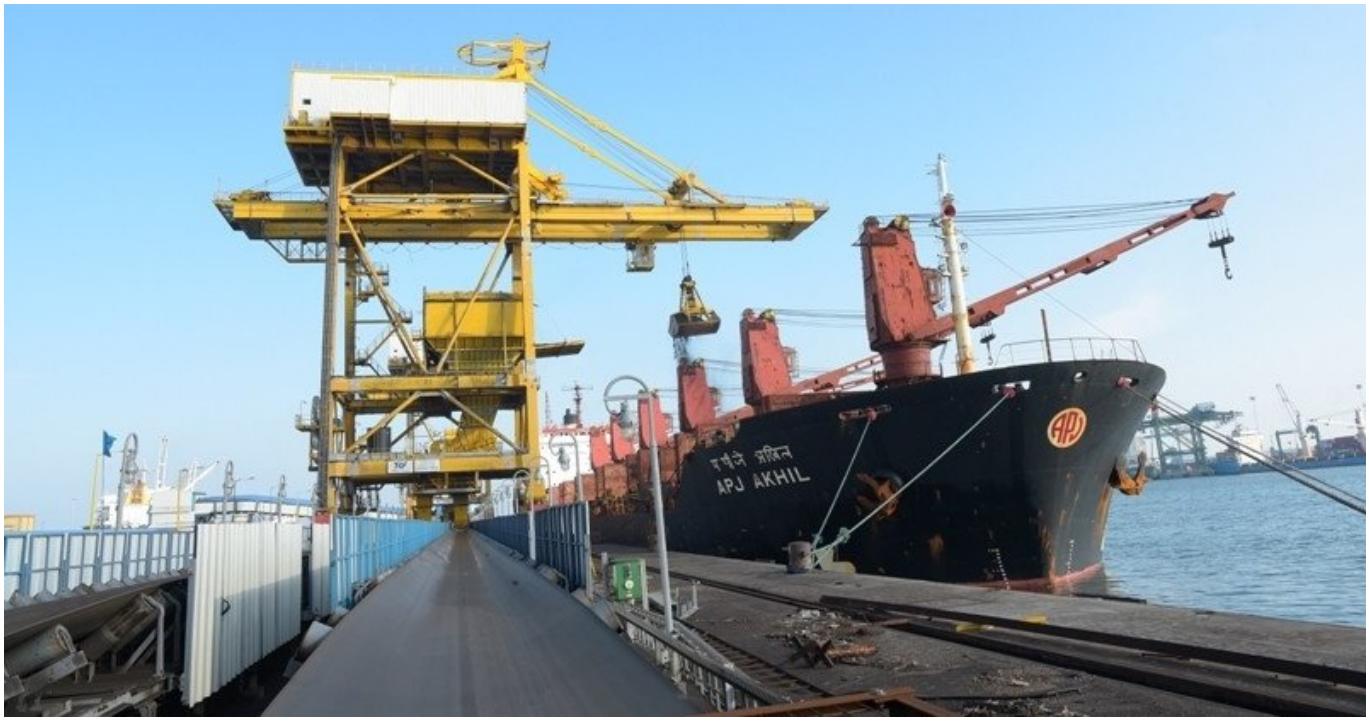
Who are the targets?

The biggest target is in terms of transportations, nuclear power plants, Power system Operation Corporation Limited, V.O. Chidambaram Port Trust, Telangana State Load Dispatch Centre, logistic industries and research organisations which eventually can lead to destruction of the whole ecosystem. The confidentiality breach in the case of medical data leak as reported by a German cyber security firm –Greenbone Sustainable Resilience wherein Picture Archiving and Communication Servers were linked to public internet without any requisite protection is a point of concern. Then, there are certain individualistic attacks such as hacking email and financial crimes (banking), etc. In the last two years the attacks radar of focus has been defence, government accounts and the vaccine manufacturing companies.



V.O. Chidambaram Port Trust. Image source: VOCPORT gov.in

Cyber Security – Individualistic awareness need of the hour:-

The target of the individual in a peculiar case which led to heinous crimes casted was due to opening of a document which was a bait to install Netwire- a malware. The bait was eventually delivered through a file and what prompted a person to open that link was a Drop box sent to him on his email was actually opening a Pandora Box of malicious command and control server. An emphasis to understand the technicality that Netwire stands for a

malware which gives control of the infected system to an attacker. This in turn paves way for data stealing, logging keystrokes and compromise passwords. In the similar vein the Pegasus used the tactic to infiltrate the user's phones in 2019.

Cyber Security – Attacking Power Distribution Systems:-

The intrusions by Chinese hacker groups in October, 2020 as brought out by Recorded Future was done through Shadow Pad which opens a secret path from target system to command and control servers. And, the main target is sectors such as transportation, telecommunication and energy .And , there are different tags that are being used by the Chinese Espionage Industry such as APT41, Wicked Spider and Wicked Panda , etc.

The institutions backing legitimisation:-

The Institutions which are at working under the cyber security surveillance are the National Security Council and National Information Board headed by National Security Adviser helping in framing India's cyber security policy .Then, in 2014 there is the National Critical Information Infrastructure Protection Centre under the National Technical Research Organisation mandating the protection of critical information infrastructure. And, in 2015 the National Cyber Security Coordinator advises the Prime Minister on strategic cyber security issues. In the case of nodal entity , India's Computer Emergency Response Team (CERT-in) is playing a crucial role under the Ministry of Electronics and Information Technology(MEITY).But, there is a requirement of clarity in National Cyber Security Policy of 2013 and the needed updates desired in it respectively.

Image source: HT

A cohesive approach – Data Protection and Privacy Importance:-

The Data privacy i.e. the personal data protection bill is an important imperative in which services of private actors can be bridged through a concerned law which is missing link in

that sense. The point of Data localisation falls squarely within this dimension of Section 40 and 41 of the draft bill where in the Indian stakeholders have the capacity to build their own data centres .In this contextualisation there also a need to understand certain technicalities involved in terms of edge computing which in a way is enabling the data to be analysed, processed, and transferred at the edge of a network. An elaboration to this is the data is analysed locally, closer to where it is stored, in real-time without delay. The Edge computing distributes processing, storage, and applications across a wide range of devices and data centres which make it difficult for any single disruption to take down the network. Since more data is being processed on local devices rather than transmitting it back to a central data centre, edge computing also reduces the amount of data actually at risk at any one time. Whereas on the other hand, there is insistence on data localisation has paved the way for companies such as Google Pay to adhere to the policy and synchronise their working with the United Payments Interface (UPI).

What do you understand by Data Share?

In the recent case of WhatsApp privacy issue and drawing in parallel other organisation a similar platform such as Facebook and Google shared the data to the third party with a lopsided agreement and with continuance of the data trade business industry. In 1996 the internet was free so was perceived as carte blanche , a safe harbour falling under the Section 230 of the Communication Decency Act in the United States but with the evolution of the circumstances the laws in that specifications are also required to change in that respect. In relations to the Indian law under the Information Technology Act, 2000 under the Section 69 the Indian government has the powers to monitor and decrypt any information that’s store in any computer resource but on certain conditions such as in regards to the sovereignty, defence and security of the country.


Image source: Getty

Cyber-attacks understanding on the International Forums :

In terms of Lieber Code of Conduct of 1863 or be it Hague Convention of 1899 there is a need of updating the definitions and where in the cyber army falling under the categorisation of civilians , not possessing any of the warfare weapons cause the main weapon that they possess is a malware which is invisible but can have deep repercussions leading to destruction of that particular economy altogether .So, in recent evolving circumstances there is an undue importance to for the target country to respond with equal force and having a right to self-defence in this manner regardless of the attack being from a non-state actor from a third country and masquerading under the civilian garb .Henceforth , there a thorough understanding of the complex environment that one is dealing with , there is undue emphasis to change and respectively update with the current world.

References:-

1. “NPCIL admits malware attack at Kudankulam Nuclear Power Plant”, *The Hindu*, October 31, 2019, https://www.thehindu.com/news/national/npcil-acknowledges-computer-breach-at-kudankulam-nuclear-power-plant/article29834644.ece

2. M.K.Narayanan, “Forestalling a cyber-Pearl Harbour”, *The Hindu*, March 15,2021, https://www.thehindu.com/opinion/lead/forestalling-a-cyber-pearl-harbour/article34068669.ece

3.Amar Patnaik and Bipul Chatterjee**, “**Data localisation: roadblocks and the way forward”, *The New Indian Express*, June 29, 2020, https://www.newindianexpress.com/opinions/2020/jun/29/data-localisation-roadblocks-and-the-way-forward-2162742.html

4. Lucas Roh, “The Forbes-Cloud Computing Vs. Edge Computing: Friends Or Foes?” *The Forbes,* March 5, 2020, https://www.forbes.com/sites/forbestechcouncil/2020/03/05/cloud-computing-vs-edge-computing-friends-or-foes/?sh=32587c6c66ee

5. Siddharth Sonkar, “Privacy Delayed Is Privacy Denied”, *the wire*, https://thewire.in/tech/data-protection-law-india-right-to-privacy

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team