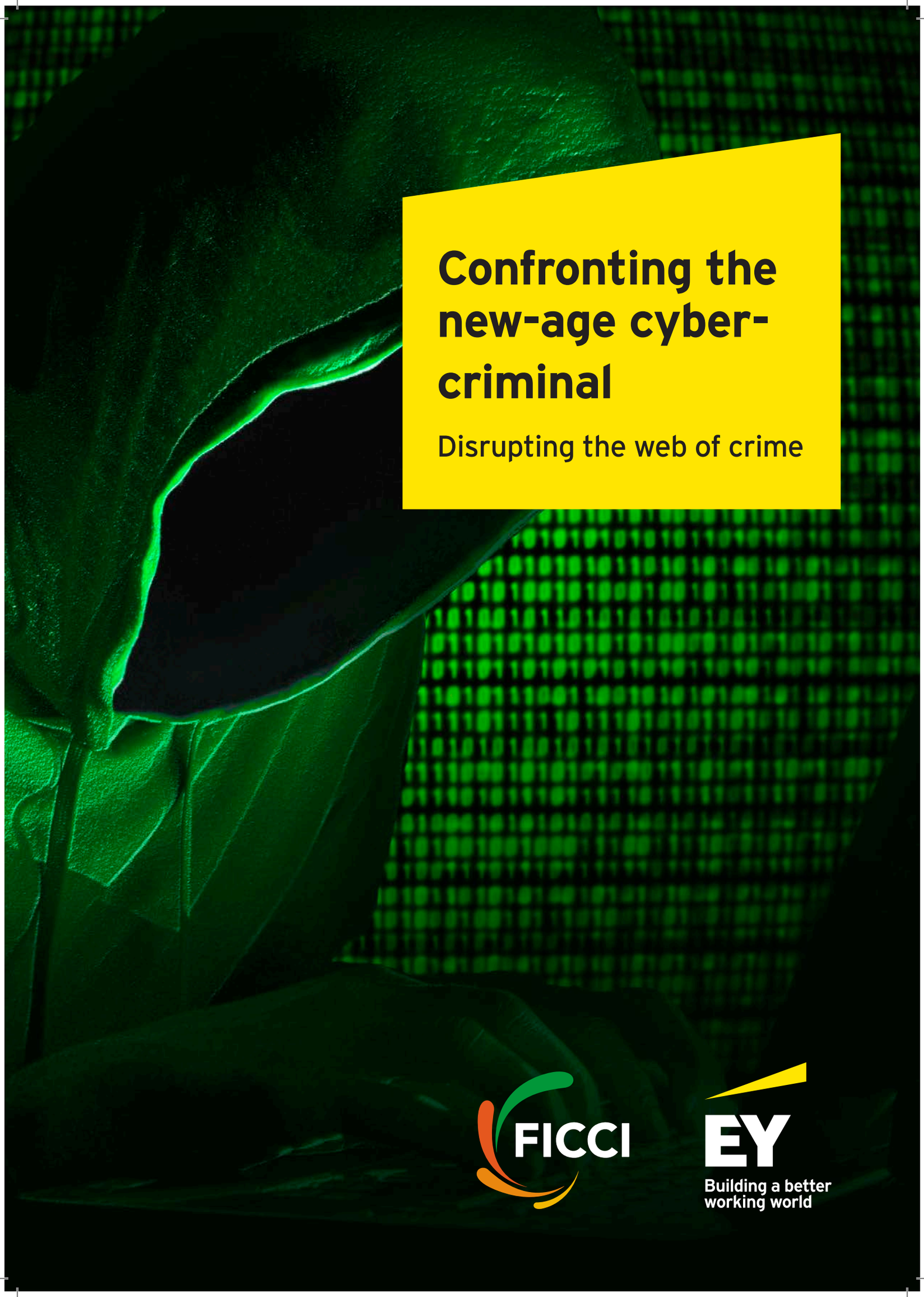


Confronting the new-age cyber-criminal

Disrupting the web of crime

FICCI

EY
Building a better working world

Foreword



The advent of Digital India and Smart City initiatives has brought about a paradigm shift in terms of connectivity, services and threats for both urban and rural eco-systems. While greater connectivity promises wider deliverables, it also paves the way for the emergence of new vulnerabilities. Leading companies in energy, telecommunications, finance, transportation and other sectors are targeted by new-age cyber criminals. As per CERT-IN, one cybercrime was reported every 10 minutes in India during 2017. This statistic is quite alarming and therefore, merits a focused and collective attention of security enforcement agencies.

The 'Make in India' initiative has identified 25 core sectors as part of its effort to give a special thrust. While cyber security is not one of the sectors, it could be embedded in certain sectors like – defence manufacturing, electronic systems, and IT & BPM. It is crucial for 'Make-in-India' to focus on Cyber security as well as promote development of indigenous solutions to combat cyber-crime.

In today's times, traditional methods of cyber-security are inadequate to combat cyber-crime. Hence, there is a requirement to devise mechanisms which are proactive in nature and help in identifying and preventing cyber-crimes.

This report delves into the strategies to confront new-age cyber-criminals with effective strategy for cyber-crime management. I am confident that this report will be of considerable value to all stakeholders in managing the threats in cyberspace which affect everyone.



Dilip Chenoy
Secretary General, FICCI

Preface



Technological breakthroughs in the cyber landscape over the past few years have caused disruptions of immense magnitude with far reaching implications. On one hand, these have been enablers for good governance, smart policing, better medical care, etc., while on the other, there has been a surge in cybercrimes, frauds and data thefts. Frequent criminalization instances of the web has resulted in proliferation of illicit trading of arms and drugs, cyberstalking, cyberbullying, cyber extortion, child pornography and so on. The protagonists have graduated from being opportunistic individuals to organized criminal groups who offer cybercrime-as-a-service at a minimal cost over the dark net.

To confront these new age cyber criminals, a well thought and effective cybercrime management strategy needs to be devised. If the law enforcement agencies have to win this battle, there is a need for a paradigm shift in the approach to policing. The focus needs to shift from conventional to contemporary methods with the right blend of upskilling and upgrading the three pillars– people, processes and technology. Predictive policing is needed to disrupt the expanding web of crime.

Policy changes at national and international levels are required to synergize the efforts of all agencies against these faceless and borderless enemies striking across time zones. Greater collaboration is needed to build a responsive framework to carry out effective cybercrime management. Enhanced citizen awareness, quick response mechanisms, technical augmentation and capacity building of law enforcement officers can go a long way in controlling cybercrimes. In addition to international cooperation, law enforcement officials must also be provided access to the tools and technologies like big data analytics, artificial intelligence, robotic process automation and blockchain to get ahead of the cyber criminals.



Rahul Rishi
Partner & Leader – Advisory Services
(Digital Government)



Content

01

Background

- Expansion of cyber ecosystem and its impact
- Cybercrimes in the connected world
- Convergence of cyber and terrorism

Page 8

02

Emerging areas for the law enforcement agencies

- Technical knowhow and skills
- Low cost high impact tools
- Technological advancements
- Territorial jurisdiction
- Defending critical infrastructure from cyber criminals

Page 12



03

Disrupting the web of crime

- Strategy
  - Awareness
  - Technical augmentation
  - Capacity building
  - International collaboration
  - Strengthen the legislative framework
  - Strengthen institutional framwork
- Big data for intelligence and security

Page 16

04

Cybercrime management framework

Page 20

05

Way forward

Page 22

Glossary of terms

Abbreviation	Definition
ICT	Information and Communication Technology
DDoS	Distributed Denial of Service
AI & ML	Artificial Intelligence and Machine Learning
NCIIPC	National Critical Information Infrastructure Protection Center
NTRO	National Technical Research Organization
CII	Critical Information Infrastructure
NCSP	National Cyber Security Policy
MoU	Memorandum of Understanding
DoT	Department of Telecommunication
IMCPF	Inter-Ministerial Committee on Phone Frauds
ISRO	Indian Space Research Organisation
CMAPS	Crime Mapping Analytics and Predictive System
ICJS	Integrated Criminal Justice System
CIP	Critical Infrastructure Protection
FBI	Federal Bureau of Investigation
CNI	Critical National Infrastructure
TOR	The Onion Router
VOIP	Voice-over Internet Protocol
CTCR	Counter Terrorism and Counter Radicalisation

Abbreviation	Definition
CERT-In	Computer Emergency Response Team -India
LEAs	Law Enforcement Agencies
MLAT	Mutual Legal Assistance Treaty
CDR	Call Data Record
LR	Letters Rogatory
SOC	Security Operations Center
FIRST	Forum of Incident Response and Security Teams
APCERT	Asia Pacific Computer Emergency Response Team
MeitY	Ministry of Electronics and Information Technology
RBI	Reserve Bank of India
RPA	Robotic Process Automation
CCTNS	Crime and Criminal Tracking Network & Systems
ANPR	Automatic Number Plate Recognition
CCTV	Close Circuit Television
FSL	Forensic Science Laboratory
UNDP	United Nations Development Programme
ACIC	Australian Criminal Intelligence Commission
Volte	Voice-over long-term evolution
NLP	Natural Language Processing
CIS	Cyber and Information Security



1 Background

> “Cybercrime has no borders and the fight against it shouldn’t either”



"Cyber related risks are a global threat of bloodless war. India can work towards giving the world a shield from the threat of cyber warfare[10]"

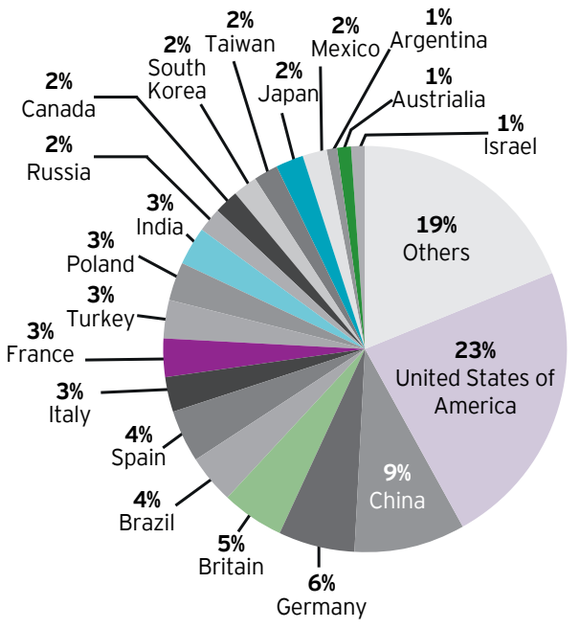
Honourable Prime Minister
Shri Narendra Modi[1]

Over the last few years, cybercrimes have become more intense, sophisticated and potentially debilitating for individuals, organizations and nations. Law enforcement agencies are finding it difficult to check and prevent the crimes in the cyber space because the perpetrators of these crimes are faceless and incur very low cost to execute a cybercrime whereas the cost of prevention is extremely high. Targets have increased exponentially due to the increasing reliance of people on the internet. Cybercrimes which were restricted to computer hacking till some time ago, have diversified into data theft, ransomware, child pornography, attacks on Critical Information Infrastructure (CII) and so on.

India is becoming increasingly vulnerable to this menace because of rapid digitization and proliferation of mobile data without matching pace of cyber security and cyber hygiene. At present, India is ranked third in terms of cybercrime incidents behind the United States and China (see fig 1) as per data shared by a leading security vendor, which compiled data of bot-infected systems controlled by cyber criminals in different countries.

As per CERT-IN, one cybercrime was reported every 10 minutes[2] in India during 2017. These statistics are quite alarming and therefore, merit focused and collective attention from Law Enforcement Agencies (LEA's).

Figure 1: Top 20 countries impacted by cybercrime



Expansion of cyber ecosystem and its impact

The increase in technology convergence has created an extremely complex ICT ecosystem of interdependencies, within and among critical sectors. This leads to an increased number of stakeholders and a larger attack surface which can be easily exploited by cyber criminals. There is no silver bullet technology which can identify or predict which element of the system (people, process or technology) is more susceptible to cybercrime, though empirically it is observed that the people are the weakest component of the cyber ecosystem.

Fig 2: Top cybercrimes in 2017

- 200K+ Computers in 150 countries were affected by the Wannacry malware
- 125+ machines in 64 countries faced the threat of Petya ransomware
- Wikileaks published a data trove containing 8761 documents stolen from the CIA
- Cyber risk researcher discovered a publicly accessible database with personal information for 198M USA voters in 2017
- Two days before France's presidential runoff, hackers dumped a 9GB trove of leaked emails from the party of Emmanuel Macron

[1]http://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece
[2]https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

Inherent anonymity and closed nature of the dark web has turned it into a safe haven for cyber criminals and their wares. The dark web hosts a wide range of illegal online markets of cyber exploit kits, drugs, counterfeit documents, stolen credit cards, bank account credentials, human trafficking, illegal immigration, etc. The dark web has thousands of forums which operate in a tightly controlled environment. Crypto currencies are used for transactions so that these transactions cannot be traced to individuals or organizations.

Ransomware continues to be a major threat the world over. In 2017, WannaCry, Petya, NotPetya, etc. caused major disruptions in the connected cyber ecosystem of the world. India was also affected. CERT-In[3] confirmed 37 incidents of WannaCry and Petya attacks in India between May and June last year. Petya caused extensive disruption of services in India. One terminal of JNPT, Mumbai had to switch over to manual operations due to this attack. India was the worst affected country in Asia and seventh overall, due to Petya attack.

Apart from ransomware, another area of significant concern is theft of personally identifiable information (PII) and financial credentials of individuals. In another incident of cybercrime, criminals stole personal data of over 2.7[4] lakh Indian users of the Ashley Madison website. Hackers, who stole 300GB of personal information of the users, put it up on sale over the dark web. Also, Cryptojacking is another lucrative method adopted by attackers to deploy a malware forcefully and unknowingly into a victim's computer to use their hardware for generating cryptocurrency. It is becoming yet another tool of choice for cyber criminals because it cannot be classically categorized as a crime.

Fig 3: Rise in cyber crime[5]

Cyber crime	2017	2016
Online banking	2,095	1,343
Facebook related	316	151
Email hacking	125	97
Sexual harassment	81	51
Lottery fraud	42	15
Data theft	47	43
Job fraud	49	40
Twitter related	12	4
Total cases	**3,474**	**2,402**

Cybercrimes in the connected world

One reason why cybercrimes are becoming more sophisticated, better orchestrated and increasingly ambitious is because many of the perpetrators operate outside the jurisdiction of the victim's country. As per industry estimates, 32% of the threat vectors originate from Eastern Europe and Russia[5] and social engineering is the preferred mode of launch for most perpetrators.

A report[6] indicates four distinct groups of cyber-criminals: Traditional gangs, state-sponsored attackers, ideological hackers and hackers-for-hire. The report also states that the entrance of new participants has transformed cybercrime from isolated and individualized acts into pervasive, savage practices run by distinct groups of individuals. Outsourcing is also possible for execution of these crimes on the dark web where cybercrime is offered as a service.

Cybercrime-as-a-service not only allows malicious actors to leverage other cybercriminals' resources to conduct attacks but also provides a cheap and easy option to others who are willing to enter the world of cybercrime at a very low entry cost. Netizens have increasingly become more active in leveraging these services, which is driving a surge in activities like illicit drug sale, trafficking of human beings, terrorism, child pornography and other crimes[7].

Illustrative rates of some of the services offered are given below

Figure 4: Rates of cybercrime-as-a-service

Account hacking program	US$12.99
Hacked Instagram accounts in bulk	1000-10,000 accounts US$15-US$60
Botnet: Blow-bot banking botnet	Monthly basic rental US$750 | Monthly full Rental US$1200 | Monthly Support US$150
Disdain exploit kit	Day US$80, week US$500, Month US$1400
Stegano exploit kit, Chrome, Firefox, Internet Explorer, opera, Edge	Unlimited traffic, day US$2,000 Unlimited Traffic, month US$15,000
Microsoft office exploit builder	Lite exploit builder US$650 Full version US$1,000
WordPress exploit	US$100
Password stealer	US$50
Android malware loader	US$1,500
DDOS attacks	Week long attack US$500-US$1,200

Cybercrime-as-a-service model has led to the emergence of a complex and multi-layered cybercrime economy where overt acts of crime have been replaced by a covert criminal ecosystem where the services and platforms feed off of and support crime-which has become increasingly low-investment, high-yield and a low-risk operation.

[3]https://economictimes.indiatimes.com/tech/internet/34-cases-of-wannacry-petya-ransomware-reported-to-cert-in-government/articleshow/59666898.cms
[4]https://www.indiatoday.in/technology/news/story/ashleymadison-hack-could-expose-2.7-lakh-indian-cheaters-283928-2015-07-22
[5]https://timesofindia.indiatimes.com/city/gurgaon/cybercrime-up-most-on-e-banking/articleshow/61634852.cms
[6]https://www.malwarebytes.com/pdf/white-papers/Cybercrime_NewMafia.pdf
[7]https://www.databreachtoday.com/how-much-that-rdp-credential-in-window-a-10590

A new method of cybercrime has emerged wherein genuine and legitimate social media platforms are used to manipulate opinions of impressionable minds through effective and sustained social media campaigns. There is enough evidence of manipulation of the election process in some countries through this method. This is an alarming sign which has far-reaching implications for the future.

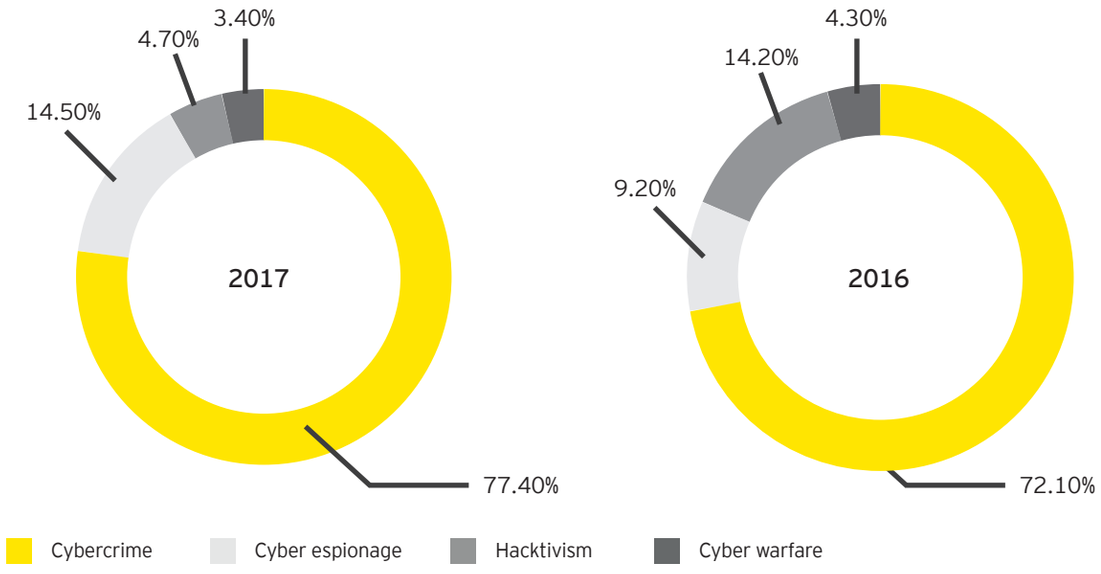
Convergence of cyber and terrorism

Cyber terrorism has been the most discussed topic during the last few years. Cyber terrorists use the computer and network technologies for promotion, communication and coordination to carry out attacks which cause public fear. The intent of conducting nationwide cyber-attacks by jeopardizing critical infrastructure (power sector, financial sector, oil, and gas, etc.) is the latest trend. The below figure (v) gives statistics on motivations behind the attacks based on the type of cybercrime[8].

Cyberattacks on energy grids are not a new thing. One such attack which was reported in January 2017 by researchers from ESET who identified a new piece of malware that is capable of controlling electricity substation switches and circuit breakers directly, in some cases literally turning them off and on again. They dubbed this malware Industroyer, which is being described as the biggest threat after Stuxnet. In-fact, it was used for Ukrainian blackout and in other critical sectors of the UK, the US and the EU. Any well-funded attacker can tailor this malware and execute a hacking campaign for specific critical infrastructure targets.

Proactive cyber patrolling and monitoring of everything digital, whether it is connected to a public network or otherwise, is the only answer to this complex problem. Technological advances in Artificial intelligence (AI) and its core areas like machine learning (ML) and natural language processing (NLP) may lead to more sophisticated cyberattacks in future. Cyber criminals may even leverage AI and ML powered hacking kits built from tools that are stolen from state-sponsored intelligence agencies[9].

Figure 5: Motivations behind attacks



"Cybercrime is the biggest challenge these days with development and access to technology across the globe. Cyber space is increasingly being used to radicalize young minds"

Honorable Home Minister, Shri Rajnath Singh[10]

[8]https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/
[9]https://www.infosecurity-magazine.com/news-features/cybersecurity-predictions-2018-two/
[10] economictimes.indiatimes.com/articleshow/51364115.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst



2 Emerging focus areas for law enforcement agencies

Technical know-how and skills[11]

Rapid and uncontrolled digitization coupled with inadequate response mechanism allows criminals to unleash cybercrimes through use of sophisticated tools which hide their identity and tamper, hinder or misdirect investigations. On the other hand, the law-enforcement agencies are still trying to upgrade their technical abilities to match the skills of their adversaries.

With the ever evolving threat landscape in the digital space, there is a constant need to upgrade technical proficiency and skills of the officers of LEAs. Whilst most of these officers are well versed in basic cybercrime investigation techniques, very few of them can be called cybercrime specialists.

Moreover, domain specialization is not institutionalized which further restricts their capability to monitor and check any form of cybercrime including trading on the dark net, human trafficking, child and women sexual abuse material, digital forensics, cyber frauds, etc.

Some states have taken initiatives to upgrade their cybercrime investigation capabilities through local software development while others are in the process of procuring tools and systems for this purpose. Few states have also procured forensic tools but lack specialized trainers who can train the law enforcement personnel. Further, there is a big crunch of resources to operate these forensic tools. Thus state wide efforts can only bear fruits if capacity building is uniform across the entire country and training programs are standardized to some extent.

Low cost high impact tools

Cybercriminals have easy access to low cost or freely available tools that can identify and exploit vulnerabilities in configuration, create phishing links and pages, design forms to steal personal information, voice impersonation tools and use dictionaries to guess passwords. Further, the distribution of these tools is widespread and law enforcement agencies have no or limited control over these.

The internet penetration rate of India is growing rapidly. However, a lack of awareness and netiquette make most of the user's easy target for cybercriminals. Phishing, for example, is mass rolled out, trapping a few in the chain. Many of the cybercrimes are either reported after a significant delay or not reported at all due to a fear of social shame, lack of knowledge or understanding of whom or where to report. Thus the crucial evidence is lost which makes the task of law enforcement agencies more difficult.

Technological advancements

Technological advancements are making the task of cybercriminals easier. Encryption and steganography are being leveraged by cybercriminals to thwart the LEAs, who are not able to decrypt the information in time to predict and prevent crimes. Criminals use the dark and deep web with impunity to exchange information without risking identification through normal and traditional search engines. The complex encryption mechanism along with anonymization tools used to access and trade over the dark net put forth complex challenges for LEAs who are unable to break into these forums and track the criminals.

Migration to VoIP, Volte and other Over the Top (OTT) services like WhatsApp and Viber, etc. has made the task of intercepting voice calls extremely complex. These calls can only be intercepted with the active support of the respective service providers. Often, servers are located outside the country and make it virtually impossible to monitor voice calls of criminals in real time. Tower dump and CDR data can only provide limited information in critical situations like the Mumbai attacks or in anti-terrorist operations.

Cybercriminals create botnets by injecting malware into unprotected systems and use them to launch DDoS attacks, command and control, spam broadcast, exfiltration, cryptojacking operations, etc. Tracking of botnets is a complicated task and may not point to the offender. As cybercriminals have easy access to advanced technologies, the gap between the capabilities of investigating authorities and activities of cybercriminals continues to widen.

Fig 6: Scale of bitcoin as ransom

Demand of Bitcoins as ransom

By tracking the Bitcoin accounts associated with ransomware, researchers at University of Padua, Italy have calculated how much cyber criminals have extracted from their victims.

They created a database of Bitcoin accounts associated with ransomware activity since 2013 when "Crypto locker" became the first ransomware to ask for payment in bitcoins. It has emerged that "Crypto wall" has collected more than US$4.5 million in bitcoins and other transactions and remains the most productive malware till date. Contrary to popular perception, WannaCry and NotPetya received only US$86,076.76 and US$9,835.86 respectively despite the hype around them.

Cybercriminals use cryptocurrencies because of anonymity. However, bitcoin transactions are pseudonymous because even a single transaction that links Bitcoin account to a personal account can reveal the identity of the cybercriminal. This prospect should excite the LEAs and encourage the use of analytics to establish such linkages.

[11]http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Territorial jurisdiction

It is a cliché that cyber space knows no boundaries. Conventional policing is geographically bound and thus, inadequately equipped to handle crimes in the cyber space. Although, Section 75 in India's Information Technology Act, 2000 specifies punishment for commission of any offence or contravention by a person outside India irrespective of his nationality (if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India), its implementation cannot be ensured due to non-availability of suitable agreements or treaties between countries from where such criminal acts originate. The physical location of servers and data is another challenge. Even if the perpetrator is identified, the process of producing evidence becomes complicated for LEAs. In such cases, there is a formal process of letter rogatory (LR) or letters of request in writing sent by the court to a foreign court requesting the suspect or witness for testimony. In the same way, a formal agreement gets invoked to get the information or accused from foreign countries called as mutual legal assistance treaty (MLAT). Even in the registered cybercrime cases channeled through MLAT (India have signed with 37 foreign countries[12]), it takes a fairly long time to obtain relevant data.

Collaboration and rapid information sharing is required among nations to combat the growing menace of cybercrime. The double criminality or dual criminality principle establishes a dependency on the individual laws of the country. Dual criminality is a required law for extradition in many countries so that a suspect may be extradited from one country to stand trial for breaking laws of the other country.

Every country has its own cyber laws enacted keeping its national interest in mind. The requirement of multinational cybercrime conventions is critical to ensure that investigation and subsequent prosecution meets legal rigor needed for bringing cybercriminals to justice. Cybercrime conventions like the Budapest convention, facilitate faster investigation and help prosecute cyber criminals within the member nations (India is not part of this convention).

Cloud storage adds to the complexity as far as territorial jurisdiction is concerned. Situations wherein some data lies outside the jurisdiction of a LEA can make evidence collection and subsequent presentation before the courts a major challenge. The data retention period for phone and internet logs are inconsistent across countries. This limits investigation capabilities of law enforcement agencies, e.g., despite the EU directive to retain data for a period of six months, in Germany, service providers are supposed to store call data records (CDR) and metadata for a period of 10 weeks and cell phone location data for four weeks only. The corresponding figures in respect of India are six months.

Sustaining critical infrastructure in wake of cyber terrorism

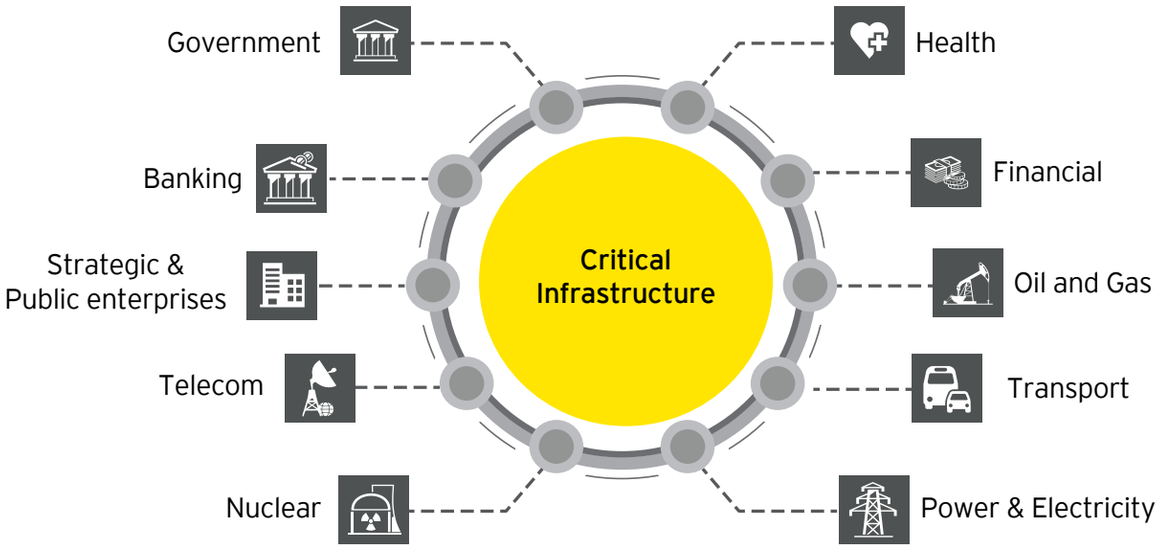
India has made significant investments in establishing the National Critical Information Infrastructure Protection Center (NCIIPC) in accordance with section 70A of India's IT (Amendment) Act, 2008. Its aim is to regulate and raise information security awareness among the critical sectors of the nation rather than technology interventions. It started off with only five sectors[13], though other countries like the US, the UK, the UAE, etc. have considered more than ten sectors as Critical National Infrastructure (CNI), that are essential for society and economy. Non-critical systems/sectors are taken care by CERT-IN.

While India's National Cyber Security Policy (NCSP) published in 2013 set the tone for formulating a comprehensive effort for protection of CII, there is still no clarity with regard to coordination mechanism between organizations such as of NCIIPC, NTRO and CERT-IN, among other agencies mentioned in the policy, specifically with regards to protection of critical Infrastructure[14] .

The FBI in the US defines cyberterrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents". Cyberterrorist attacks are not the same as hacking or breach of consumer data but they aim to source global panic or mass-loss of life by disrupting the critical infrastructure. The law enforcement agencies need a focused approach, enhanced technical skills and strengthened international collaboration to defend the CII.

Also, ancillary cyber activities by terrorists to spread propaganda through the internet is not treated as cyber terrorism. These pose major challenges for the law enforcement agencies.

Figure 7: Critical infrastructure



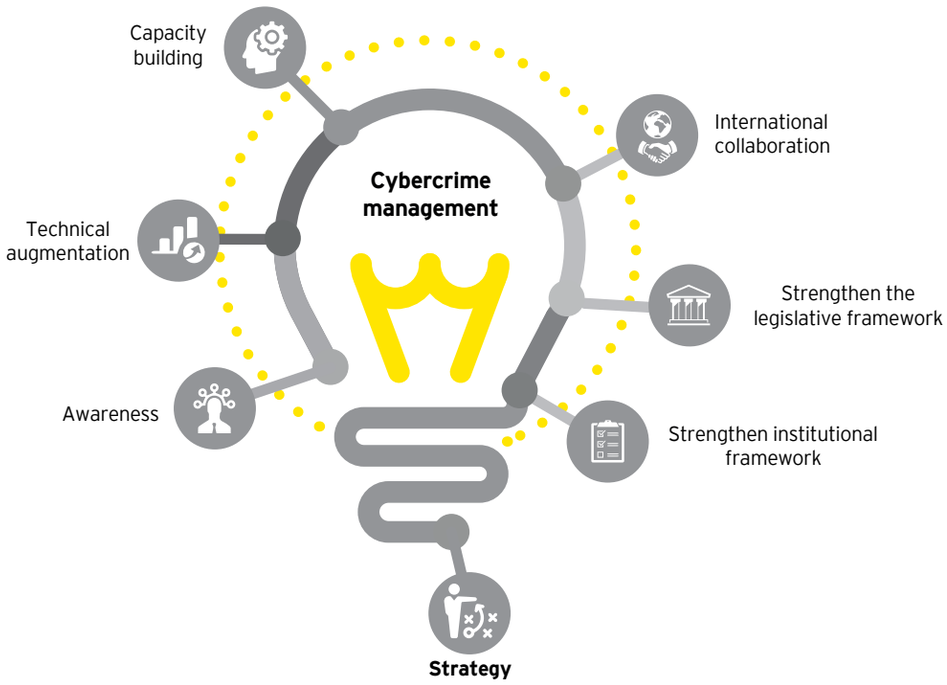
[13]http://www.digitalpolicy.org/nciipc-evolving-framework/
[14]https://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review



3 Disrupting the web of crime

Strategy

Figure 8: Cybercrime management strategy



Awareness

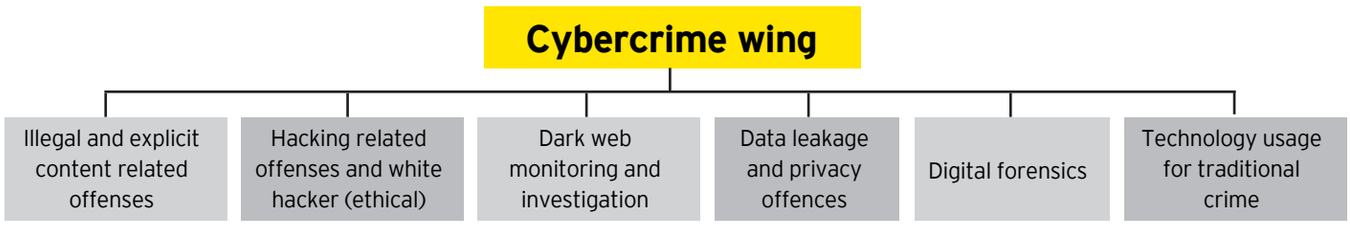
One of the easiest and simplest methods of preventing cybercrime is greater awareness. Most of the cyber frauds occur due to a lack of awareness and poor cyber hygiene amongst the citizens. Basic awareness can reduce the effects of various forms of fraudulent social engineering significantly. Innovative and appealing cyber awareness campaigns (with long recall value) can help in this regard. As part of public awareness campaign, citizens should be informed about the most recent cybercrime and cyber frauds and means to tackle them. They should be encouraged to report all incidents of cyber frauds, without the fear of being ridiculed or harassed.

Technical augmentation

Evolution of innovative cybercrime techniques and the increasing threat landscape has resulted in the need to enhance technical capabilities for law enforcement agencies. A focused approach and investigation is required to investigate and prevent cybercrimes. For law enforcement agencies, it is important to make a transition from working in isolation to a collaborative approach and increase their capabilities through technical empowerment of their cadre. Such collaboration may be with the private sector or other states who have taken progressive steps in this domain.

This would help identify gaps in the technical capabilities and undertake steps to overcome them. Further, it would act as an enabler in the long terms for creating in-house advanced technical capabilities, better administration, focused investigation and to shorten the investigation time period. An indicative breakdown of a conventional cybercrime cell can be viewed in Figure (9).

Figure 9: Illustrative Organization structure of Cybercrime Wing



[11]http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Capacity building

Capacity building is one of the main pillars for an effective cybercrime management strategy. LEAs have taken the first step towards capacity building by training officers on cybercrime investigation techniques. It should be taken further by providing focused training in areas like dark web monitoring, network security, cryptography, image processing, ethical hacking, digital forensics, etc. Experts for each domain need to be identified and mapped against sub-units of the cyber wing. The skill upgradation should be carried out in smaller cycles to keep in pace with technological progress.

A specific budget should be allotted for capacity building programs. Annual training plans should be rolled out along with contingency plan as the law enforcement officers might need to handle ad-hoc requests and cases. While developed countries have molded the culture of expert cyber policing, other nations have novice or intermediate level cyber investigation capabilities. This gap can be covered via international collaboration, which has its additional advantages, as discussed in next section.

International collaboration

Challenges related to territorial jurisdiction, information exchange and enhancing MLAT can be achieved via effective diplomatic dialogues and international collaboration.

Credible threat intelligence can be developed through inputs from multiple nations working in a collaborative manner. LEAs should engage in multilateral law enforcement and information sharing with international agencies like the Interpol and Europol. MoUs can be signed with agencies like the FBI, Australian Criminal Intelligence Commission (ACIC), National Crime Authority-UK, Europol, etc. Further, to strengthen the institutional framework the CERT-In along with conceptualized sectoral CERTs should collaborate with CERT US, FIRST, APCERT and other computer emergency response teams over the globe.

To facilitate interaction with national and international agencies India will setup its first cybersecurity cluster called as Hyderabad Security Cluster (HSC[16]) similar to the lines on world's largest cybersecurity cluster The Hague Security Delta.

Legislation

With the current geopolitical situation prevailing in India, we should strengthen our IT laws to check the growing crime on the World Wide Web. India should participate in as many international conventions and MLAT treaties and increase the number of MoU's with international agencies to curb cybercrime menace from adversaries. We need to work on bringing laws rather than guidelines, which are enforceable and deterrent in nature. Cybercrimes should be treated as acts against national security if needed.

Policies need to be rephrased and effective legal frameworks need to be put in place as part of the overall strategy to counter cyber offences. There is a need to issue practical policies on protecting the critical infrastructure of the nation and clearly define roles and responsibilities of each agency mentioned in the policy.

It is essential to address private CII operators about whom they should be accountable to in the event of cyber-attacks. The center has to identify and operationalize sectoral CERTs to tackle cyber threats in specific sectors. The need for standards on critical infrastructure protection (CIP) need a detailed roadmap.

Certainly, the public and private partnership is crucial for sharing cyber security information, but there should be an approach to facilitate the coordination between security firms and initiate new campaigns on recommendations towards technology verge.

Strengthening the institutional framework

Centers like "Cyber Swachhta Kendra" are steps towards the right direction in creating a secure cyber ecosystem. But it would need a lot more background work to create a realm of tools that citizens trust and use to protect their sensitive data.

Though we have forensic science laboratories (FSL) to conduct digital forensic investigations, the center should also facilitate crime investigation labs focusing on specific domains under cyber security, viz., dark web monitoring, open source intelligence, crime against children and women and other malware attacks. As a first level of defense in cybercrime and cyber security, implementing a security operations center (SOC) with adequate people, process and technology are essential to strengthen the institutional framework.

Initiatives taken by the Government of India under the Ministry of Home Affairs formulated two new divisions[17] to thwart cyber fraud and check radicalization, namely, Counter Terrorism and Counter Radicalization (CTCR) Division and Cyber and Information Security (CIS) Division. The objective of CTCR is to devise strategies and prepare action plans for combatting terrorism, whereas CIS has been created for monitoring online crimes and counter threats like online frauds, dark net, hacking, identity theft, etc.

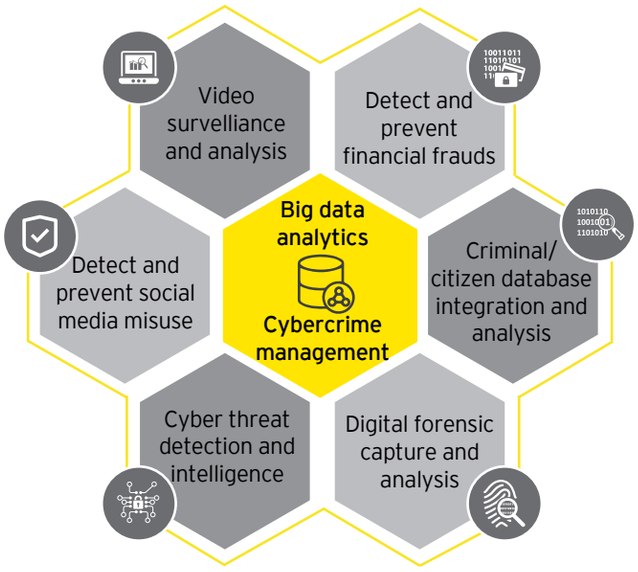
[16]https://timesofindia.indiatimes.com/city/hyderabad/indias-first-cyber-security-cluster-to-come-up-in-hyderabad/articleshow/63450161.cms
[17]http://pib.nic.in/newsite/PrintRelease.aspx?relid=176314

Strengthening the institutional framework

With the proliferation of digitization, many projects like the Crime and Criminal Tracking Network and System (CCTNS) and Integrated Criminal Justice System (ICJS) have been undertaken by the police forces to bring transparency in police functioning and to provide a hassle-free environment to the citizens. This brings in multiple databases and software applications which need to be managed by police departments. Policemen also collect data from sources like CCTV footage and automatic number plate recognition (ANPR) data through routine policing. Thus, a huge amount of unstructured data is generated which has to be incorporated in the overall response strategy.

Big data technologies can be applied to policing for the collection of data from various sources and apply intelligence and analytics on it to gain a richer understanding on specific crime or criminal. LEAs can benefit tremendously by collecting, integrating, analyzing and delivering real-time crime data using this technology. The inputs can be from internal (crime databases) as well as external sources (like social media). Some of the possible scenarios are depicted in figure (10)

Figure 10: Indicative areas of big data for analytics



Big data can help in descriptive, diagnostic, predictive and prescriptive analysis, as given in figure (11), thereby giving the LEAs unprecedented advantage over the cyber criminals. Predictive policing can only be achieved through the adoption of a comprehensive and focused approach in this direction.

Fig 11: Cybercrime data modelling techniques

Big data modelling techniques to tackle cybercrime

Predictive

Analyze current and historical facts to forecast about future or otherwise unknown crimes

Descriptive

Analyze real-time crimes along with the relationships between factors responsible for them

Diagnostic

Identification of why crime occurred by analysis of the background/history, study signs to identify probable causes

Prescriptive

Using data and analytics to improve policing decisions and therefore the effectiveness of initiatives to prevent criminal actions

4 Cybercrime management framework

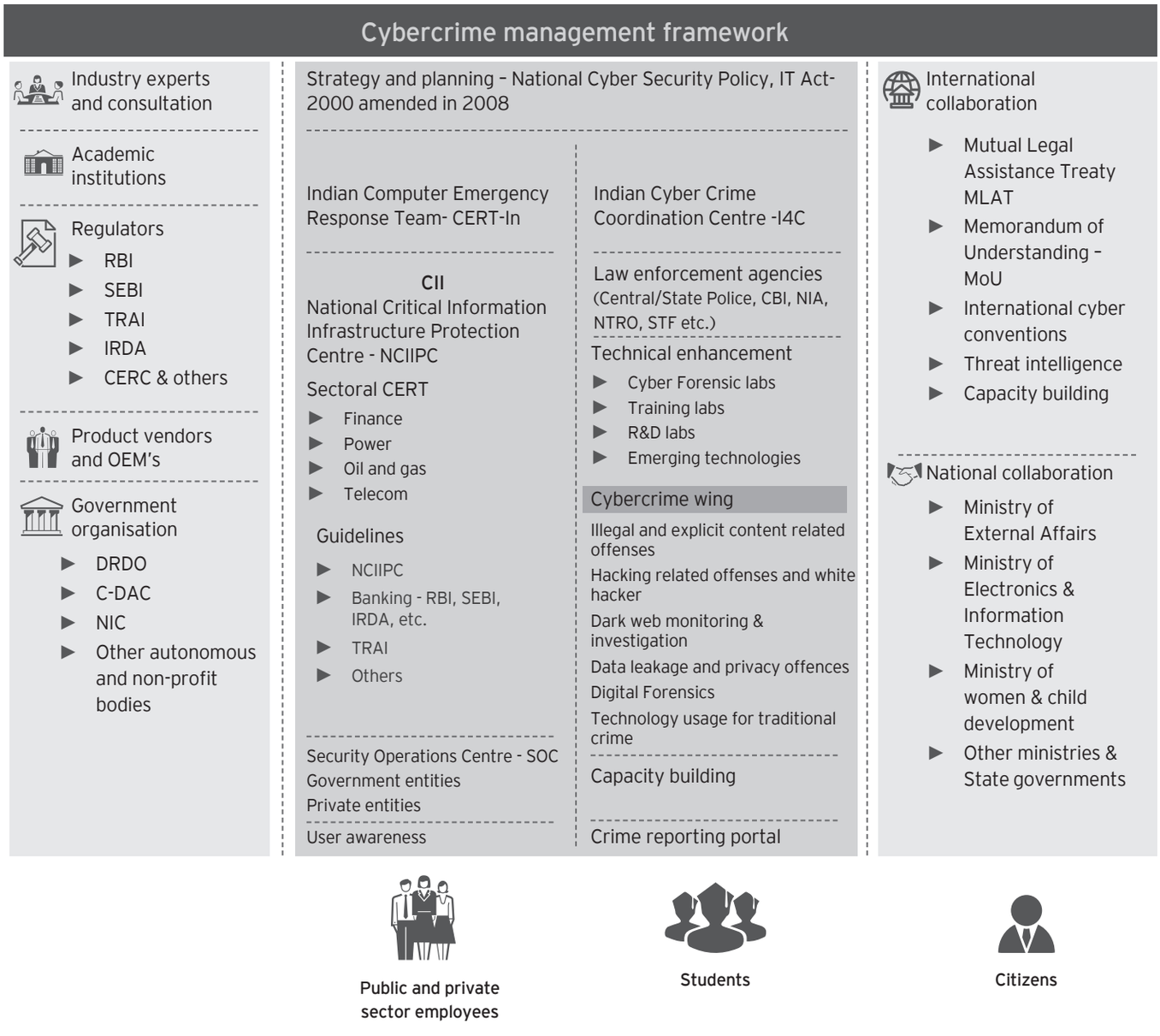


Initially, cybercrime evolved as a threat to individuals and organizations. However, today it has started impacting the nations as well. In order to tackle this problem, a synergized and holistic framework is required to be developed which must be universally acceptable and implementable in order to counter the threat of cybercrimes and associated risks in cyber space. An illustrative framework [as shown in figure (12)] explains that cybercrime is a shared responsibility of each and every stakeholder without whose contribution, the cyber ecosystem cannot be protected.

Crime Mapping analytics and Predictive System (CMAPS): By leading police agency

An Indian Law Enforcement Agency has implemented an application with free and open source tools called Crime Mapping Analytics and Predictive System (CMAPS). It is integrated with emergency management system like Dial-100, CCTNS (Crime and Criminal Tracking Network and Systems), archived crime data and ISRO satellite image repository to create and visualize cluster maps used for tracking crimes.

Figure 12: Cybercrime management framework



5 Way ahead



Frequency, sophistication and destructive potential of cybercrimes is increasing at an alarming pace. Traditional methods of cyber security are not adequate to combat these crimes. So, there is a requirement to devise mechanisms which are proactive and are able to identify and prevent cybercrimes. Cybercrime management is an effective and credible mechanism to thwart cybercrime. This requires higher focus and commitment with a multi-stakeholder framework with an impetus on:

- Strong bilateral agreements (national and international) on cybercrime investigations, information sharing, intelligence, the applicability of international and territorial laws, capacity building, research and development.
- Modular restructuring of cybercrime cells with high tech tools, refining practices and investigation techniques along with human skill enhancement in the areas of digital forensics, dark web monitoring, tackling crime against women and children, etc.
- Strengthen the national core networks and systems with establishment/ enhancements of Cybersecurity Incidence Response Team (CSIRT), Security Operations Center (SOC), etc.
- Develop and refine cybercrime reporting methodologies along with the adoption of emerging technologies like Robotics Processing & Automation (RPA), Artificial Intelligence (AI) and analytics for smart policing and investigations.
- Sponsor nationwide cyber awareness programs for citizens and central, state government employees.

In order to build a credible and strong cybercrime management framework, it is essential to create an empowered state-of-the-art cybercrime coordination center which should be the nodal agency for formulating a national cybercrime strategic plan, policies, gather information and interact with all major stakeholders. It should be able to coordinate activities of all LEAs and other stake holders to thwart criminal activities by international cyber gangs who infiltrate the critical networks and extricate data.

The need of the hour is to develop a framework for solving cyber cases as developed by few countries including China. An Inter-Ministerial Committee on Phone Frauds (IMCPF[18]) has been constituted in the Ministry of Home Affairs in Sep, 2017 comprising of MHA, MeitY, Department of Financial Services, Department of Telecommunication (DoT), Reserve Bank of India (RBI) and other law enforcement agencies. This Committee should be mandated to include cybercrimes also as part of its charter because the distinction between phones and computers has virtually disappeared with the proliferation of smart phones.

To strengthen the law enforcement against cybercrime, international law enforcement agencies like the EUROPOL have already established a dedicated hub, called the European Cybercrime Centre (EC3[19]) . It has made a significant contribution to the fight against cybercrime and has formulated a three-pronged approach or framework. This comprises of forensics, strategy and operations. Though EC3 draws on existing law-enforcement, it had set up Joint Cybercrime Action Task Force (JCAT) to work on international cybercrime cases. They also publish the internet organized crime threat assessment report (IOCTA) which gives findings on new developments and emerging threats in cybercrime.

The two major concerns considered by law enforcement agencies (like the FBI[20]) in the developed countries are:

- Reporting the cybercrime
- Public awareness

By reporting internet crime, victims are not only alerting law enforcement to the activity, but aiding in the overall fight against cybercrime. Digital crime complaints are increased only with the help of announcements and advertisements reiterating the importance of reporting. Encouraging these initiatives on awareness may help the LEAs to mitigate and combat cybercrime. Awareness may also include current or top crimes reported like financial frauds, personal data breach and phishing.

Currently, India has MoUs with Bangladesh, Israel, Japan, Russia, Singapore, Spain, Malaysia, US, Uzbekistan, Vietnam and the EU in the fields of cybercrime and cyber fraud[21]. The Indian government should further increase collaboration with other countries in this sphere. This will result in a more coordinated governance on cyber related issues. In addition to this, modernization of the LEAs and capacity building at various levels will allow India to carry out effective and timely cybercrime management at all levels.

LEAs have to strive to step up the investigation, leverage provisions of various procedures and agreements, share intelligence and ensure multi-agency collaboration to secure the prosecution of criminals. It will ensure the efforts and resources that are effectively expended in the response to the evolving landscape of crime. Takedowns of websites and forums on the dark web through multi nation collaboration has been done in Europe recently. This initiative has to be supported and cooperation extended to other nations so that the web of crime is disrupted and prevented from turning into a web of profit for the cyber criminals.

[18]http://pib.nic.in/newsite/PrintRelease.aspx?relid=173446
[19]https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[20]https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-ic3-2017-internet-crime-report-and-calls-for-increased-public-awareness
[21]http://meity.gov.in/content/active-mous

Reference

1. https://economictimes.indiatimes.com/articleshow/51364115.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
2. https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
3. https://www.cybriant.com/2018/03/2018-cybercrime-stats/
4. https://www.businesstoday.in/technology/internet/cryptojacking-attacks-rose-by-8500-per-cent-globally-in-2017/story/274145.html
5. https://www.infosecurity-magazine.com/opinions/cyber-gangs-smarter/
6. https://www.malwarebytes.com/pdf/white-papers/Cybercrime_NewMafia.pdf
7. https://www.armor.com/app/uploads/2018/03/2018-Q1-Reports-BlackMarket-DIGITAL.pdf
8. https://www.databreachtoday.com/how-much-that-rdp-credential-in-window-a-10590
9. http://news.softpedia.com/news/the-number-of-reported-cyber-attacks-grew-in-2015-500303.shtml
10. https://cdn1.esetstatic.com/ESET/US/resources/white-papers/ESET_Trends_Report_2018_final.pdf
11. https://www.infosecurity-magazine.com/news-features/cybersecurity-predictions-2018-two/
12. https://www.cybersecobservatory.com/2018/02/09/6-cyber-attacks-business-networks-will-face-2018/
13. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
14. https://www.cioinsight.com/security/slideshows/cyber-criminals-found-a-home-on-social-media-sites.html
15. https://timesofindia.indiatimes.com/city/gurgaon/cybercrime-up-most-on-e-banking/articleshow/61634852.cms
16. http://cbi.nic.in/interpol/invletterrogatory.php#assist
17. https://www.technologyreview.com/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/
18. http://www.digitalpolicy.org/nciipc-evolving-framework/
19. https://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review
20. http://pib.nic.in/newsite/PrintRelease.aspx?relid=173446
21. http://meity.gov.in/content/active-mous
22. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
23. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-ic3-2017-internet-crime-report-and-calls-for-increased-public-awareness

FICCI Homeland Security Department

FICCI has many specialised committees where key concerns of the industry are debated and discussed with the specific aim of presenting the recommendations to the Government for favourable decisions.

Considering internal security is the backbone of growth and overall development of the nation, FICCI has constituted a Committee on Homeland Security (HLS), which is working towards bridging the gap between policing and technology.

Some of the focus areas:

SMART Policing: FICCI has instituted the first ever SMART Policing Awards in India for best practices in SMART Policing, with the objective to promote initiatives taken by the Police for safety and security of Indian citizens. This can change public perception and build positive and progressive image of the police among people. FICCI SMART Policing Awards provide a platform to police officials across India to learn from the experiences of other states and also for possible adoption of the best practices to further enhance policing in their respective states.

Police Modernisation: FICCI is working towards bridging the gap between policing and technology. We engage with various enforcement agencies and provide them a platform to interact with industry, to articulate their requirements and to understand new technologies for security. This initiative is under our umbrella theme of "Modernisation of India's Internal Security Mechanism".

Smart Border Management: FICCI is working towards addressing the emerging challenges faced by India in smart border management, by bringing stakeholders together to discuss how India can create smart borders that, on the one hand, allow enhanced trans-border movement of peoples, goods and ideas, and on the other, minimise potential for cross-border security challenges.

Indian Unmanned Aerial Vehicle (UAV) Policy & Regulations: FICCI has set-up Working Groups in areas of: (a) enabling regulations for developmental use of UAVs, and prevention of rouge UAVs; (b) framework for permission and licencing for manufacturing of UAVs; and (c) technological structure for detection and neutralisation of unidentified UAVs. FICCI has recently submitted its preliminary suggestions and recommendation for Indian UAV Policy & Regulations to the NITI Aayog, Ministry of Home Affairs and Directorate General of Civil Aviation.

Policy for Public Procurement in Internal Security: FICCI is working towards advocacy for bringing well-defined procedures for fair and transparent procurement of security products and solutions, so as to provide level playing field to the industry. Although the Central Armed Police Forces (CAPFs) and State Police Forces are guided by the same policies and guidelines for public procurement as other government organizations, the nature and requirements of public procurement process for police forces is different from that of the general government departments. FICCI has provided policy inputs to the Government of India for numerous challenges in regard to procurement by Internal Security forces, in the areas of policies and regulations, processes, technological advancements and capacity-building.

Cyber Crime Management: FICCI has initiated working towards promoting development and implementation, of systems and concepts to combat cyber-crime as well as improve cyber security.

Road Safety: United Nations has proclaimed 2011-20 as the Decade of Action on Road Safety. FICCI feels that the Indian Industry can play a significant role in addressing the issue of road safety.

Contacts

Mr. Sumeet Gupta
Senior Director
Email: sumeet.gupta@ficci.com

Mr. Ankit Gupta
Senior Assistant Director – Homeland Security
Email: ankit.gupta@ficci.com
Mobile: +91-99900 89493

FICCI
Federation House, Tansen Marg, New
Delhi 110 001
Telephone: +91-11- 23487212, 23487474
www.ficci.com



EY contacts

Gaurav Taneja
National Director
Phone: +91 124 671 4990
Email: Gaurav.Taneja@in.ey.com

Nitin Bhatt
Global Leader -Risk Transformation and
India Leader - Risk Advisory Services
Phone: +91 806 727 5127
Email: Nitin.Bhatt@in.ey.com

Rahul Rishi
Partner & Leader
Advisory Services (Digital Government)
Phone: +91 116 623 3183
Email: Rahul.Rishi@in.ey.com

Vidur Gupta
Partner – Advisory Services (Cyber Security)
Phone: +91 124 6711380
Email: Vidur.Gupta@in.ey.com

Akshya Singhal
Director – Advisory Services
Phone: : +91 124 464 3277
Email: Akshya.Singhal@in.ey.com

Aseem Mukhi
Sr. Manager – Advisory Services
Phone: +91 999 000 2658
Email: aseem.mukhi@in.ey.com

Sunil K Agarwal
Manager – Advisory Services

Hijaz Ali Shaik
Consultant – Advisory Services

Prathamesh Pande
Consultant- Advisory Services



EY offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near C.N. Vidhyalaya
Ambawadi
Ahmedabad - 380 015
Tel: + 91 79 6608 3800
Fax: + 91 79 6608 3900

Bengaluru
6th, 12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 4027 5000
+ 91 80 6727 5000
+ 91 80 2224 0696
Fax: + 91 80 2210 6000

Ground Floor, 'A' wing
Divyasree Chambers
11, O'Shaughnessy Road
Langford Gardens
Bengaluru - 560 025
Tel: +91 80 6727 5000
Fax: +91 80 2222 9914

Chandigarh
1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: +91 172 331 7800
Fax: +91 172 331 7888

Chennai
Tidel Park, 6th & 7th Floor
A Block (Module 601,701-702)
No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100
Fax: + 91 44 2254 0120

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurugram - 122 002
Tel: + 91 124 464 4000
Fax: + 91 124 464 4050

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 6671 8000
Fax + 91 11 6671 9999

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Noida - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000
Fax: + 91 120 671 7171

Hyderabad
Oval Office, 18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500 081
Tel: + 91 40 6736 2000
Fax: + 91 40 6736 2200

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur - 831 001
Tel: +91 657 663 1000
BSNL: +91 657 223 0441

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 304 4000
Fax: + 91 484 270 5393

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 2281 7750

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 1000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E),
Mumbai - 400 063
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 3000

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 6603 6000
Fax: + 91 20 6601 5900

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

© 2018 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN1805-009
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RG

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialisation, and its emergence as one of the most rapidly growing global economies.

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

© Federation of Indian Chambers of Commerce and Industry (FICCI) 2018. All rights reserved.

The information in this publication has been obtained or derived from sources believed to be reliable. Though utmost care has been taken to present accurate information, FICCI makes no representation towards the completeness or correctness of the information contained herein. This document is for information purpose only.

This publication is not intended to be a substitute for professional, legal or technical advice. FICCI does not accept any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents

ey.com/in

@EY_India EY|LinkedIn EY India EY India careers ey_indiacareers