GS Paper - 3
Security – Aug'18

CERT-In Report on Cyber Attacks

Syllabus: Basics of cyber security

***Also refer the topic National Information Security Policy and Guidelines (NISPG) from July CA magazine*.**

In News

- Indian Computer Emergency Response Team (CERT-In) has prepared a report which analysed cyber attacks from April-June 2018.
- The report has been sent to the National Security Council Secretariat (NSCS) and other security agencies.

Key Highlights

- The report said that the maximum number of cyber attacks on official Indian websites are from China, US and Russia.
- It has also flagged the possibility of "malicious actors from Pakistan using German and Canadian cyberspace for intruding into Indian cyberspace and carrying out malicious activities.
- The cyber attacks from China made up 35% of the total number of cyber attacks on official Indian websites, followed by US (17%), Russia (15%), Pakistan (9%), Canada (7%) and Germany (5%).
- The report has identified many of the institutions impacted by the malicious activities, and they have been advised to take appropriate preventive action.
- These include Oil and Natural Gas Corporation (ONGC), National Informatics Centre (NIC), Indian Railway Catering and Tourism Corporation (IRCTC), Railways, Centre for Railway Information Systems (CRIS) and some banks like Punjab National Bank, Oriental Bank of Commerce, State Bank of India and state data centres, particularly in Maharashtra, Madhya Pradesh and Karnataka.

Internet Security Threat Report 2017

- The latest release of Internet Security Threat Report, by security solutions provider *Symantec*, summarizes the state of cyber threats across the world.
- According to report, India emerged as third most vulnerable country in terms of risk of cyber threats, such as malware, spam and ransomware in 2017. India has moved up by one place over previous year.
- India is ranked third among list of countries globally where most of the threats were detected and it is second in terms of targeted attacks. The United States led the pack, followed by China at the second spot.
- India was ranked second globally when it comes to spam and phishing (misleading emails, weblink etc). However, complex cyber attacks -- ransomware and network attacks in India increased in terms of global percentage.

- The report said that India is one of victims of targeted attack because a lot of intellectual property rights are generated here and the criminals may intent to steal them.
- India was also ranked second after the US where the highest number of malwares for mobile phones were detected the by company.

CERT – In

- CERT – In is the national nodal agency for responding to computer security incidents as and when they occur.
- In the recent Information Technology Amendment Act 2008, CERT – In has been designated to serve as the national agency to perform the following functions in the area of cyber security:
  - Collection, analysis and dissemination of information on cyber incidents.
  - Forecast and alerts of cyber security incidents
  - Emergency measures for handling cyber security incidents
  - Coordination of cyber incident response activities
  - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
  - Such other functions relating to cyber security as may be prescribed

***Also refer the topic National Information Security Policy and Guidelines (NISPG) from July CA magazine*.**

Benami Transactions (Prohibition) Act

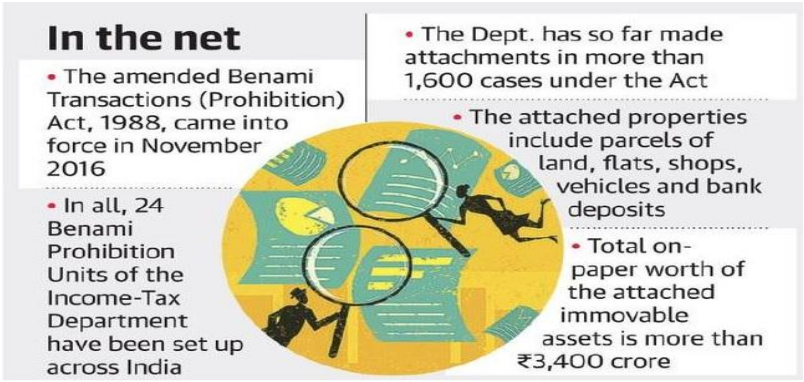
Syllabus: Money-laundering and its prevention

In News

- Special Courts under this act have not yet been set up across the country.
- This has scuttled the prosecution of accused persons in almost 100 confirmed cases instituted under this act.

Key Highlights

- The Act provides that the Central government, in consultation with the Chief Justice of the respective High Courts, will establish Special Courts through notification. Such courts are to be constituted to ensure that the trials are conducted "as expeditiously as possible".
- However, the required Special Courts have not been set up yet. Therefore, despite the fact that investigations in almost 100 cases have been completed by the I-T Department in different States, including confirmation of attachment of properties by the Adjudicating Authority, the prosecution of accused persons has not started.



Assets worth more than ₹5,000 crore have been attached by the Income-Tax Department under the law.

About The Act

- Though the Benami Transactions (Prohibition) Act, 1988 has been on the statute book since more than 28 years, the same could not be made operational because of certain inherent defects.
- With a view to providing effective regime for prohibition of benami transactions, the said Act was amended through the Benami Transactions (Prohibition) Amended Act, 2016.
- The Act seeks to: (i) define the benami transactions, (ii) establish adjudicating authorities and an Appellate Tribunal to deal with benami transactions, and (iii) specify the penalty for entering into benami transactions.
- The act defines Benami transactions as transactions where: (i) the transaction is made in a fictitious name, (ii) the owner is not aware of denies knowledge of the ownership of the property, or (iii) the person providing the consideration for the property is not traceable.
- However, certain cases has been exempted from the definition of a benami transaction. These include cases when a property is held by: (i) a member of a Hindu undivided family, and is being held for his or another family member's benefit, and has been provided for or paid off from sources of income of that family; (ii) a person in a fiduciary capacity; (iii) a person in the name of his spouse or child, and the property has been paid for from the person's income
- The act defines benamidar as the person in whose name the benami property is held or transferred, and a beneficial owner as the person for whose benefit the property is being held by the benamidar.
- The act seeks to establish four authorities to conduct inquiries or investigations regarding benami transactions: (i) Initiating Officer, (ii) Approving Authority, (iii) Administrator and (iv) Adjudicating Authority.
- If an Initiating Officer believes that a person is a benamidar, he may issue a notice to that person. The Initiating Officer may hold the property for 90 days from the date of issue of the notice, subject to permission from the Approving Authority.
- At the end of the notice period, the Initiating Officer may pass an order to continue the holding of the property.
- If an order is passed to continue holding the property, the Initiating Officer will refer the case to the Adjudicating Authority. The Adjudicating Authority will examine all documents and evidence relating to the matter and then pass an order on whether or not to hold the property as benami.
- Based on an order to confiscate the benami property, the Administrator will receive and manage the property in a manner and subject to conditions as prescribed.
- It also seeks to establish an Appellate Tribunal to hear appeals against any orders passed by the Adjudicating Authority. Appeals against orders of the Appellate Tribunal will lie to the high court.
- The penalty for entering into benami transactions is rigorous imprisonment of one year up to seven years, and a fine which may extend to 25% of the fair market value of the benami property.

- The act also specifies the penalty for providing false information to be rigorous imprisonment of six months up to five years, and a fine which may extend to 10% of the fair market value of the benami property.

Quad Countries On Ocean Security

In News

- A report on the policy recommendations on Indian Ocean security has been released by four think tanks from the Quad countries.
- This report consists of 20 policy recommendation.

Key Highlights

- The report mentions that Australia, India, Japan and the US should work with partner countries to oppose the establishment of permanent Chinese military bases in the Indian Ocean Region (IOR).
- It said that the Quad nations should work in the IOR to help maintain independent security and economic policies by supporting high-quality alternatives to unilateral Chinese investments and "political alignments with regional objectives".
- One of the suggestions for the US and Japan was also to consider participation in the Asian Infrastructure Investment Bank (AIIB) to encourage high-standards for projects involving China and to build their economic cooperation with others, including Australia and Japan.
- The report also suggests that the Quad countries should cooperate with and support the Indian Ocean Rim Association (IORA), the Indian Ocean Naval Symposium (IONS), the South Asian Association for Regional Cooperation (SAARC) and other regional framework in the Indian Ocean and South Asia.
- The report urged Australia, India, Japan and the US to enhance sea land defence capabilities in the Indian Ocean and suggested that India, the US and Japan should invite Australia to participate in the currently trilateral maritime exercise.

Quad Group:

- In a significant geostrategic move India, the US, Japan and Australia resurrected their quadrilateral grouping on the sidelines of the Asean summit in Manila.
- The grouping of four countries aims to pursue their common interest in the Indo-Pacific.
- The leaders of the four countries met at Manila in November last year to hold their first talks. In June 2018, senior officials of the Quad countries held their second consultative meeting in Singapore on the sidelines of an Association of Southeast Asian Nations senior officials meeting.
- This grouping gives New Delhi a powerful platform to advance its interests in East Asia, coordinate strategies with powerful friends and add more strength to its Act East initiative.
- India was circumspect about the grouping because it felt that its interests may not get properly represented within the forum. Plus, given the current status of the India-China relationship, New Delhi may not have wanted to rock the boat too much in east Asia either.

Ballistic Missile Interceptor Advanced Area Defence

In News

- India has successfully test-fired its indigenously developed supersonic interceptor missile.
- Developed as part of efforts to have a multi-layer ballistic missile defence system, it is capable of destroying incoming hostile ballistic missiles.

Key Highlights

- The supersonic ballistic interceptor missile dubbed as Advance Air Defence (AAD) was fight tested from Abdul Kalam Island, a part of Integrated Test Range (ITR) off Odisha coast.
- The endo-atmospheric missile showed its capability of intercepting incoming targets at an altitude of 15 to 25 km.
- The interceptor is a 7.5-metre long single stage solid rocket propelled guided missile equipped with a navigation system, a hi-tech computer and an electro-mechanical activator.
- The interceptor missile had its own mobile launcher, secure data link for interception, independent tracking and homing capabilities and sophisticated radars.

India's Ballistic Missile Defence System

- The Indian Defence Research and Development Organisation (DRDO) is developing a two-tier Ballistic Missile Defence (BMD) system that provides a multi-layered shield against ballistic missile attacks.
- The two-tier system is intended to destroy an incoming missile, at a higher altitude, in the exo-atmosphere and if that miscarries, an endo-atmospheric interception will take place.
- It can intercept incoming missiles at exo-atmospheric altitudes of 150km and endo-atmospheric altitudes of 80km.
- The BMD system consists of a Prithvi Air Defence (PAD) missile and an Advanced Air Defence (AAD) Missile for high and low altitude interception.
- The PAD intercepts missiles at altitudes between 50km-80km and the AAD missile destroys them at altitudes of 15km-30km.
- DRDO plans to develop two new ballistic missiles, namely AD-1 and AD-2, in phase 2 of the missile shield development. The AD-1 and AD-2 interceptors can engage intermediate-range ballistic missiles (IRBMs) / intercontinental ballistic missiles (ICBMs).

PAD Ballistic Missile Interceptor

- PAD is a two stage missile based on the Prithvi missile. Also known as Pradyumna, PAD has a maximum interception altitude of 80km.
- The first stage is liquid fuelled and the second stage is solid fuelled.

AAD Ballistic Missile Interceptor:

AAD is a single stage solid rocket propelled guided missile. It can intercept incoming ballistic missile at altitudes of up to 30km.

Swordfish Radar

- Swordfish is a long-range tracking radar developed for the BMD system. It was derived from the Israeli Green Pine long range radar.

- Swordfish guides the exo-atmospheric interceptor missile PAD to engage aerial targets at altitudes over 80km. The radar can detect very small targets within the range of 600km-800km.

Smart Anti Airfield Weapon

In News

The Defence Research and Development Organisation (DRDO) has successfully tested indigenously developed light weight glide bomb Smart Anti Airfield Weapon (SAAW) dropped from an Indian Air Force (IAF) aircraft. Total of three tests with different release conditions and ranges were conducted at Chandan range near Pokhran in Rajasthan.

Smart Anti Airfield Weapon (SAAW)

- SAAW project is India's first fully indigenous anti-airfield weapon project sanctioned by Government in September 2013. It was indigenously developed by state-run Defence Research and Development Organisation (DRDO) in collaboration with IAF and the Research Centre Imarat (RCI). It will be inducted soon into the Armed Forces.
- SAAW is long-range lightweight high precision-guided anti-airfield weapon. It is 120 kg smart weapon capable of engaging ground targets with high precision up to range of 100 km. It is designed for deep penetration and is armed with high-explosive warhead, which is usually very difficult to achieve operationally with simple gravity bombs.
- It is meant to deal debilitating damage to ground infrastructure such as runways, taxi ways, aircraft hangars and bunkers among other things. Depending on operational requirements, it can also be used against other ground targets to give Indian forces enhanced area-denial capabilities, like taking out ground infrastructure.
- The guided bomb is considered to be one of the world-class weapons system. It is said to have higher precision and much cheaper compared with missiles. It can be integrated into varied types of multi role fighter jets of IAF such as MiG, Sukhoi Su-30 and ground attack SEPECAT Jaguar. It will enhance capability of IAF to easily hit targets across border without putting pilot and aircraft at risk.

Anti-airfield weapons

They are critical in war-like scenarios, since they help to give debilitating blow to adversarial air forces. These high-explosive warheads are meant to cause maximum damage possible to runways and other key infrastructure, in way that prevents quick repair. If successful, attack using such bombs render airfield useless, grounding all the war planes that are based at that air field.

Vertically Launched Short Range Missile Systems

In News

- Defence Acquisition Council (DAC) has approved procurement of 14 vertically launched Short Range Missile Systems.
- Of these, 10 systems will be indigenously developed and remaining four will be imported. These missile systems will help boost the self-defence capability of ships against anti-ship missiles.

- **DAC is Union Defence Ministry's highest decision making body on capital procurement** of Indian Armed Forces (Army, Navy and Air Force). It is **chaired by Defence Minister.**

About Vertically Launched Missile Systems (VLS)

- VLS is an advanced system for holding and firing missiles on mobile naval platforms, such as surface ships and submarines.
- Each **vertical launch system consists of a number of cells, which can hold one or more missiles** ready for firing.
- Typically, **each cell can hold number of different types of missiles, allowing ship flexibility** to load the best set for any given mission.

Helina Successfully Flight Tested

In News

- Indigenously developed helicopter launched anti-tank guided missile HELINA has been successfully flight tested from Army helicopter in the ranges of Pokhran. The weapon system has been tested for its full range.
- The missile is guided by an Infrared Imaging Seeker (IIR) operating in the Lock on Before Launch mode. It is one of the most advanced Anti-Tank Weapons in the world.
- The weapon system was integrated with live warhead and has destroyed the targets with high precision. The telemetry and tracking systems captured all the mission events.

Government Announces Regulations for Drones

In News

- The Union Minister of Civil Aviation Shri Suresh Prabhu has announced the Drone Regulations 1.0.
- These regulations will enable the safe, commercial usage of drones starting December 1, 2018.
- Going forward, the Drone Task Force under the chairmanship of the Minister of State Shri Jayant Sinha will provide draft recommendations for Drone Regulations 2.0. These regulations will examine the following issues:
  - Certification of safe and controlled operation of drone hardware and software,
  - Air space management through automated operations linked into overall airspace management framework,
  - Beyond visual-line-of-sight operations,
  - Contribution to establishing global standards,
  - Suggestions for modifications of existing Civil Aviation Requirements (CARs) and/or new CARs.

Key Features of Drone Regulations 1.0

- The drones are classified into five categories based on their maximum take-off weight: nano (up to 250 gm), micro (251 gm to two kg), mini (2 kg to 25 kg), small (25 kg to 150 kg) and large (greater than 150 kg).
- All Remotely Piloted Aircraft System (RPAS) except nano and those owned by NTRO, ARC and CIA are to be registered and issued with Unique Identification Number (UIN).
- Unmanned Aircraft Operator Permit (UAOP) shall be required for RPA operators except for nano RPAS operating below 50 ft., micro RPAS operating below 200 ft., and those owned by NTRO, ARC and Central Intelligence Agencies.
- The mandatory equipment required for operation of RPAS except nano category are (a) GNSS (GPS), (b) Return-To-Home (RTH), (c) Anti-collision light, (d) ID-Plate, (e) Flight controller with flight data logging capability, and (f) RF ID and SIM/ No-Permission No Take off (NPNT).
- As of now, RPAS to operate within visual line of sight (VLoS), during day time only, and upto maximum400 ft. altitude.
- For flying in controlled Airspace, filing of flight plan and obtaining Air Defence Clearance (ADC) /Flight Information Centre (FIC) number shall be necessary.
- Minimum manufacturing standards and training requirements of Remote Pilots of small and above categories of RPAS have been specified in the regulation.
- The regulation defines “No Drone Zones” around airports; near international border, Vijay Chowk in Delhi; State Secretariat Complex in State Capitals, strategic locations/vital and military installations.
- Operations of RPAS to be enabled through Digital Sky Platform. The RPAS operations will be based on NPNT (No Permission, No Take off).
- There will be different colour zones visible to the applicant while applying in the digital sky platform, viz, Red Zone: flying not permitted, Yellow Zone (controlled airspace): permission required before flying, andGreen Zone (uncontrolled airspace): automatic permission.

Defence India Startup Challenge

In News

- With a view to leverage defence-related startups and strengthen their collaboration with the defence forces — the Indian Army, Navy, and Air Force — Government has launched the Defence India Startup Challenge.
- A joint initiative of the Atal Innovation Mission, the Department of Industrial Policy and Promotion (DIPP), and the Defence Innovation Organisation (a ministry of defence initiative), the Defence India Startup Challenge is looking for startups to innovate in 11 categories.
- The 11 Defence India Startup Challenges are: 1. Individual protection system with built-in sensors 2. See-through armour 3. Carbon Fibre Winding (CFW) 4. Active Protection System (APS) 5. Secure hardware-based offline encrypt or device for graded security 6. Development of 4G/LTE-based tactical local area network 7. Development of advanced technology based desalination system (water purification) and bilge oily water separation system 8. Artificial intelligence in logistics and supply chain management 9. Remotely piloted airborne vehicles 10. Laser weaponry 11. Unmanned surface and underwater vehicles.
- A support framework kit named SPARK — Support for Prototype and Research Kickstart (in Defence) — has also been launched to enable startups to participate in the challenge.

- Under this framework, the Defence India Startup Challenge will call for proposals to address the specific technology needs of the Indian Defence Establishment.
- The incentive will be distributed through the Defence Innovation Organisation (DIO), a non-profit joint venture company, formed between public sector units (PSUs) Hindustan Aeronautics Limited (HAL) and Bharat Electronics Limited (BEL).