace

① PMLA, 2002 - to prevent and control money laundering.

② Narcotics Drugs and Psychotropic Substances Act 1985.

③ Member of FATF - watchdog of money laundering at international arena

④ Fugitive economic Offenders Act 2018

India has 3rd highest trade related illicit financial flows (Global financial Integrity 2020) - there is dire need to implement existing laws robustfully.

Overall Grading (√)

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

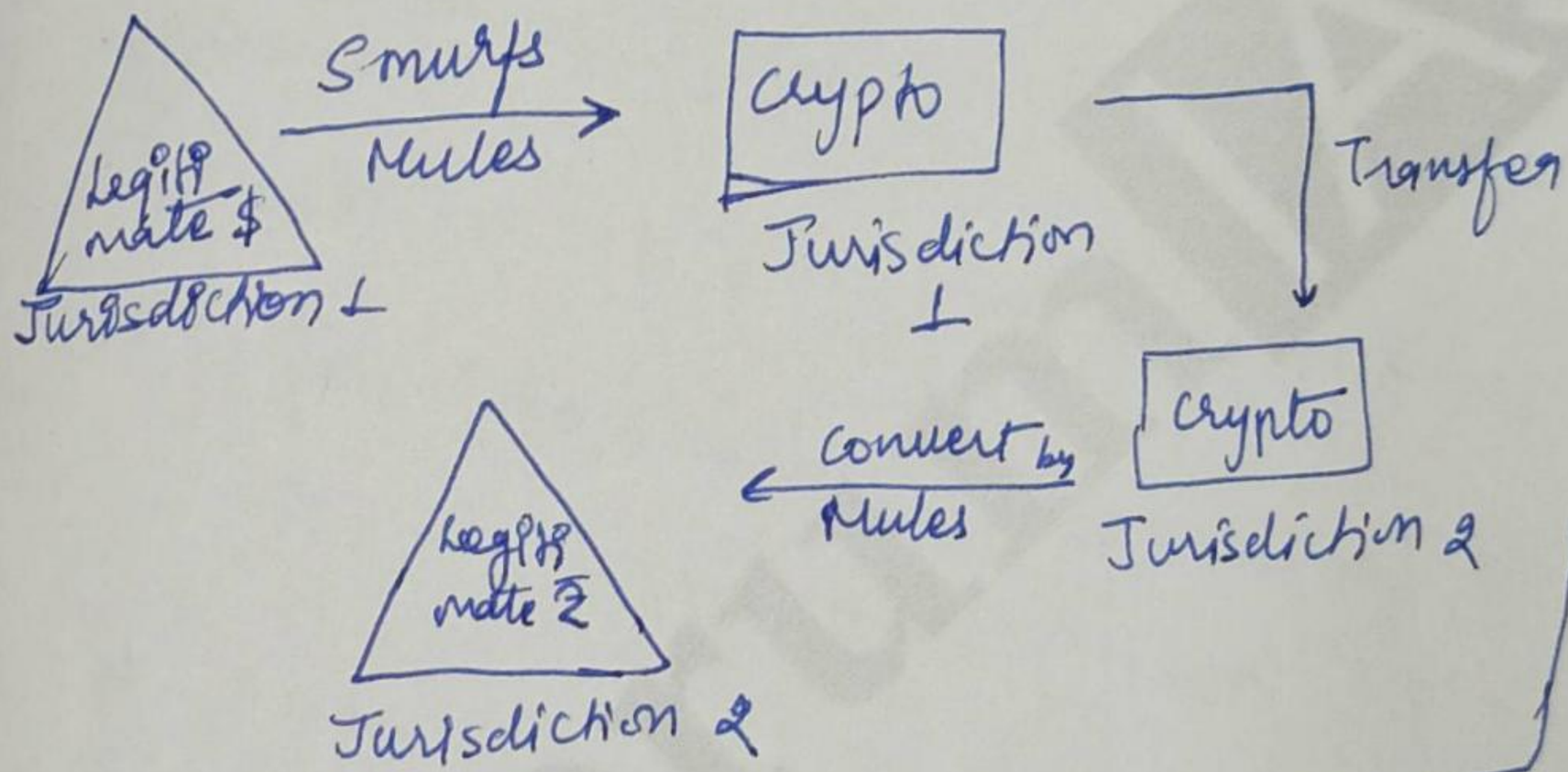
This Generic QCA booklet can be used to attempt all GS Advanced Program Tests.

anything

(Don't Write anything in this

.7)

According to cryptocurrency anti money laundering report - Criminals laundered $ 2.8 billion in Bitcoins in 2019.



New technologies - New methods to launder

① Policy - Lack of policy/regulators across the world on cryptocurrency and NFTs → give leverage to criminals.

(2) NFTs - still low awareness and is seen only in upper class individuals → low social acceptance → easy to launder.

(3) Anonymous Nature - laundered money got unnoticed by law enforcement agencies - due to usage of blockchain technology.

(4) Use of technology - use of unconventional platforms such as deep web, deepfakes - get launders an upper hand.

(5) Digital nature - no requirement of bulk cash smuggling from one place to place.

Impact of new technologies

(1) Economy → loss of revenue to public exchequer.

(2) Security → financial terrorism

→ Use for smuggling of arms to Naxals and insurgents - disturb internal security.

(3) Vulnerable to cyber attacks - as ransomware attacks on a rise → ransom asked in Bitcoins - ~~extract~~ eventually use to fund terrorism.

(4) Social - misguided youth → learn new techniques → detrimental to the country; demographic dividend.

(5) Promotes crime → eg: criminal economy of small towns like Jamtara.

Measures:
- Narcotic drugs Act 1985
- PMLA 2002
- FATF
- FEMA
- Fugitive Offenders Act 2018

The standing committee on finance estimated the amount of Black money may vary from 7% of GDP to 120% of GDP. → Making it more vulnerable to money laundering crimes with growing technologies.

Overall Grading (√)

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