

# **The Need for India's National Cyber Security Strategy**

**By Kanishk Gaur, Director, Ernst & Young**

## Abstract

In this Paper I emphasize the need to create a national cyber security strategy which could benefit the Indian government departments, Businesses, Academia and Citizens. A strategy that recognizes India as a Sovereign Cyber State protecting its economic, democratic interest and working towards strengthening its economy through reforms like Digitization, Unified Taxation, Divestment of public sectors units and merging of public sector banks.

The Cyber Strategy would work towards making the cyberspace secure and resilient for its citizens, businesses and government.

The cyber strategy will enable different government departments to implement the national cyber security policy to meet their organization's objectives, need and build up cyber security competence to support the organizations goal.

A complex cyber security structure and lack of central leadership for cyber security makes it difficult for India to manage security of national information and communication infrastructure, assure citizen of safety & security of Digital India [8] programs, manage cyber-crime in the country and respond to cyber incidents originating from hacktivists, state and state sponsored actors. The complex structure also makes it difficult for India to engage with International community on cyber dialogue with more government departments under Ministry of Home Affairs, Ministry of External Affairs, Ministry of Defence getting approval to run and manage cyber security situation worsens as funding situation worsens as no single state actor has complete ownership of cyber operations and also look after cybercrimes impacting its citizens.

As more government organizations turn to boutique private cyber security firms in India to carry complex cyber operations on their behalf, an unthoughtful and unprovoked cyber offensive targeting critical infrastructure of neighbour states could push India towards complex relationship with its neighbours.

As India races towards digitization of its economy through key programs enabling digital payments, adoptions of internet governance schemes, digital identity based authentication through UIDAI (AADHAAR) [5] for its citizens to access key lifeline enabling services (Banking, Communication, Healthcare, Transport, Power supply) makes it mandatory for India to protect its cyber space from cyber-attacks and more importantly maintain cyber peace with its neighbour states.

It's important that India maintains a single cyber strategy which is sovereign, in line with its government's internal, foreign policy and also respects the sovereignty of its neighbours.

**Keywords:** - Cyber Security Strategy, Critical Infrastructure Protection, Cyber Dialogue, Digital Economy, Digital Payments.

## Organization of Paper

The paper first describes the current situation in India highlighting the key reforms the government has taken. It introduces government programs like Digital India [8], Make in India [9], Digital Payments, Digital Locker [2], UIDAI (AADHAAR) is the world's largest biometric ID system, Smart City program and then Indian good and services network establishment (GSTN).

The paper then next deep dives on the impact of these key government reforms i.e. how it transforms India to a digital economy with increase in no. of internet users and huge rise in digital transaction happening through electronic platforms.

Post which I cover Cyber Security issues arising out of rapid digitization and highlight some of the key cyber issues current programs face due to lack of national cyber security strategy

After this I cover the current security structure in India, how cyber security is aligned with it, and current complexity in managing cyber security operations in India with such a structure.

## Current Situation and Structure

This section explains the current situation in India i.e. how the BJP led national democratic alliance since leading majority in the Sixteenth Lok Sabha Election (2014-19) has led massive reforms like Digital India [8], Make in India [9], Digital Payments, GST roll, Digital Locker [2], UIDAI (AADHAAR), Smart Cities Mission, roll out of Public Wi-Fi schemes. It also explains the current security structure in India, how cyber security links to national security and various government agencies, departments involved in managing cyber security operations for India.

## Massive reforms launched by current government of India led by B.J.P National Democratic Alliance

Source: Created by author based on basis review of government of India websites and interaction with senior leaders in Indian government department on structure and process.

### i. Digital India [8]

The Digital India [8] campaign by the Government of India was designed to improve the digital literacy of the country and make India more technologically empowered especially targeting the rural areas.

### ii. Make in India [9]

The Make in India [9] Initiative was launched by the Government of India for 25 different economic sectors to transcend Indian business communities and entrepreneurs for transforming India into a global design and manufacturing hub for stimulating potential investors and partners around the globe.

### iii. Digital Payments

As the part of Digital India [8] campaign, the government of India has been promoting and encouraging digital mode of payment to transform India into a cashless economy.

iv. Digital Locker [2]

The Government of India has now provided “Digi Locker” or Digital Locker [2] that serves as an online repository for Indian citizens to store their official documents on the cloud to push the agenda of Paperless administration as a part of Digital India [8].

v. Unique Identification Authority of India (UIDAI) also known as AADHAAR

UIDAI (AADHAAR) [5] is a statutory authority established by the Government of India responsible for implementing the AADHAAR scheme which has established itself as the world’s largest biometric system. AADHAAR is a 12-digit unique ID that can be availed by Indian citizens based on their biometric and demographic data.

vi. Smart Cities Program

Smart Cities Mission [12] is an urban development program by the Government of India with a mission to make 100 cities effectively sustainable by providing them cutting-edge infrastructure and increase their socio-economic growth.

vii. The Goods and Service Tax Network (GSTN)

The Goods and Service Tax Network (or GSTN) or GST portal serves as channel to support services for GST (Goods and Services Tax), a unified multi-stage indirect tax levied by government of India

viii. Public Wi-Fi on Airport, Railway stations.

Governments plans to enable free Public Wi-Fi to Indian Citizens on all airports and railway station so more people can access digital services, however government plans to secure these Wi-Fi networks nationally remains an aspect yet to be addressed.

### Impact of key government reforms

A detailed description on how key government reforms have impacted India as a country through rapid increase in no. of mobile phone, internet users, massive digital transaction.

I look at how this translates to a trillion-dollar opportunity for the technology industry in India and what could be future growth aspects for India’s Digital ascent.

### Digital Transformation reforms have poised India to be world’s fastest growing economy-

Rapid digitization pushed by government in India has also got the Indian enterprise supporting it. The Indian Internet Service and Telecom Service, Banks have also pushed

digitalization in their services as well with like of Reliance Jio, Airtel and Vodafone focusing on data backed services instead of voice segment. However, it still lacks a cyber-strategy to protect and make it resilient.

### Large volume and value digital transaction through electronic platforms

1. The volume and value of transaction happening through electronic platforms has significantly increased in India. There has been financial security measure imposed by government to secure electronic platforms issued by National Payments Corporation of India (**NPCI**) of India) and Reserve Bank of India however there seems to lack a common national strategy which would work towards securing digital transaction in the country and build confidence of consumers towards adopting newer payment mechanism.

### Rapid increase in internet users in India

Post demonetization and launch of Digital India [8] program there has been a rapid surge in the no. of internet users in India. While the government declared that there will be separate CERT (Computer Emergency Response Team) for financial institution called Fin-Cert, there still lack of clarity on how Fin-cert will coordinate its work with existing cyber security organization in the country.

### A Trillion Dollar Opportunity for the Technology Industry

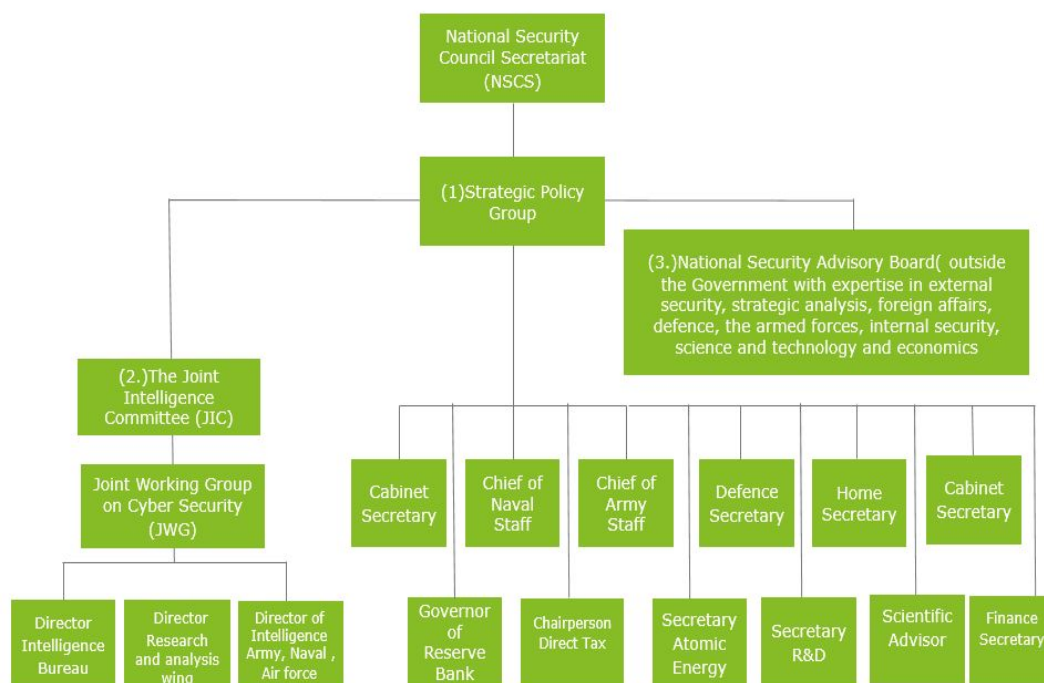
The key reforms launched by government of India have created a trillion-dollar opportunity for technology industry in the country and opportunity for Indian youth to take up more jobs in the Indian IT Sector which is focused towards enabling below mentioned programs.

### India's Digital Ascent Future Projections-

As per Boston Consulting Group report India is expected to have 442 million smart phone users. The total no. of internet users is expected to be 730 million by 2022 with 129 Million Indians utilizing Digital Locker [2] services while financial transacting more than 15 billion dollars in e-KYC transactions. With such large growth projected for Digital transaction and internet users I will need a cyber-security strategy at national level strategy which is reviewed periodically to support the growth of Digital Economy.

## Current security structure in India

Indian Current National Security Governance Structure is shown in the below mentioned figure, illustrates various governments who have specific remittance in cyber security. This is based on author's interactions with various government departments. The hierarchy also indicates reporting lines of leadership in Ministry of Defense, Ministry of External Affairs,



Source: Created by author based on government of India websites and interaction with senior leaders in Indian government department on structure and process.

The National Security Council Secretariat (NSCS) (Rāṣṭrīya Surakṣā Pariṣada) of India is an executive government agency tasked with advising the Prime Minister's Office on matters of national security and strategic interest. It was setup under the Atal Bihari Vajpayee government on 19 November 1998, with Brajesh Mishra as the first National Security Adviser. Prior to the formation of the NSC, these activities were overseen by the Principal Secretary to the Prime Minister.

The National Security Council Secretariat (NSCS) is the apex body with a three-tiered structure of the national security management system in India. The two tiers are the Strategic Policy Group, and the National Security Advisory Board.[2]

### *Strategic Policy Group*

The Strategic Policy Group is the first level of the three tier structure of the National Security Council. It forms the nucleus of the decision-making apparatus of the NSC. Cabinet Secretary is the chairman of the group and it consists of the following members:

- Cabinet Secretary
- Chief of the Army Staff , Naval Staff ,Air Staff
- Governor of the Reserve Bank of India (RBI)
- Defence Secretary
- Foreign Secretary
- Home Secretary
- Finance Secretary and Secretary
- Secretary (Defence Production)
- Secretary (R) (i.e. the head of the Research and Analysis Wing)
- Secretary (Atomic Energy)
- Secretary (Department of Space)
- Chairman of the Joint Intelligence Committee
- Chairperson, Central Board of Direct Taxes
- Director of the Intelligence Bureau
- Scientific Advisor to the Defence Minister

The Strategic Policy Group undertakes the Strategic Defence Review, a blueprint of short and long term security threats, as well as possible policy options on a priority basis. So far Cyber Security threats are not mapped at Strategic Level or as part of short and long term threats.

#### *Joint Intelligence Committee*

The Joint Intelligence Committee (JIC) of the Government of India analyses intelligence data from the Intelligence Bureau, Research and Analysis Wing and the Directorates of Military, Naval and Air Intelligence. The JIC has its own Secretariat that works under the Secretariat. Cyber Security is part of Joint Intelligence Committee with each agency contributing individually through its cyber intelligence

#### *National Security Advisory Board*

The National Security Advisory Board consists of persons of eminence outside the Government with expertise in external security, strategic analysis, foreign affairs, defence, the armed forces, internal security, science and technology and economics.

### **1. Complexity in Indian Cyber Security Organization Management Structure -**

For the past one decade managing security of cyberspace has been tasked to multiple agencies, several ministries, departments and even non-government organizations (NGO), with lack of clear role, understanding responsibility and mandate for cyber affairs for the

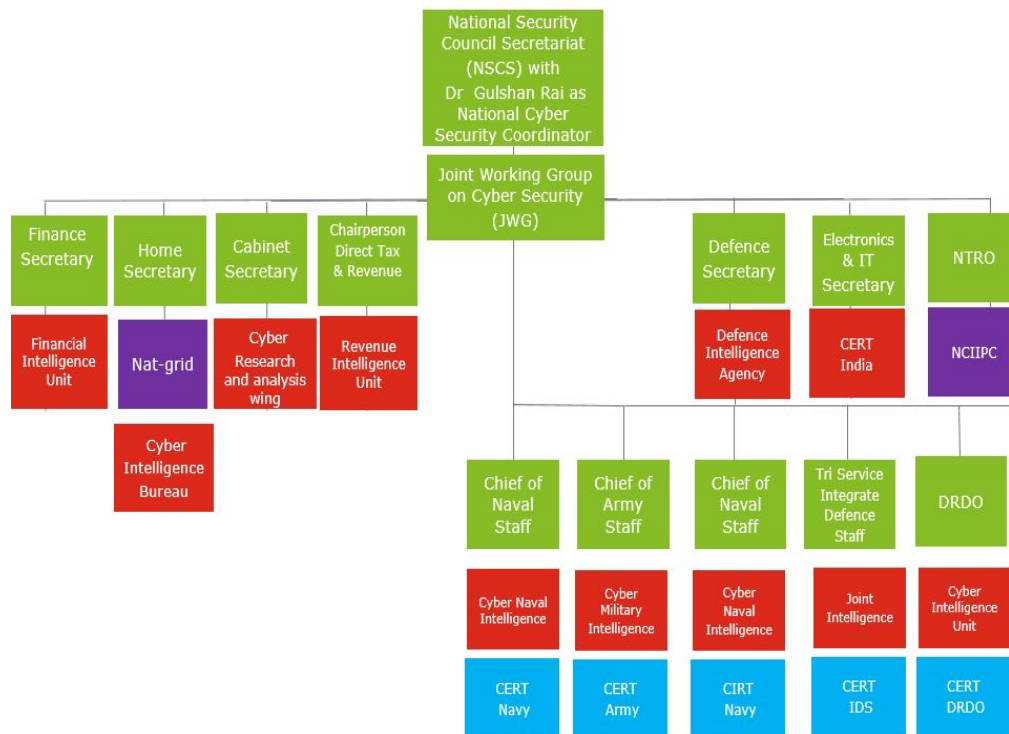
country, hence making consistent government-wide action a challenge. The below mentioned table depicts all recognized agencies involved in cyber security.

India – Cyber Organisation					
PM Office/ Cabinet Secy (PMO/ Cab Sec)	Ministry of Home Affairs(MHA)	Ministry of External Affairs (MEA)	Ministry of Defence (MOD)	Ministry of Common Info Technology (MCIT)	Non Govt Organisation (NGO)
National Security Council (NSC)	National Cyber Coordn Centre (NCCC)	Country Ministers and Ambassador	Tri Service Cyber Command - Pending Operationalisation	Department of Information Technology (DIT)	Cyber Security and Anti hacking Organisation (CSAHO)
National Technical Research Orgn (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecommn (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre(NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (DNI)	Indian Computer Emergency Response Team CERT-IN	Centre of Excellence for Cyber Security Research & Development In India (CECSRDI)
Joint Intelligence Group (JIG)	Central Forensic Science Lab (CFSLs)		Air Force (AFI)	Education Research Network (ERNET)	Cyber Security of India(CSI)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research and Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center (MAC)			Defence Research Dev Authority (DRDO)	Standardisation, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

Source: Created by Author based on review of government of India websites

- Appointment of Lt. Gen Rajesh Pant as National Cyber Security Coordinator and member of National Security Council Secretariat** – Lt. Gen Rajesh Pant has been appointed the National Cyber Security Coordinator appointed by the current Government to combat the increasing cyber-attacks and secure the digital assets of the country. This move by the PMO was necessary as an authority was needed to control the accelerating cyber security incidents impacting India. However there still no national cyber security strategy in place to govern cyber security.

## Indian Cyber Security Governance Structure



	Offensive Capability
	Defensive Capability
	Combined offensive, defensive capability

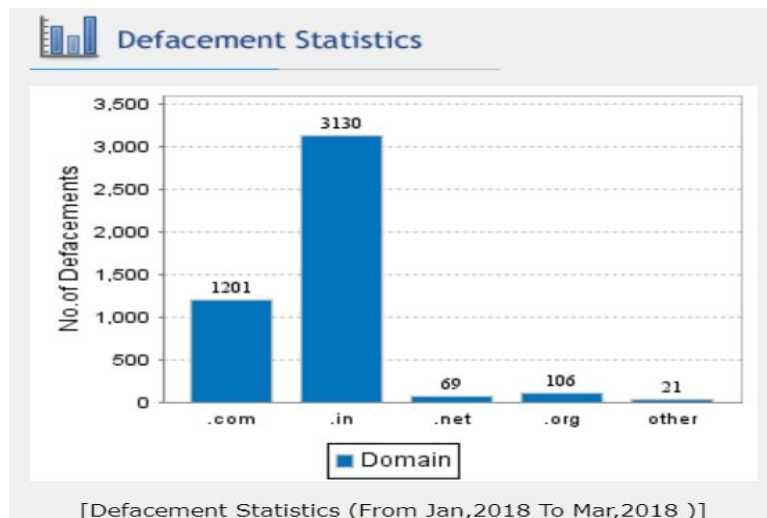
Source: Created by Author basis review of Indian govt. websites.

**No national cyber-crime agency appointed in India** -Indian government has been spending a lion's share of its resources in dealing localized cybercrime in response to the major attacks with a case-by-case approach. It needs to set bigger objectives to eliminate the root cause and also do offensive counter attacks when it is required.

### 3. The Indian Computer Emergency Response Team (CERT-In)

CERT India acts as the nodal agency for all cyber security emergencies with full functionality. Ever after securing India's cyberspace, the NCSP still cannot counter current cyber threats because of a less detailed and flexible approach, which is neither binding nor enforceable. The policies can be easily amended by the organizations according to their requirements which can pose as major threat.





Source – Cert India website

4. Key reforms pushed by government to India did not take into account cyber security as key fundamental in them, hence none of them had security by design built in them.

#### 1. Limitations with current structure

Lack of national level strategy from the government to address cyber security challenges creates mode hurdles to address threats and vulnerabilities impacting India's economy.

Lack of greater cyber security strategy at national level guiding sectoral regulators in different sector i.e. RBI in Banking, NCIIPC in Critical Infrastructure, SEBI Indian Stock Exchange, and DOT/TRAI in Telecom will increase financial risk, frauds and hamper confidence of Indian consumers toward adopting digital transaction media.

India today faces massive cyber security threats from its neighbors and has been under continuous cyber-attacks originating from outside its territorial boundary. Hacktivists groups like Anonymous have also been involved in targeting Indian National Critical Information Infrastructure attacking large Indian Telecom service providers and Indian National Public Sector Banks.

The loosely adopted and executed Indian IT Act 2008 only pushes case strongly for a greater national cyber security strategy coupled with stronger enforceable Information Technology laws.

#### 2. Current Cyber Security Policies in India

Multiple cyber security policies operating in one country as times confuses Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing Information Communication

Technology operations. Hence there is a need for single national cyber security strategy which guides implementation of cyber security policy for various government departments and enterprise clients.

#### **a) Indian National Cyber Security Policy**

The National cyber security policy 2013 was built with a vision to build a secure and resilient cyberspace for citizens, businesses and Government for tackling online radicalisation and cyber terrorism. The NCSP consists of an architecture for the data and information protection in cyberspace with greater emphasis on R&D of indigenous cyber security technology, and their effective testing and deployment. It aimed at encouraging public and private organizations to adopt IT policies in pace with the international standards. It has a vision to employ 500,000 cyber specialists in the next five years and perform various training programs. Auxiliary services like the protection of private information in process, transit and storage; the creation of a well-defined legislative framework to deal with criminal investigations and prosecution; and the promotion of individual responsibility in dealing with cyber security also find a mention in the policy.

#### **b) NCIIPC Cyber Security Guidelines**

National Cyber Security Policy an organization of the Government of India under National Technical Research Organization created under Sec 70A [1] of the Information Technology Act, 2000 (amended 2008), Based in New Delhi, India, was designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection – In 2013 It came up with its own Cyber Security guidelines which it enforced to following 6 sectors identified by it as critical for functioning of Indian democracy and essential for safety, security of Indian Citizens ( Banking, Insurance, Energy, Power, Transport , Sensitive Government Organization, Telecom, identified by it . More than 900 organization in government and private sector were asked to comply with cyber security guidelines.

- 1) Power & Energy
- 2) Banking, Financial Services & Insurance
- 3) Telecom
- 4) Transport
- 5) Government
- 6) Strategic & Public Enterprises

### **3. Current Cyber Security guidelines and regulations in India**

In India with no central governance structure for cyber security and no national level cyber security strategy multiple government departments and agencies have issued cyber

security guidelines which other government departments and enterprise companies operating in India need to ensure compliance. Lot of precious time of these government departments and private enterprise businesses goes as implementing multiple cyber security guidelines, carrying out internal / external audit to take of this compliance and manage of regulatory affairs of reporting to government. If there was one overall national cyber security agency issued cyber security guidelines against which compliance was to be maintained, lot of precious time could have been invested to improve cyber security posture of government departments and enterprise clients and make them resilient cyber-attacks.

#### **a) Department of Telecom (DOT) Network Security Policy**

Department of Telecommunications (DoT) under the Ministry of Communications and Information Technology, Government of India, set up a Cyber Security (CS) Division to abide by the guidelines issued by CERT-In, This department is responsible for maintaining telecom network security during cyber incidents. The division maintains security activities for ICT network, in accordance with the security indexing guidelines for critical equipment as recommended by ITU-T and security audit guidelines as per ISO 27001. The department reports the security threats to the relative government agencies including the Indian Computer Emergency Response Team (CERT), telecom sectoral CERT and National Cyber Coordination Centre (NCCC) that also monitor their traffic. The DOT came up with its own cyber security policy which it enforced on Telecom Service Providers in India. DOT believes that it needs a separate security policy apart from the National Cyber Security Policy to deal with the critical issues in the information infrastructure.

#### **b) Reserve Bank of India (RBI) Cyber Security Guidelines**

The Reserve Bank of India also issued its own cyber security guidelines for banks as Information Security incidents began to disrupt banking operations. The RBI Cyber Security policy mandates the bank to have a resilient cyber security framework for continuous protection from threats, frauds and vulnerabilities. This mandates that the bank create their own Cyber Security policy and get it approved Cell of Department of Banking Supervision (CSITE), Reserve Bank of India on the basis of the relative checklists for the defined risks with associated parameters. The cyber security guideline also mandates that IT infrastructure should be evaluated against with the security parameters laid out by RBI guidelines to ensure banks network and database are secure. A Cyber Crisis Management Plan (CCMP) also needs to be created which needs to be approved by the banks board. It also mandates that awareness amongst the top management and stakeholders in the bank is ensured for a cyber- safe environment. Banks are encouraged to report the cyber incidents with the RBI for risk analysis and recovery.

### **c) Insurance Regulatory and Development Authority (IRDA) Cyber Security Guidelines**

The Insurance Regulatory and Development Authority also known as IRDA came up with its own cyber security guidelines which it maintained to all insurance companies operating in India. The guidelines mandate appointment of a qualified and experienced Chief Information Security Officer (CISO) who will be responsible to draft and enforce the cyber security policies to protect their information assets and the formation of Information Security Committee (ISC). The entire process involves identification of threats and vulnerabilities, formation of a Cyber Crisis Management Plan and formulation of Information and Cyber Security assurance programme has to be in accordance with the Information and Cyber security policy. The board of the insurance company needs to timely review organization's Information and Cyber Security policy and get external audit carried out by independent auditors.

### **d) Ministry of Home Affairs (MHA) Cyber Security Guidelines**

The Ministry of Home Affairs (MHA) also came up with its full-fledged National information Security Policy and Guidelines which were issued by the (C&IS) division to ensure cyber security is well managed within department of MHA. The MHA cyber security guidelines mandate each department to setup four wings namely, Cyber Security Wing, Cyber Crime Wing, Information Security (CSIO) wing and Security clearance wing. Each wing is expected to be headed by an Under Secretary level officer. The main motive of MHA issuing these guidelines is to ensure MHA agencies and department following certain best practises in awake new of cyber security incidents impacting them.

### **e) Ministry of Electronics and Information Technology (MEITY) guidelines for Chief Information Security Officer's (CISO) and 8 best Practices for a Safe & Secure Cyber Environment**

Ministry of Electronics and Information Technology (MEITY) [22] on 19th May 2017 issued guidelines highlighting key roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations. On 11th April 2018th followed these guidelines by issuing 8 best practises for Chief Information Security Officers (CISOs) for promoting a safe & secure cyber environment.

## **4. Threat Actors**

- I. **State and State Sponsored Attackers** - India information communication technology infrastructure has long been attacked by its neighbor states
- II. **Organized Hacking Group** – Hacking groups with aim of causing defacement and disruption of national critical infrastructure attack India.

This includes groups like anonymous which have attacked Indian ISP's multiple times

- III. **Cyber Criminals** – Cyber criminals with an aim to make money find vulnerabilities and exploit them digital system, insecure software used by banks, payment gateways and telecom service providers.
- IV. **Cyber Terrorist** – Often linked to terrorist groups cyber groups backed by global terrorist outfits like DAESH, Al-Qaeda, Jaish-e-Mohammed and Lashkar-e-Taiba have often used defaced Indian Sites to gain media traction
- V. **Script Kiddies** - They attack because they seek attention of media and find naïve users on the Internet who are less aware about security and are vulnerable due to non -updated systems.

i. **Key reforms**

Partnership agreement in the 5th Global Conference on Cyber Space held in India last year – The government of India and U.K pledged to work towards a safe, secure and inclusive Cyberspace for sustainable development. GCCS

India and U.K also agreed to work on a common Framework for the UK-India Cyber relationship that would articulate common commitment to maintaining the increasing economic and social benefits enabled by a free, open peaceful and secure cyberspace.

ii. **International engagement/standing**

India has been a long member of the commonwealth group and continues to support commonwealth standing on cyber security

Apart from commonwealth India is also a member of United Nations and has been supporting United Nations charter on cyber security and peace

## **Current threats and risks**

A detailed analysis of the current threats and risk looming over Indian Digital dream, how they impact India's consumers, enterprises and makes government programs vulnerable to cyber-attacks. Threat Landscape impacting India and who are the threat actors behind these risk? A case study on "Hypothetical situation of multiple cyber security agencies in India targeting the same threat actor and its impactation".

### India's complex Cyber Security problem

Poised to be the fastest growing economy in the world today a look at how India has missed on cyber security aspects of its key reforms most recently. A perspective on India's growing cyber security concerns impacting its citizen's, business house and government. As result of massive digitization and reforms which have been launched not in line with a national cyber security.

### Cyber Security threats to government enabled Smart City Program

Major programs like smart city are under threat due to lack of progress made on national cyber strategy. The national cyber security policy came in 2013 post which the smart city program has been launched which will have a major dependence on IOT devices and security of IOT devices will be a major concern in India. But neither the national cyber security policy has been updated since 2013 nor a national level strategy which addresses security of new age technologies like IOT being made to handle emerging threats.

### Rise of client side attack on Digital platforms of UIDAI (AADHAAR)

Increasing maturity and robustness of perimeter controls coupled with not-so-defensive internal network topology are leading to rise of client side attacks on digital platforms which have not been created to include security by design.

Below mentioned case study highlights major security weaknesses in the current structure of AADHAAR [5] and creating review of the current ecosystem.

### Current Threat Landscape impacting India

1. **The fragile software** used in key government program like UIDAI (AADHAAR) [5], Digital India [8], GSTN were not strategizing to include security by design in them, hence exposing them to inherent risks

**Mix of open source and commercial software application makes system vulnerable-** Often user workstations in Indian enterprise and government departments are characterized by richer mix of applications (targets), relatively lax patch management, less stringent protection /detection mechanisms hence these have better success rate for payload obfuscation mechanisms.

### **Lack of Antivirus on computer systems and enforcement of patch management policies**

-Client side attacks often serve as a conduit for reaching the internal server landscape of enterprises and government controlled computer system. Hackers often target Microsoft Office Suite, Adobe Acrobat Reader, Adobe Flash and web browsers (as well as their add-ons / plug-ins).

**Phishing and Social Engineering as means for targeted attacks:** Today attackers use phishing and social engineering technique to obscure user to click malicious links and launch targeted attack. One of the primary means of such targeted attacks is Information centricity rather than technological asset centricity which is vector favored for Advanced Persistent Threats and ransomware attack by hackers

## **2. Advanced Persistent Threats impacting India**

- APT's Characterizes the attacker with Hostile Intent, Capabilities to launch targeted stealth attacks on the user which have increased likelihood of attacks succeeding. India has been a long target of APT based attacks be it Ghost net based attacks launched against it by the Chinese
- Targets assets that may have significant long-term strategic value are compromised through network of Well-funded, persistent and sophisticated attackers.
- APT target people and processes as much as they target technology
- APT based Cyber-attacks are aimed to promote political ends or increased theft of Personally Identifiable Information (PII)
- Non-opportunistic nature of attacks implies relative security posture does not influence an organization's chances of survival
- Greater payoffs from auditing / monitoring mechanisms aimed at detection than excessive investments aimed at prevention
- Although often associated with state agencies (Stunt), high profile enterprises are targets too
- Techniques range from leveraging zero-day exploits through social engineering to compromising apparently unrelated enterprises in an attempt to gain unauthorized access to targets
- Leverage Client-Side exploits to target the internal assets of the ultimate target organization
- While the ultimate target organizations may be governments, defense contractors or financial institutions, enabling companies (such as technology firms) may be the intermediate targets (used to eventually attack the ultimate targets)

## **3. Maturing Zero-Day Marketplace**

- Traditionally, disclosure has been the norm although underlying motives evolved as the community moved from full disclosure to responsible disclosure
- Responsible security disclosure => Patches for vulnerabilities going public + Bad name driving secure software development initiatives –

Also cost of proactively addressing flaws significantly lower compared to reactive actions

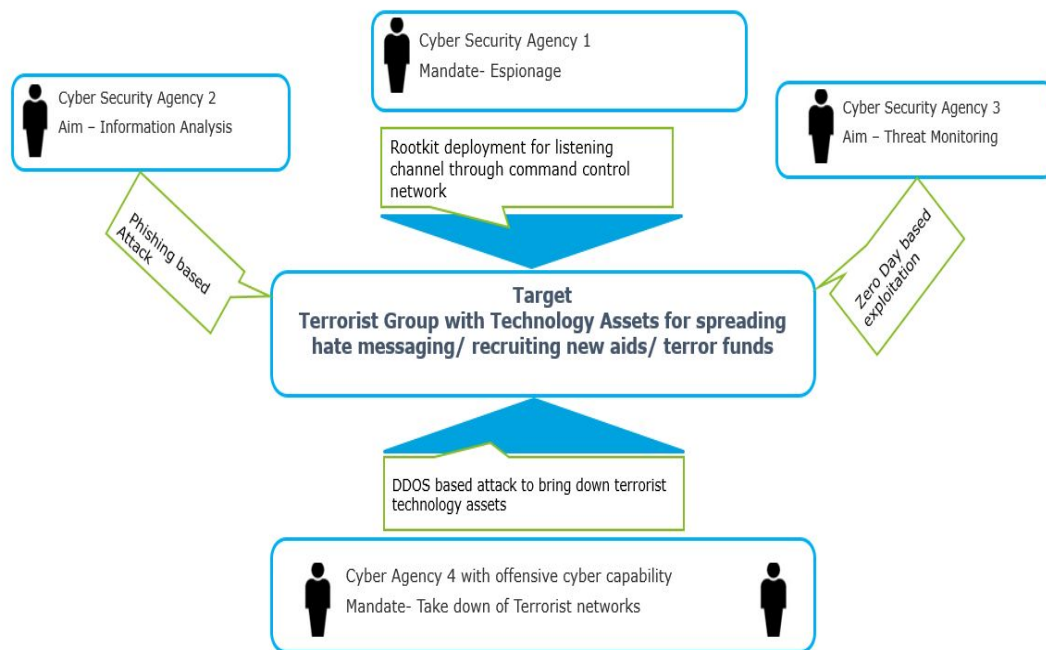
- Increasingly, software companies, governments and large defense contractors have demonstrated interest in buying 0-day with the intention of keeping them secret and exploit them (See typical price list for exploits)
- Maturing marketplace is dangerous – Vulnerabilities remain secret / unpatched, responsible disclosures may shrink, programmers may turn unethical
- Issue compounded by lack of security measures built into SDLC to detect and prove mal-intent.
- Exclusive sale, the most modern version of the software in which vendor not alerted.
- Top Sellers include: Vupen, Endgame, Netragard, Northrop Grumman, Raytheon
- Buyers: Hacktivists, States and State Sponsored agencies

#### **4. Unaware users of information system**

Today most of the users of digital platforms in India are unaware about best practices of information security. Due to such lack of awareness of most of government department USB/Hard drives are openly used by workforce on workstation for transferring data from their personal computer to workstation and vice versa. Hence Drive-by infections is on the rise followed by the establishment of a Command & Control Channels. Furthermore, bar has lowered for successful client-side attacks as exploitation tools and frameworks have matured. Open end devices with little or no end security mechanism built makes enforceable end security policy in place makes these systems vulnerable to cyber-attacks.



## Case study on “Hypothetical situation of multiple cyber security agencies in India targeting the same threat actor and its impact”.



In the above-mentioned case we have multiple cyber security agencies with different aims and mandate going after same target without cooperation and intelligence sharing above themselves.

### Target Group

Target is a global terrorist organization with technology assets spread on internet which conduct hate messaging and use social media to recruit and brain wash youth. The target also runs a terror fund network through crypto currencies.

### Complexity in Cyber operations

Given the nature of operations multiple organization are interested in going after this target setup.

However due to lack of coordinated effort and information sharing among different agencies. Operations of Agency 4 impacts operations of rest of three agencies who have their own objective and goals.

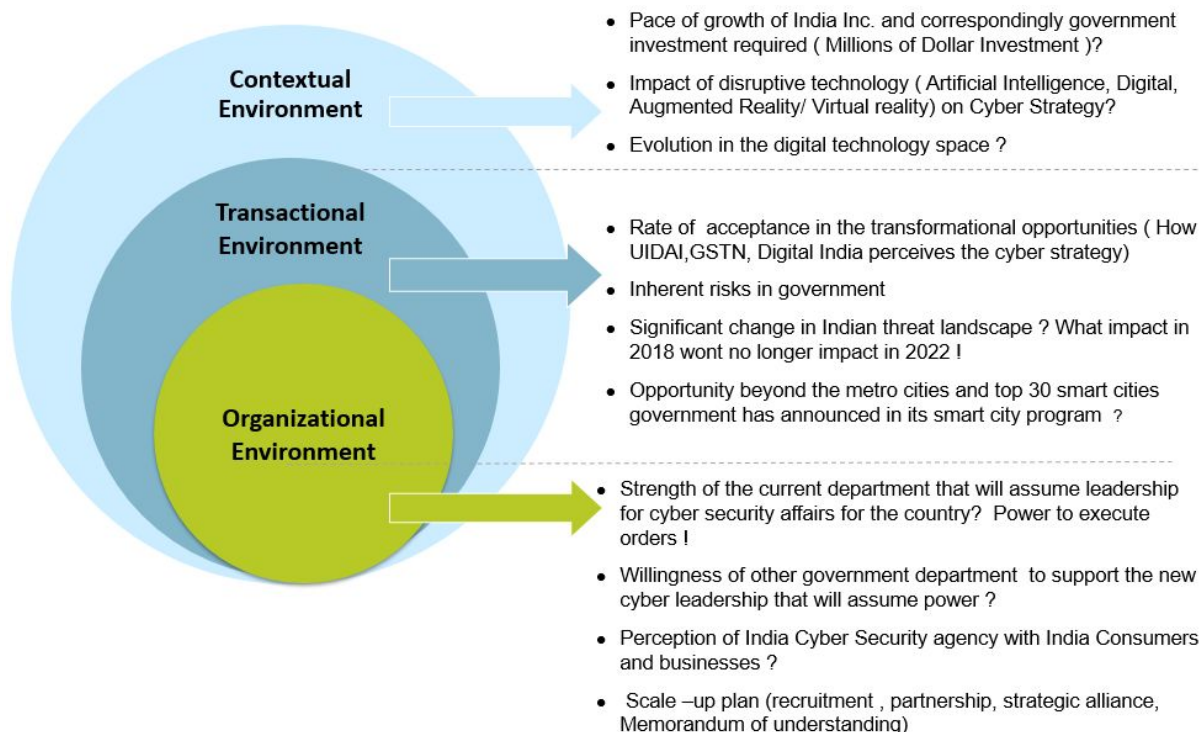
### Solution

A national level cyber security strategy will prevent cross fire between agencies and help them coordinate effort for achieving mandate. A national level cyber strategy would also enable organization to share valuable

information and use cyber warfare as assets of the country to their advantage and build long term strategic capability for cyberwarfare.

## 5. Need for National Cyber Security Strategy

Given the current situation in India with many reforms shaping the future of the country a national level cyber strategy supporting successful enablement of these programs is need of the hour. A centralized leadership to govern this cyber strategy is also needed to ensure its successful implementation of this strategy along with government's flagship programs like Digital India [8], Make in India [9], UIDAI (AADHAAR) [5], and Good and Services Tax Network (GSTN).



## Challenges of developing a National cyber security strategy

A strategy has not meaning if there is no strong team to supports its implementation, hence a cyber-security leadership department must be formed in India with constitutional authority to drive change management and executive orders for cyber strategy implementation.

Hence there are some key assumptions listed below that must be tested while preparing India Cyber Security Strategy.

**Contextual Environment** – Situational factors applicable to the current problem that must be addressed and taken into consideration. Macro-economic variables i.e. Current situation, cost of setup, investment required, return on investment. Another important aspect is to consider factors that could disrupt current situation or lead drastic change in current macro-economic variables.

- Pace of growth of India Inc. and correspondingly government investment required to support Cyber Security Strategy (Million Dollar Problem)?
- Impact of disruptive technology (Artificial Intelligence, Digital, Augmented Reality/ Virtual reality) on Cyber Strategy?
- Significant change in Indian threat landscape? What impact in 2018 won't no longer impact in 2022!
- Evolution in the digital technology space? As machine learning and artificial intelligence take over work of humans, a strategy must be prepared keeping in the evolving digital technology trends

**Transactional Environment**- Refer to of variable that contribute to transactional analysis i.e. brand image of government, internal support of key government programs, consume and business perception of government.

- Rate of acceptance in the transformational opportunities (How UIDAI (AADHAAR), GSTN, Digital India [8] perceives the cyber strategy) Do they see cyber strategy an enabler or show stopper?
- Inherent risks in government image t (e.g. declining public perception, image of govt. among citizens and businesses due to some recent policies like demonetization and centralized tax policy i.e. GSTN)?
- Opportunity beyond the top 30 cities in India? Strategy must address to the common man of India which is beyond the metro cities and 30 Smart Cities announced by government so far.
- Perception of India Cyber Security Agency leading cyber strategy with Indian Consumers and businesses?

**Organization Environment** – Refers to how the new government department assumes leadership and how much power the current government assigns it. The

- Strength of the current department that will assume leadership for cyber security affairs for the country? Power to execute orders!
- Willingness of other government to support the new cyber leadership that will assume power? Support from MHA, MEA, MOD, MEITY?
- Scale –up plan (recruitment, partnership, strategic alliance, Memorandum of understanding with key departments) how robust and feasible it is?

- Leadership and people management – How skilled is the new leadership assuming national cyber strategy and how effectively it can exercise power. How it manages its relationship with other government department t. How cohesively the new team can work over

Hence keeping this key assumption in mind, the government could also look at an existing body like the National Security Council Secretariat (NSCS), but full authority must be given to NCSS to preside over cyber security affairs for the country with reporting to the National Security Advisor in the Prime Minister's Office.

**Acceptance of National Cyber Security Policy introduced by Ministry of Electronics and Information Technology (MEITY) by other government departments** - On 2<sup>nd</sup> July 2013, Ministry of Electronics and Information Technology ( MEITY) came up with National Cyber Security Policy which it wanted to enforce nationally and get acceptance from Ministry of Home Affairs, Ministry of External Affairs which had its set of guidelines for cyber security and had strong opposition to follow guidelines set by another department. Hence an important considerable to be addressed is whether the strategy must be in line with MIETY's National Cyber Security Policy or be overarching this policy?

**Setting up a Strategy Implementation Office:** A strategy implementation office must be setup to ensure successful execution of the cyber strategy. This would also plan cyber development projects of national important and track cyber security initiative with departments like UIDAI (AADHAAR), coordinate across key government program and resolve firefighting situations with other government departments.

### Scope for strategy

- 1) The national cyber security strategy must address countries clear objective as nation state and guarantee fundamental rights to its citizen and defining government role in protecting and safeguarding its citizen's interest.
- 2) The National cyber security strategy must reinforce states role in guarding its territorial borders from hostile states, nations and state actors and use of cyber space in doing so by carrying offensive cyber operation.
- 3) The national cyber security strategy must align with whole government structure in India i.e. with federal union comprising 29 states and 7 union territories to convey one nation intent to other nations and stakeholders [20].

- 4) The strategy should define roles and responsibilities of various department of government when it comes to managing cyber security operations. The cyber security strategy should mandate agencies with responsibility to handle diplomacy cyber-crime, offensive cyber operations, research and development, training and awareness, Incident response and resilience.
- 5) The strategy must also clearly articulate role of Indian National Security Council Secretariat or equivalent as single cyber nodal organization for the country which will give directions to various government i.e. CERT India, NTRO, MEA, MHA and MOD and could mandate offensive cyber operations.
- 6) The cyber strategy must mandate laws under which cyber security will be governed in the country with respect to handling cyber-crime, protecting national state from hostile attacks, data protection, and social media.
- 7) The Cyber strategy must call out for leader who will be responsible for driving cyber security for the country and define his reporting structure to the Prime Minister's office and must empower him to act as per the Indian Federal Laws.
- 8) The Cyber Strategy should articulate how cyber security is linked to national security and protection of countries citizens' safety and security.

#### Role of government departments

- 1) The national cyber security strategy should enable body like National Security Council Secretariat (NSCS) [21] to govern and lead cyber security operations for the country and dedicate a person as head of cyber security for the country.
- 2) Cyber diplomacy, offensive cyber security and cyber defence operation should be mandated under this head of cyber security for the country.
- 3) CERT India instead reporting to Ministry of Electronics and Information Technology (MEITY) should be directly under the head of cyber security at National Security Council Secretariat (NSCS).
- 4) CERT India should be given charge to coordinate help different states setup their own State CERT's
- 5) Cyber Crime managing institution should be setup under Head of Cyber Security under the National Security Council Secretariat (NSCS) which should support police in various states and union territories on cyber-crime management, prevention, readiness preparation, investigation, and response and building resilience.
- 6) Cyber Intelligence agencies should be tasked to operate under the head of cyber security for the country giving him charge to mandate cooperation among various cyber security.

- 7) Revenue, Tax, Special wings should also have reporting to the head of cyber security and roles, responsibility for level of cyber security operations.
- 8) Offensive cyber security capability should be given charge to single department or organization directly under the head of cyber security
- 9) Cyber Research & Development should also be directly under head of cyber security, so it is aligned with warfare doctrine.
- 10) Cyber Intelligence Analysis Unit should be central agency and its role should be only to carry out information analysis and not offensive or defensive cyber security.
- 11) Cyber Regulatory guideline issuing should be a single national body under head cyber security which could issue sector specific guideline which are in line with National Cyber Security Strategy
- 12) Cyber Security Capacity building should also be under the central nodal agency and head of cyber security to enable industry partnership and academia development.

## Conclusion

The general who wins a battle makes a calculation in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus, do many calculations lead to victory, and few calculations to defeat: how much more no calculations at all! It is by attention to this that I can foresee who is likely to win or lose – Quoted from “Sun Tzu on the Art of War”.

The India government needs to make better calculations of the threat vector it faces today surrounded by two hostile neighbours, come up with its own Cyber Security Strategy and setup a national level institution to govern, and manage cyber security for India as Nation with involvement of academia, industry and citizens.

A National Cyber Security Strategy led by PMO will lay a strong foundation for any law the Indian government plans to bring in for Privacy and Data Protection and also help government deliver to its promise of creating national cyber security center of excellence.

## Reference

1. Jandhan Yojna <sup>1</sup> Pradhan Mantri Jan-Dhan Yojana (P.M.J.D.Y), Prime Minister's People Money Scheme is India's National Mission for Financial by the Prime Minister of India Narendra Modi on 28 August 2014.

<https://www.pmjdy.gov.in/>

2. Digital Locker

<https://digilocker.gov.in>

3. World Bank report on India economic Growth FY 19, April 2018 :  
<https://data.worldbank.org/country/india>.
  4. Economic Times Article on India GDP Growth Mar 15, 2018  
<https://economictimes.indiatimes.com/news/economy/indicators/world-bank-projects-in-dias-fy19-gdp-growth-at-7-3-pc/articleshow/63300359.cms>
  5. Unique Identification Authority  
[https://UIDAI\(Aadhaar\).gov.in/](https://UIDAI(Aadhaar).gov.in/)
  6. Start-up India  
<https://www.startupindia.gov.in/>
  7. National Optics Fibre Communication  
<http://www.bbnl.nic.in/index1.aspx?lsid=249&lev=2&lid=21&langid=1>
  8. Digital India  
<http://digitalindia.gov.in>
  9. Make in India  
[www.makeinindia.com](http://www.makeinindia.com)
  10. Swift India Limited  
<https://www.swiftindia.org.in/what-purpose-swift-india>
  11. National Payments Corporation of India (NPCI)  
<https://www.npci.org.in/>
  12. Smart Cities Mission  
<http://smartcities.gov.in/content/>
  13. Sharma, Vakul. Information Technology-Law & Practice (2nd Edition): Universal Law Publishing Co. Pvt. Ltd, New Delhi, 2007
  14. Godse, Vinayak. Building an Ecosystem for Cyber Security and Data Protection in India , Data Security Council of India, NASSCOM
  15. Singh, Davinder -CYBER WARFARE: CHANGING CONTOURS OF WARFIGHTING, 2017, Centre for Land Warfare Studies (CLAWS), New Delhi 2017  
[http://www.claws.in/images/events/pdf/909097382\\_DasCyberWarfare.pdf](http://www.claws.in/images/events/pdf/909097382_DasCyberWarfare.pdf)
  16. Singh, Davinder , Strategic Year Book Centre for Land Warfare Studies (CLAWS), Bloomsbury Publishing India Pvt. Ltd. New Delhi, 2017
  17. Relia, Sanjiv. Cyber Warfare: Its Implications on National Security: Vij Books India Pvt. Ltd. New Delhi, 2015
  18. Mahopatra Das, Sucheta, Digitization of Battlefield , SP Guide Publication, 2013  
<http://www.pressreader.com/india/sps-landforces/20131210/281522223940218>
  19. Chabhra, Sanjay. India's National Cyber Security Policy (NCSP) and Organization- A Critical Assessment, Naval War College, India
  20. Luijck, Eric & Besseling, Kim & Graaf, Patrick. (2013). Nineteen National Cyber Security Strategies. International Journal of Critical Infrastructure Protection.
9. 3. 10.1504/IJCIS.2013.051608
21. Donthula Ravi Kumar\*, Indian Perimeter Cyber Security: Cyber Security Policy and Implementation.

22. [Indian Ministry of Electronics and Information Technology \( MEITY\) , Chief Information Security Officer's \(CISO\) Top Best Practices for a safe & secure Cyber environment 11th April 2018.](#)

[http://meity.gov.in/writereaddata/files/cisos\\_top\\_best\\_practices\\_guidelines.pdf](http://meity.gov.in/writereaddata/files/cisos_top_best_practices_guidelines.pdf)