CONCEPTUAL FRAMEWORK

FOR ESTABLISHING

STATE CYBER CRIME

COORDINATION & SECURITY CENTRE

Contents

STATE CYBER CRIME COORDINATION & SECURITY CENTRE

1. Introduction

TS Police has the vision to develop as an information-centric police organisation that is well-connected with the civil society, leveraging ICT to provide efficient and uniform police service delivery to the citizens of Telangana State in order to prevent crime and provide an environment for well-being. TS Police is striving continuously to deliver the most efficient, effective, and quality police services to the advancement of a cooperative partnership with the community to develop better policing and reduced crime. With the advent and support of new technologies, TS Police could able to produce gradually the productive results in all aspects of policing especially in crime prevention and control.

Currently, TS Police is focussing on how to effectively counter threats posed by cybercriminals. While cybercrimes evolve, new challenges emerge for traditional regulatory and law enforcement agencies. TS Police has contemplated giving impetus on delivering the most efficient services to the citizens in respect of emerging cybercrimes and criminal threats. As such, there is a need to go beyond traditional law enforcement and explore means that predict, prevent, and disrupt online criminal activities through an effective capacity building framework.

The development of the Internet and its continued growth has a significant impact on the development of societies across the world. The Internet is now an integral and essential component of our society and our economy apart. The rise of the Internet has fostered the emergence of new criminal threats. These threats pose significant risks for companies, governments, and individuals.

The fight against cybercrime has become a major global challenge due to the international dimension of this new organized crime often. Cybercrime is evolving every day, revealing new forms of risk and techniques to circumvent the law. The only possible step is to make people aware of their rights and duties (to report the crime as a collective duty towards the

society) and making the application of the laws more stringent to check cybercrime.

1.1. Cybercrime – a new phenomenon

Criminals are using new technologies to commit cyberattacks against governments, businesses, and individuals. These crimes know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. "Pure cybercrime" refers to crimes against computer and information systems, where the aim is to gain unauthorised access to a device or deny access to a legitimate user. Cybercrime is a relatively new phenomenon. Services such as telecommunications, banking and finance, transportation, electrical energy, water supply, emergency services, and government operations rely completely on computers for control, management, and interaction among themselves. Most of the global businesses maintain WWW sites and over half of them conduct electronic commerce on the Internet. The rise in popularity of the Internet for both private persons and businesses has resulted in a corresponding rise in the number of Internet-related crimes.

1.2. Cybercrimes and the changing scenario

Traditional forms of crime have evolved as criminal organisations turn increasingly to the internet to facilitate their activities and maximise their profit in the shortest time. After the USA and China, India has the highest number of internet users. So, the rate of cybercrime is increasing rapidly. Criminals are mostly exploiting the speed, convenience and anonymity of the internet, commit various criminal activities and pose a real threat to victims all over the world. These "cyber-enabled" crimes are not necessarily new - such as theft, fraud, illegal gambling, and the sale of fake medicines, drugs, arms, etc – but they have taken on a new dimension.

Cybercrimes have become an increasingly large problem in our society both in the proliferation of crimes and associated impact on victims through financial loss, invasion of privacy, and even blackmailing. Growing Cyber threats such as identity thefts, phishing, cyberstalking, social engineering,

online scams, hacking, malware, ransomware, cyber terrorism, espionage, and other cyber-related crimes are affecting citizen's lives more than ever before. Further, cybercrimes against women and children are on the rise nowadays, and they have been drastically victimised in the cyberspace.

Criminals of the World Wide Web (WWW) exploit internet user's personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services. They even gain access to classified government information. Social Media remains a favoured target for them to spread scams and fake links. Every year several lakhs of citizens of our country are affected by cybercrimes, suffering huge personal and monetary losses. Cyberattacks on individual citizens, communities, and organisations can have instant and far-reaching consequences for the nation's economic security interests. The number of cyber cases registered by various police units in India is alarming on the rise. Cybercrime is one of the fastest-growing criminal activity and affects both individuals and businesses in different ways posing significant challenges for police organisations.

National Crime Records Bureau (NCRB), MHA, New Delhi collected crime statistics under different types of cybercrimes such as Cyber Blackmailing / Threatening, Cyber Pornography, Cyber Stalking, Defamation/Morphing, Fake Profile, Internet Crimes through Online Games, etc., The NCRB recorded 9,622, 11,592 and 12,317 cases of cybercrime in 2014, 2015 and 2016 respectively. In 2017, a total of 21,796 instances of cybercrime were recorded, an increase of 77% over the previous year's numbers of 12,137. Whereas, the 2016 number was only 6% more than the 2015 number of 11,592. The state of Karnataka had the highest rate of cybercrime, followed by Assam, Telangana, Maharashtra, and Uttarpradesh.

The details of cybercrime incidents occurred under different types in Telangana State were recoded as 1205, 1205, 2240 in 2017, 2018, and 2019 (up to November) respectively and are as detailed below:

Sl. No.	Name of the Unit	No. of cases registered				No. of cases detected (Upto Nov 2019)	No. of persons arrested (Upto Nov 2019)
		2017	2018	2018 (upto Nov)	2019 (Upto Nov)		
1.	Hyderabad City	328	428	394	1213	207	124
2.	Cyberabad	255	293	263	282	121	223
3.	Rachakonda	366	187	174	334	60	65
4.	All Cybercrime units in rest of Telangana state (Including CID)	256	297	268	411	144	156
	Total:	**1205**	**1205**	**1099**	**2240**	**532**	**568**

In the category of cybercrime, "Cyberstalking on women and children" is concerned for the complete country, Telangana stood 4th place with 26 cases registered, as against the total number of 542 offences across the country. Under the new crime heads introduced in the 2017 report, Telangana registered 56 cases under ATM fraud, 111 cases under online banking fraud, and 61 cases under OTP frauds. Consequently, Telanagana State stood third in the country in 2017, with a high rate of 3.3 cybercrimes per 1,00,000 population.

In 2017, a total of 11,601 persons were arrested across the country for cybercrime cases, 8,306 were charge-sheeted, and only 162 were convicted. In respect of Telangana, as of today, 2,184 cases were under investigation and 510 cases were under pending trial in the court(s).

1.3. Challenges in Cybercrime Management

The cybercrime is generally increasing and is becoming a prevalent choice of most of the criminals due to the ease, and attackers derive in committing them. These crimes also offer less risk of getting caught as police officials lack knowledge, skills, ability, and resources which can be useful in effective cybercrime management. A few of the major challenges are furnished below

which needs to cater to and thwart the menace of cybercrimes and threats robustly:

i) Anonymity of the accused
ii) Encryption of the data
iii) Safety and security of digital data in cyberspace
iv) Trans-jurisdictional nature of the crime
v) Lack of expert cadre to handle cyber threats and investigate Cybercrimes
vi) Lack of capability to investigate cybercrimes
vii) Absence of tools and resources
viii) Thwarting Dark web markets
ix) Examination of case data suffers from undue delay
x) Inadequate training infrastructure
xi) Lack of platform where central agencies and state police units can collaborate or assist investigation officer in cybercrime cases.
xii) Lack of cooperation from Internet Service Providers (ISPs)
xiii) Lack of awareness among the public about types of cybercrimes and mode of occurrence.

1.4. Need for establishing a dedicated multi-specialised Centre at State level

Telangana State is the one of the top 5 states of the country in terms of technology landscape and Hyderbad is among the world's fastest growting technology hubs having home for global biggies like Google, Microsoft, Apple, Facebook and Uber with over 1.2 Lac crores IT exports annually. Hyderabad City has 50 Lac + Internet Users and it is expected to grow at rapid speed with State's further push of Internet penetration through initiatives like T-Fiber, Digitalization and On-going wireless coverage expantion by leading Telcos.

The use of Information Technology by government organisations has grown rapidly and is now an important part of the operational strategy of government organisations. The number, frequency, and impact of cyber

incidents/attacks have increased manifold in the recent past, more so in the case of government applications, networks, and employees. These cyberattacks are usually aimed at accessing, changing or destroying sensitive information; extorting money from users; or interrupting the normal business processes. While rapid growth in internet and computer technology has enabled economic and social growth, an increasing reliance on the internet has created more risks and vulnerabilities and opened up new possibilities for criminal activities.

Most communications in the new era are dependent on Information & Communication Technology (ICT). The rapid development of technology not only brought convenience to citizens but also aiding cybercriminals to commit crimes through various modus operandi. In view of the growing use of the Internet and Social Media Applications by people and organisations for various aspects, it has become imperative for Police Organisations to address the emerging challenges and protect their privacy, assets, critical information and cyberspace.

Further, Government initiatives such as 'Digital India" and "Smart City" are nation-building endeavours forcing the country rapidly towards a digital economy, increasing adoption digital banking, e-wallets, mobile banking are some of them that are vulnerable to be targeted by the criminals.

Today, the modus operandi by the cybercriminals is also growing in sophistication, frequency and extending beyond geographical boundaries, making it complex to track and sometimes even remediate. Tracking them has become a profound issue both for private and public organisations. In such a scenario, the TS Police has felt that the development of a dedicated multi-specialised centre that is equipped with a special cadre of manpower (a combination of SMEs / digital forensic experts/professionals and select Police personnel), cyber tools, IT infrastructure, etc to combat and handle efficiently the cybercrimes. Further, the police personnel of the units needs to be imparted highly specialised training in multi-disciplinary skills to operate ICT and Cyber tools and understand the concepts of cybersecurity, data security, Big data analytics, Internet of Things and other related areas as per the assigned roles. As such, they can improve their knowledge to

understand the types of cybercrimes and cyber threats, and the skills & ability to tackle the cybercrimes in an effective and efficient manner.

Mitigating and eradicating cyber threats affecting the community cannot be achieved by just using technology and its' services. It has to be coupled with a robust and up-to-date cybercrime investigation and security framework to counter the dynamic nature of ICT environments and Cybercrime manoeuvres.

Now, the TS Police has been realising the importance of having an in-depth understanding of cybercrimes along with paradigm shift of use cases and technology evolution to counter the emerging cyber threats that are rendering the traditional investigative mechanisms ineffective and its management. Police units are collecting data related to crimes at an exceptional rate. This data either pertains to cybercrimes or crimes enabled by technology. The majority of the data is unstructured and is stored in fragmented repositories across the nation leading to its underutilisation.

Cybersecurity consists of technologies, processes, and controls designed to protect systems, networks, and data from cyberattacks. Effective cybersecurity reduces the risk of cyberattacks and protects against the unauthorised exploitation of the systems, networks, and technologies. There is an urgent need to put in place a robust cybersecurity/resilience framework at government organisations to ensure adequate security of their assets on a continuous basis.

Handling cybercrime at state level warrants a concerted, integrated and collaborative framework at the State level which will be finally integrated to the National level. It may consist of components such as leveraging analytics as data to derive the meaning from data trails, sharing of intelligence information, in-depth understanding of emerging technologies and law of the land, etc.

In view of the above, a paradigm shift is imperative in the approach of dealing the cybercrime and its related aspects. Hence, a dedicated multi-specialised centre need to be set up at the Telangana State Police

Headquarters in order to curb not only existing crimes but also to get readiness to deal with upcoming new age crimes in future's digitally driven socities and businesses. Also, it is essential to coordinate cybercrimes, take necessary measures to improve cyber forensic facilities to prevent & control cybercrimes / incidents, expedite investigation & detection of cybercrimes through law enforcement machinery, issue cyber-related alerts/advisories, training of law enforcement officers, etc.

1.5. TS Police Cybercrime Strategy

Facing an increase in threats in cyberspace, cohesive and comprehensive policies are essential in building an effective cyber defence. The changing face of cyberattacks and sophistication of attack methodologies have presented new cybersecurity challenges. The need for individuals and organizations to keep pace and be prepared to prevent and respond to these security risks and challenges is growing.

TS Police recognised the serious threats posed by cybercrime and the necessity to trial cybercriminals. The knowledge, skills, and abilities of the criminal justice system need to improve in order to detect, handle and prosecute cybercriminals. Further, the judiciary must advance their understanding in terms of the technicalities and complexities where cases are brought before courts. It is therefore imperative to develop a coordinated approach in terms of a State Cybercrime Strategy that would cater to these needs.

Accordingly, the State Cybercrime Strategy is constructed to provide a swift response to cybercrime through improved law enforcement capability, effective criminal justice framework, and active international engagement. In addition, a collaboration between all key players in both public and private sectors is essential to safeguard national cyberspace. Six high priority areas have been identified for help in strengthening the response to cybercrime. The details of focussed areas are furnished below:

1.5.1. Development of an effective legal framework to detect, handle, and prosecute cybercrime:

This will facilitate the enforcement of new laws with regard to different types of cybercrimes and its prosecution. It would also provide legal practitioners and judicial officers with the capacity and expertise to deal with digital evidence.

1.5.2. Building capacity to better address cybercrime.

The capacity and capability of police officers, legal professionals, and the judiciary need to be enhanced to deal with the technical aspects of cybercrime such as examination of the digital evidence.

1.5.3. Cyber intelligence and cyber defence

The value of collecting intelligence about cyber threats cannot be under-estimated. To tackle cybercrime, it is important to gather intelligence from the public, businesses and government agencies and disseminate the same in the form of alerts /advice for cyber defence.

1.5.4. Public and Private Partnership

The dynamic participation of the public and private sector is a key component in the fight against cybercrime. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

1.5.5. International collaboration

Cybercrime is an international problem that requires a coordinated and cooperative international response. The aim is to strengthen partnerships against cybercrime by signing multilateral agreements and information exchange.

1.5.6. Advocacy and Public awareness

The public needs to be made aware of possible cyber threats. Education on the responsible use of the Internet and the impact of cybercrimes is key.

Combating cybercrime is a shared responsibility and requires the attention of a broad range of stakeholders to become successful. Accordingly, TS Police Cybercrime Strategy has placed a strong emphasis on cyber training and capacity building to improve law enforcement capability and enhance the criminal justice framework. Also, it is the need of the hour to establish a dedicated multi-specialised centre at the State Police Headquarters, with the objectives mentioned below, for dealing the cybercrime and its related aspects.

1.5.7. Objectives:

i) Act as a cyber nodal agency in the state to fight against cyber-related incidents/attacks to create a secure cyber ecosystem.
ii) Ensure that Law Enforcement Agencies are able to prevent, investigate, and detect cybercrimes/attacks in a more efficient manner.
iii) Provide an efficient framework so as to ensure resilient cyberspace for citizens and the Telangana Government.
iv) Responsible for handling cybersecurity issues and the protection of critical infrastructure.
v) Creation of a culture of cybersecurity through an effective communication and promotion strategy on the risks of cybercrime /attacks.
vi) Conducting regular training programs to spread awareness about cybercrimes to law enforcement personnel/prosecutors / judicial officers/public.
vii) Improve LEAs response to cybercrime working closely with State and National cyber & other technical organisations.

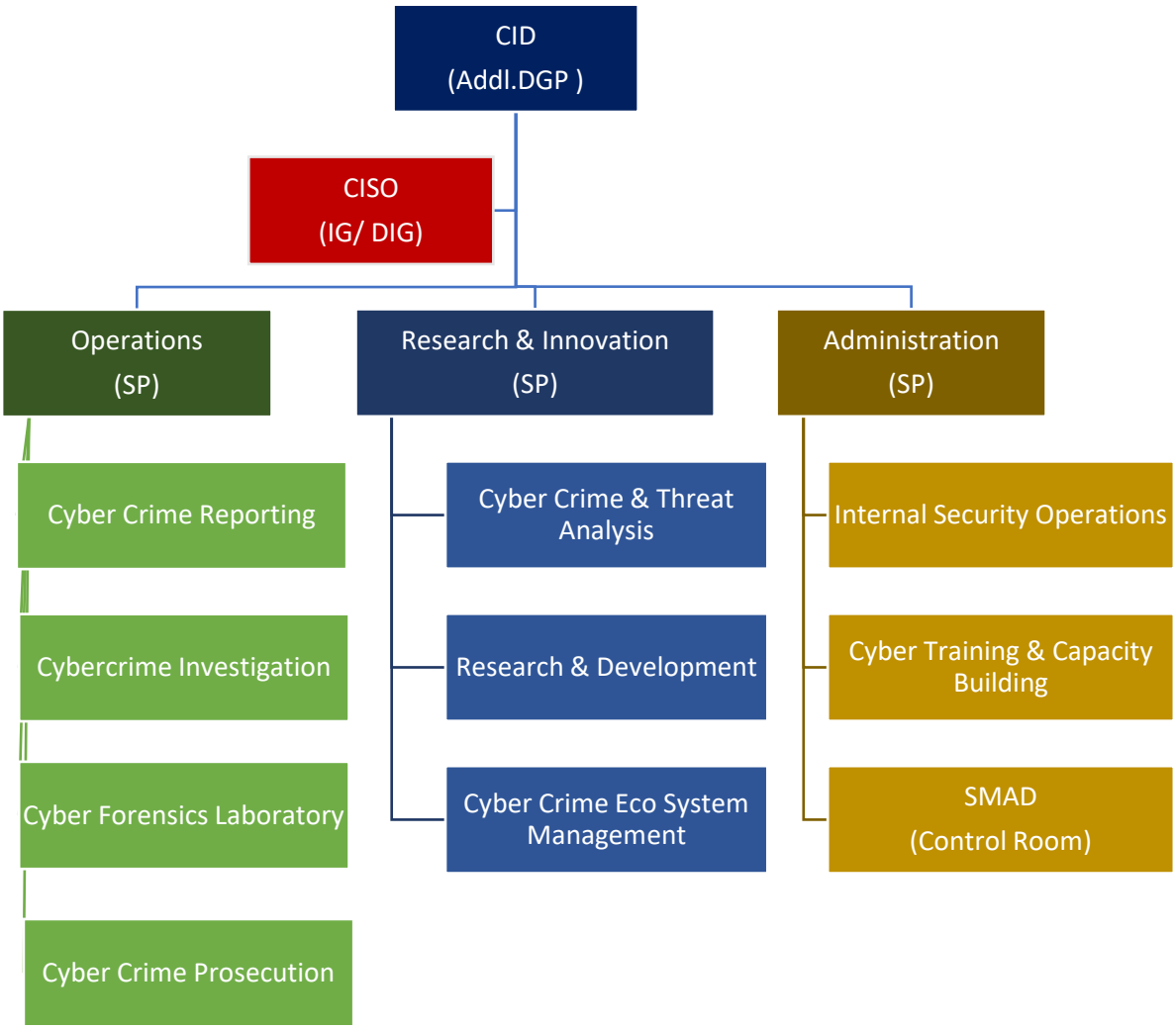
1.6. Framework for Organisational Setting

The legal framework states the moment to set-up cybercrime Centre, the department to which it is attached to, its components, internal orders and regulations, functions and responsibilities, jurisdiction, tasks and relationship with other police units.

The centre will work directly under the administrative control of Addl. DGP, CID, Hyderabad. The centre will be headed by the CISO in the rank of IG/DIG Rank Officer and assisted by three Superintendents of Police in charge of Operations Wing, R&D Wing, and Administration Wing. Each wing consists of related functional components manned by the Police Officers and Cyber Experts/ ICT Professionals.

1.6.1. Structure of the Centre

An effective fight against cybercrime requires a highly developed organisational structure. With having the right structure in place, it will hardly be possible to carry out complex investigations that require the assistance of different legal as well as technical experts.



1.6.2. Internal Orders and Regulations

The orders and regulations will be assigned by the Police Authority and the concerned Ministry, in accordance with the national law. Futher, the centre will have its own internal regulations and functions.

1.6.3. Functions and Responsibilities

Functions and responsibilities that require for creation of a capability to combat criminal use of technology, and in particular, the development of a State Cybercrime Investigation & Incident Reporting Centre are furnished below. Functions and responsibilities may include all or a combination of:

- Investigations
- Collection of data and forensic analysis
- Intelligence collection, analysis, and dissemination
- Assessment and analysis of cybercrime phenomena
- Contribution to drafting national legislation on cybercrime
- Contribution to defining national cybercrime strategy
- Coordination of regional/territorial units
- Specialised support to other police units
- Cooperation with the private sector
- International cooperation
- Prevention of cybercrimes and attacks
- Defining internal procedures
- Training programs
- Development of national reporting systems.

1.6.4. Interagency, public/private and international Cooperation

The State cybercrime centre cooperates with CERT-In and other competent institutions like CFSL, C-DAC etc in order to perform preventive initiative actions in this area or to carry on investigations.

There will be cooperation protocols signed with private companies, NGOs for cybercrimes.

The State cybercrime centre administers the portal for reporting complaints about cybercrimes and threats.

The representatives of the State cybercrime centre participate and organise annual training courses, workshops, refresher courses, round tables with representatives of other institutions responsible in the areas of cybercrime prevention, including the bank sector.

The Office will have direct communication and good cooperation with all the service providers from both public and private sectors such as the ISP's, Banks, Credit Card companies, etc.

The State cybercrime unit serves as the 24/7 point of contact for Telangana State. This centre functions in coordination with the Indian Cyber Crime Coordination Centre (I4C) and territorial subordinated units in Telangana. It should be authorised to

- provide technical advice to the investigating officers / public and private organisations.
- provide for the preservation of data
- provide for the collection of evidence
- provide legal information
- facilitate in identification of the location of suspects and
- send/receive judicial cooperation/mutual legal assistance requests

The centre cooperates with forensic specialised units in investigating criminal offences related to computer systems and data as well as in collecting and securing electronic/digital evidence of the criminal offence, frequently through I4C and cooperates accordingly with the requesting jurisdiction.

1.7. Main components and functionalities -

i) Cybercrimes and Threats Analysis Division
ii) Cyber Crime / Incident Reporting
iii) Cyber Crime Investigation Division
iv) Cybercrime Forensic Laboratory
v) Cyber Training and Capacity Building Division

vi) Cybercrime Ecosystem Management Division
vii) Cyber Research and Innovation Division
viii) Internal Security Operations (includes Risk assessment & Mitigation)
ix) Situation Monitoring & Analysis Division (Control Room)

1.7.1. Cyber Crime and Threat Analysis Division

Monitors regularly the criminal activities such as online fake news, online frauds, identity data thefts, social engineering of people for cheating, fake products selling, and advertisements of fake e-commerce sites which carry out on social media. Further, conducts close monitoring of Dark Web to curtail criminal activities such as online hawala, trading on arms, narcotics, and organs, trafficking of woman & children, sale of identity data and details of Credit & Debit cards, etc of the organised syndicate. The data collected will be analysed and shared with the concerned to facilitate them to reduce cybercrimes and arrange proper preventive measures to control untoward incidents.

1.7.2. Cyber Crime/Incident Reporting Portal

This portal facilitates victims/complainants to report cybercrime complaints online. This portal caters to complaints pertaining to cybercrimes only. The portal also enables citizens to report online content pertaining to the cybercrimes that include online frauds, computer-related offences, data theft, cyberstalking, trafficking, child pornography, stealing identities, or violating privacy and cybercrimes against women and children and victimising them on cyberspace. Complaints reported on this portal will be dealt with as per legal provision by police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing a complaint about initiating action.

1.7.3. Cyber Crime Investigation Division

A first responder will always be law enforcement agents. The investigation officers who are tasked with responding to incidents of cybercrime will conduct cybercrime investigation and will be supported

by the digital forensics expert, private expert investigator, and information technology specialist during the process of investigation. The national investigation agency as well as to conduct cybercrime investigations. Search and seizure practices for Information and Communication Technologies (ICT) will be in accordance with the national law, and the methods used to obtain digital evidence from ICT will be valid and reliable to ensure its admissibility in a court of law.

1.7.4. Cybercrime Forensic Laboratory

The field of cybercrime investigation is growing, especially as law enforcement and legal entities realise how valuable Cyber Forensic Laboratories are when it comes to investigation procedures. The laboratories need to be equipped with requisite cyber tools and manned by both experts/professionals and law enforcement agents who have technical skills in tracking malicious online activity.

Forensic Laboratory will conduct digital forensics process which involves the: search, acquisition, presentation, and maintenance of digital evidence; description, explanation, and establishment of the origin of digital evidence and its significance; the analysis of evidence and its validity, reliability and relevance to the case; and the reporting of evidence pertinent to the case. Various digital forensics methodologies have to be developed and adopted. There is need to develop a model Integrating Digital Forensic Techniques into Incident Response: the collection phase, which includes the identification of evidence at the scene, and its labelling, documentation and ultimate collection; examination phase wherein the appropriate forensic tools and techniques to be used to extract relevant digital evidence, while preserving integrity are determined; analysis phase whereby the evidence extracted is evaluated to determine its usefulness and applicability to the case.

1.7.5. Cyber Training and Capacity Building Division

Cybercrimes/threats cannot be investigated or dealt with by police officers as other traditional crimes. The officers who have undergone

highly specialised training in multi-disciplinary skills will understand the type of cybercrime/nature of the cyber threat and investigate or counter them in an effective and efficient manner. The Investigation Team will have adequate knowledge and ability to take forward the investigation, detection and prosecution processes.

Strategic planning and developing training schedules including awareness campaigns/programs, refreshers courses and workshops around the year for improving cyber knowledge and cyber skills are essential for police officers and the support staff (Incident handlers). Develop a well-defined citizen awareness programs for students at educational institutions, citizens at community centres, and employees at public/private organisations across the state, as a proactive mitigation initiative. Further, awareness about cybercrimes and cyber hygiene will be delivered to the citizens and police officers through a web portal and police social media apps.

Virtual Training with Hands-on Lab- Physical distances and the lack of resources make it difficult to gain more knowledge and also for seamless training. Also, qualified instructors are always a scarce resource today. Hence the solution to this problem is a "Virtual Lab". The virtual lab is easy to set up, use and maintain; with a notable reduction in cost and effort. The interactive nature of the virtual training lab enables the optimal conditions for knowledge retention and also cases of training.

Virtual training labs are cloud-based training environments that emphasize an online, hands-on learning experience over a passive classroom-based environment. Without the need for physical travel, virtual classrooms are more convenient for both the audience and instructors. Virtual sessions and lessons can be accessed from anywhere around the world using a simple web browser.

*Knowledge / Content Management***-** Knowledge Management has to be applied to cybercrime investigation. Knowledge Management has to be promoted as a way to deal with the obstacles to cybercrime

investigations that concerns the human & technical resources, and the knowledge, skills, and abilities need to conduct these investigations. Knowledge Management is essential to create, safeguard and put to use a wide range of knowledge assets such as people and information to improve process or outcome. Knowledge management involves the identification and assessment of knowledge needs for general and specific cybercrime investigations. Comparing the knowledge needs and the current knowledge possessed by investigators, knowledge gaps can be identified. Further, Knowledge sharing is an integral part of knowledge management in law enforcement, it includes both outside forces that push knowledge to others through education and awareness campaigns/programs and inside factors that drive others to seek knowledge, such as seeking out expertise or assistance on a matter.

There are two forms of knowledge that are to be managed and shared: explicit knowledge and tacit knowledge. Explicit knowledge is formal knowledge that is collated, documented and easily defined (e.g. documents, cases, laws, etc). Content Management Portal which needs to be created to house explicit knowledge, manage cybercrime, and cybercrime investigation knowledge by making it available on a website and/or searchable database. This portal also includes a directory of competent national/state authorities/agencies (NCFL and associated Central Forensic Science Laboratories, CDAC, etc) that can obtain, respond to and process mutual legal assistance treaties, case law, legislation, and a bibliographic database. It also includes a repository of cases laws, legislation, and lessons learned in cybercrime investigations.

1.7.6. Cybercrime Ecosystem Management Division

Cybercrime is no longer a one-man operation. Within the cybercrime underground, an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack life cycle.

Development of Cybercrime ecosystem management is imperative to monitor and understand how cybercriminals operate, what drives them, what techniques they use and how the regular internet user is part of the cybercrime ecosystem. The technical details and up-to-date research on the threat landscape facilitate a more realistic understanding of why cybercrime is a problem and how this can be prevented. As such, there is a need to develop a cybercrime ecosystem that brings together academia, industry, and government to operate, investigate a cybercrime basis established standard operating procedure, understand the impact of cybercrimes, and respond to cybercrimes in an efficient manner. This unit also provides incubation support for the development of all components of the cybercrime combatting ecosystem. Hence, the necessary budget/funds need to be allocated regularly every year for the development of the cybercrime ecosystem with the support of academia and industry.

1.7.7. Cybercrime Research and Innovation Division

Research and Innovation are needed to develop new technologies and ways of working that can make the practitioners more effective: those who are directly called up on to respond to security challenges which include cybercrimes (illegal trafficking in people and goods), threats as well as those working in prevention. It is also about developing insights that keep decision-makers well informed. Research & innovation is needed to keep pace with fast-moving developments in the realm of cybercrime, and to enable law enforcement to take advantage of new technologies.

Close partnerships with industry, academia, and research community are required – grouping for which security research projects are ideally suited.

Research & innovation targeting cybercrime and threat need to be allocated required budget/funds regularly every year.

1.7.8. Internal Security Operations Division

Internal Security Operations (ISO) Division is a centralised location where IT technicians directly support the efforts of remote monitoring and management software. ISO teams are heavily utilised in the managed IT services space, and a tremendous driver of service delivery for many managed services providers (MSPs). Technical teams keep a watchful eye over the endpoints that they monitor and manage, independently resolving issues they arise and take preventive steps to ensure many issues do not occur.

While known threats are detected and blocked by the solutions that exist, there happens a significant risk of unknown threats bypassing these controls and breaching the network either causing downtime due to next-generation malware or ransomware or by the hack of critical resources either through insider threats or external entities. With the increased sophistication of attacks, police organisations need to detect and respond to these emerging advanced threats.

Network Security Operations Unit will support/conduct some of the following critical tasks:

i) Network Operations Monitoring
ii) Network vulnerability assessment
iii) Identify suitable applications dynamic scans and proxy tools
iv) Provide security threat intelligence that could be directly integrated into SIEM for real-time.
v) Perform advanced threat hunting on network and end-points to detect advanced attacks.
vi) Provide services like Web application monitoring & site validation and Email accounts monitoring and verification in the deep web.
vii) Cyber Security Training

Further, the ISO team will configure and implement the Security Incident & Event Management (SIEM), and Threat intelligence solutions at CoE Cyber Safety locations. The teams will also go to / access remotely all CoE Cyber Safety locations, and configure the tools for all

critical systems like Servers, Routers, Switches, and Firewalls. It performs Vulnerability Assessment and Penetration Testing periodically with internal and external expertise to minimize the attack vector and organization to patch the vulnerabilities proactively.

1.7.9. *Situation Monitoring & Analysis Division* (SMAD)

It is an advanced Situation Monitoring & Analysis Division having capabilities of data analysis and situation/incidence monitoring need to be set up to function in tandem with Cyber Forensic Labs. During the normal course, both the Cyber Forensic Labs (CFL) and the SMAD function as independent entities. But, in time of need, both the components will work jointly to yield productive results and for seamless execution of operations. The coordination between the two components will improve the accuracy of the analysis results.

The SMAD needs to be equipped with a big Video wall with six sets of monitors supported by Intelligent Control Table fitted with high processing Workstations for analysis of various types of live feeds and crime data. This facility will have the capability to analyse data generated or received from various sources such as CCTV, Social Media, Electronic Media, Police applications, Police Station Data, etc. This Centre will also have the facility to view various types of data at once on the video wall and perform big data analytics on them. This allows the investigation teams to view different types of data in one place and also helps them to have a better grasp of the situation for better decision making. The SMAD can also be used as monitoring, controlling and mitigation unit during emergency situations by the Senior Officers.

The SMAD will be networked with all Cyber Forensic Labs in the District/Commissionerate headquarters established under Centres of Excellence (CoEs) for live crime scene data analysis and will cater to the cybercrime investigative needs of the Investigating Officers and staff of the concerned vertical.

1.8. Staffing the Centre

The Officers working in the State Cybercrime unit need to be carefully selected and included in ongoing training programs. The officers should have knowledge of Computers, the Internet, Police Investigation, and Legislation governing cybercrime. Depending on their functions, they should have qualifications, mostly in criminal investigation and ICT.

The structure of the centre has to be considered and a distinction has to be made between the officers who will perform the investigation in various areas and the officers who have knowledge about computers and legislation, but also subject-matter knowledge.

The method of selection and positioning the personnel for investigation or computer forensics is critical factor for effective functioning of the centre. The private sector may have qualified experts. However, public salaries are usually not competitive enough to attract them to serve in a cybercrime unit. On the other hand, many young police officers may know about computers and be motivated, but they may not have sufficient investigative experience.

The fluctuation of personnel is a major problem affecting cybercrime units. Over time, the best investigators often move to private companies with much higher salaries. This is a reason to keep selecting new officers preferably young ones who are computer passionate and to provide them with ongoing ICT and cyber training courses.

For staff dealing with computer forensics, different selection criteria need to be applied. They must be specialised in their work, but they do not necessarily have to be police officers.

S.No	Wing / Division	S.P	DSP	Inspector	SIs	PCs	Forensic Experts	Prosec-utors
I	**Operations Wing**	1						
	Cyber Crime/Threat Analysis		2	2	4	15		
	Investigation Division		1	1	2	4		
	Cyber Forensic Laboratory		1	2	4	6	3	
	Prosecution Division							4
II	**Research & Innovation Wing**	1						
	Cyber Crime & Threat Analysis Division		1	2	4	10	2	
	Research & Development Division		1	2	2	4		
	Cybercrime EcoSystem Management Division							
III	**Administration Wing**	1						
	Internal Security Operations Division		1	2	2	10		
	SEIM Division		1	2	2	10		
	Cyber Traning & Capacity Building Division		2	4	8	10		

Presently, some scant dedicated staff members are working in the State Cyber Police Station which is under the administrative control of CID.

As of today, there is no multi-dimensional specialised cybercrime centre in the structure of the Telangana State Police Organisation which can coordinate the efforts/activities related to cybercrime investigation, detection, and prosecution, etc.

1.9. Budget Eestimates

Financial implications estimated for setting up a comprehensive centre with the above-mentioned components and making it completely operationalise at State Police Headquarters are proposed with an outlay of Rs. …… . . over five financial years under MOPF Scheme, starting from 2020 – 2021, with Rs.. . . . . Since the development and stabilisation of the centre in one go is difficult, this scheme will run in the next 4 years i.e 2021 – 2025, accordingly, a perspective plan has to be prepared for sanction of funds under MOPF Scheme.

Under the circumstances stated above, there is an imperative need to set-up a comprehensive centre to coordinate various efforts pertaining to cybercrime prevention and regulation in Telangana State. It will provide necessary assistance/support to police officers in the investigation and combat cybercrime. It also facilitates police officers and investigating officers in taking legal action as per the provision of law against cybercrime offenders. The centre helps in strengthening the law enforcement response to cybercrimes and to protect citizens and businesses. Further, it is especially aimed to spread awareness on cybercrimes for both public and police personnel.

ANNEXURE - I

Overview of Capacity Building from the perspective of TS Cybercrime Strategy

Capacity building as an approach to cybercrime has a number of advantages. It responds to needs and produces immediate impact, favours multi-stakeholder cooperation and contributes to human development. The National Cybercrime Strategy stresses the importance of building capacity on different levels of the institutions dealing with cybercrime. The proposed recommendations are as follows:

[*Cybercrime Investigation*
The investigation of crimes involving technology requires that new knowledge and skills are acquired by those tasked with the investigation process. A comprehensive capacity building program to be developed to enhance the cybercrime investigation expertise within the units under Telangana State Police dealing with cybercrime.

Forensic Examination of Digital Evidence
A forensic examination of digital evidence is a key component in the investigation and prosecution of cybercrime. This process requires trained staff due to its fragile and easily tampered nature. The strategy proposes specialised training programs in digital forensic skills for police officers.

Cybercrime Assessment Exercises
Cybercrime Assessment Exercises in the form of cybersecurity drills will be carried out to assess and evaluate the capabilities of law enforcement agencies and the other stakeholders dealing with cybercrime. It is also an effective way to join forces in combatting cybercrime at National and State levels through information sharing, investigation and capacity building.

Educational Campaigns
As part of the "Cyber Smart Programme", educational campaigns targeting diverse groups in society will be organised to raise awareness on cybercrime issues and the measures required to protect it.

Promotion and Development of Best Practices on Cybercrime

To encourage businesses to adopt practices aimed at promoting secure online behaviour throughout the wider community, the distribution and development of low-cost tools need to be promoted to help businesses to prevent and detect online threats.

Combating cybercrime is a shared responsibility and requires the attention of a broad range of stakeholders to become successful. The TS Police has placed a strong emphasis on capacity building to improve law enforcement capability and enhance the criminal justice framework. The implementation of the capacity building programs mentioned in Annexure-I on cybercrime will certainly build a better protection framework.

Criminal Justice Agents such as a) Police Officers, Investigators, Incident handlers, and b) Prosecutors and Judicial officials are responsible for the prevention, mitigation, investigation, detection, prosecution, and adjudication of cybercrimes.

a) Training for Police Officers, Investigators & Incident Handlers

Police are the first responders in cybercrime investigations and responsible for **Securing** digital evidence at the **Scene** of cybercrime. Sometimes in the local areas, the first responder can be a digital forensics expert, an information technology specialist or another person, an employee in the workforce, who is tasked with responding to incidents of cybercrime.

The police officers require specialised knowledge, skills, and abilities beyond those required to investigate, prosecute and/or adjudicate (offline) criminal cases. The police officers should be able to investigate cybercrimes and/or other crimes incidentally involving Information & Communication Technologies (ICT) and properly handle ICT during the investigation. The police organisations have limited abilities to investigate cybercrimes due to a lack of specialised knowledge, skills, training, human and resources.

b) Training for other Criminal Justice Agents

Other Criminal Justice Agents such as prosecutors and judges, also requires specialised knowledge of cybercrimes and digital forensics for those who focus on

criminal procedure law and evidence as applied to computers and related devices. Like police officers and Investigating officers, the sufficiency of training of prosecutors at the local level and judicial officers varies. The need to be well equipped with knowledge and skills to prosecute cybercrimes. Judiciary training is needed on basic cybercrimes, and digital forensics information, expert testimony on cybercrime matters, and digital evidence admittance in a court of law.

Some of the trainings required initially are need to be designed to master an overview of knowledge, skills, and techniques for cybercrime investigation such as how to identify, respond and investigate cybercrimes which are required by Police Officers, Investigators, etc.

Capacity Building with Virtual Labs with Hands-on

This project deals with Virtual Labs which is capable of potentially providing training to law enforcement officers with a hands-on learning experience on Cybercrime interstation and Digital forensics in support of an online educational offering. This Virtual Lab offers a significant instructional advantage in delivering a cost-effective and flexible hands-on learning experience. This effort is also a force-multiplier for the different stakeholders from LEA who are to face the challenges of present-day cybercrimes, cyber investigation, and cybercrime resilience

Benefits of Virtual Training with Hands-on Labs:

There are many challenges while imparting practical training on Cyber Forensic tools at multiple locations as their tools are mostly "server-based", "Non-portable", "locked to specific hardware", "version-controlled" and also "expensive".

Hence, the virtual lab with web access is the solution which can ensure the following

- A single place of installation
- No additional cost of licensing
- Availability of updated/patched tools

- 24x7 access over the internet connection
- Concurrency of usage, by providing session/instance based login for students/learners simultaneously
- Cost-Effective
- Rapid version control and availability to users
- Installations of tools available on optional hardware or compatible OS

Courses in Virtual Lab:

- Certified Cyber Crime Investigator
- Digital Forensic Investigation
- Cyber Crime Awareness

The virtual cyber lab entails the following objectives for better performance:

Accessible, secure and seamless connectivity will be provided to the remote virtual cyber labs. This ensures that the trainer is available for consultation at any time of the day, based on the trainee's convince of accessing the lab, which is otherwise available 24x7, 365 days a year throughout the course.

The otherwise cent percent reliable remote virtual server will serve a significant number of concurrent users with scaled-down dedicated resources. No significant delay will be observed even if a large number of concurrent users access the lab.

The Virtual Machine (VM) will be configured with the appropriate operating system(s) including the required security tools to support lab exercises.

Trainees will have privileged/access rights on the virtual machines to execute security or network tools. Note that this implies that trainees may potentially exploit the system resources intentionally or unintentionally. As a result, the virtual lab environment will be monitored to avoid these adverse consequences and remedial measures implemented immediately at the VM end.

Value addition and Force Multiplier aspects:

The virtual lab is a web-enabled cloud-based environment, with access to it based on security credentials provided for login to the participants. Hosting the lab on a cloud enables users, service providers and the facilitator with many advantages. It not only increases efficiency but also drastically reduces the cost of ownership and operation cost.

To understand the value additions and the very fact that this virtual lab has its own merits, the following are ceratin enumerated below:

Up-market Training- The availability of "virtual lab" with the up-market tools on the cloud, will facilitate the "Training Facilitator" to demand the 'updated' and 'up-market tool' training without worrying about internal infrastructure augmentation and extensive planning.

Cost of Ownership- The Training Facilitator need not incur on the requisite tools at the onsite facility for imparting training.

Infrastructure Cost- The tool and lab environment requires a specific configuration of hardware. The advantage of this 'Virtual Lab' model will be well implemented as the training facilitators need not go for the procurement of optimal hardware to install the tool (that is used for training) or need not invest in continued 'Hardware Upgrade' to host the tools.

Elevated collaboration Model- All stakeholders involved in the training, can extract the best as the roll-over and conduct of training through the 'Virtual Lab' will provide the latest in the market with the most updated version/feature that is trending in the environment.

No Constraint on Hardware Machine/Storage- The advantage of the 'Virtual Lab' provides for no restriction of Hardware control and also augmentation of storage space, as this is the aspect to be addressed by the service provider and the exploitation of the cloud features.

24x7 Access- Virtual labs are available to the training stakeholders at their convenience. Hence, the virtual lab offers a plethora of advantages.

Offsite Access- The Lab facility to the trainees is available on a virtual/cloud-based ecosystem. Hence, the trainees can carry-over the 'Hands-on' training facility beyond the classroom at their own convenience.

Feature of Fail-over- The Virtual Lab access is web-enabled and if the trainee encounters any problem, he/she can switch over to the next available IP address/alternate domain, to continue his/her training.

Easy to protect IPR/Licence integrity/Theft of license- The Virtual Lab has its own advantage of protecting the spurious installation or theft of the expensive tool elsewhere.

Easy to Manage- The 'Virtual Lab' can be maintained for updated patching/upgrade. Also, the lab is best available all across the web irrespective of the trainee/training location.

Ease of Security- The security of the 'Virtual Lab' is at its best, as the login is based on individual user credentials and all the user is logged. Further, the Session/ Instance/Username based access can also be monitored and suspended based on policies.

Uninterrupted Service- The Virtual Labs is based on internet-connectivity. In case of interruption, the uptime to restart the services will be minimal as the same environment can be provided through as DR (Disaster Recovery) or mirror site.

Compliance- For the Training Facilitator and the service provider, the cost of the ownership and compliance to all Protocol and Laws is made easy in a 'Virtual Lab' Environment.

Cost Factor- Since the license required is minimal and that the multiple users are all based on the Concurrent Usage Licence Model. The envisaged training can be done at a lower cost, that otherwise could have been exponentially higher.

Optimisation of Resource- The 'Virtual Lab' also facilitates the philosophy of "Optimal Use of Resources". One ecosystem of 'Virtual Lab' based on cloud is accessible by all participant's pan-web. Also the 'System Administration' is also

centralised and can be managed/ administrative from a web console form any location.

Establishing an eco-system for providing the 'one-of-a-kind' Training environment for the Cyber Security/ Digital Forensics domain for all the stakeholders in an innovative way through the use of 'Virtual Labs' comes with a lot of value addition and advantage.

Courses Planned

A) *Certified Digital Crime Investigation Professional for Law Enforcement/Police Officers*

Considering the rapid increase of ICT in all walks of life, most of the crimes now have an element of misuse of computers, smartphones, communication networks, etc. These technologies are increasingly being used by criminals in committing conventional crimes. Increasing the use of the internet and social media resulted in a plethora of varied crimes being committed in the cyber domain. Therefore it has become imperative for the law agencies to have an in-depth understanding of the working of the cyber domain and the modus operandi of crimes being committed therein. The understanding can't be limited to a few specialist investigation officers, but it is a must for all police officers, especially those who act as first responders to victims of crime and recording them.

This course has the following 10 sessions including 16 practical labs that provide a better understanding of crime investigation.

- Introduction to Computers
- Introduction to Cyber Crimes
- Scene of Crime Management
- Web and Email Investigation
- Social Media Investigation
- Communication device based Investigation
- Mobile Forensics
- Investigation of financial frauds & Cyber Crimes
- Investigation Abroad
- Cyber Laws

Key Learning Objectives

- ✓ Understanding the different types of cybercrimes.
- ✓ Able to conduct a computer-related crime investigation.
- ✓ Investigating a fake profile in social media and to recognize the phishing mail/link.
- ✓ Perform mobile-related crime investigations.
- ✓ Understanding and apply the cyber laws as per IT act

Certification (Optional)

At the end of the course, certificates endorsed by the eminent body in cybersecurity shall be issued to the participants. The certified trainees will be able to handle the cybercrime cases as per IT Act.

B) *Digital Forensics Investigation*

Now a day's computer crime continues to escalate. As more cybercrimes get reported, more investigation techniques and qualified forensic investigators are needed. This Course endeavours to enhance the technical understanding and hands-on practice of the forensic techniques and processes for solving the cases. Almost all financial fraud or employee misuse cases involve a very strong element of computer-based evidence. This course can be done by anyone who wants to make their career in the field of digital forensics.

This course has the following 10 sessions including 10 practical labs that provide a better understanding of crime investigation:

- Introduction to Digital Forensics
- Cellular communication technology and protocols
- Mobile Operating Systems
- Mobile Device Artifacts
- Mobile Forensics Fundamentals
- Extraction Techniques
- Logical & Physical Acquisition of data
- Android Forensics
- Computing Device Forensics

- Network Device Forensics
- Cloud Forensics

Key Learning Objectives

- ✓ Understanding the basics of Mobile Forensics
- ✓ Artifact analysis
- ✓ Understanding mobile-related artifacts
- ✓ Understanding the extraction techniques
- ✓ Ability to analyse the evidence.
- ✓ Ability to recover the data from evidence (material objects).
- ✓ Capable of using different types of tools in investigating digital evidence.
- ✓ Able to understand how the investigation process carries out.
- ✓ Capable to detect malicious activity in a system.
- ✓ Incident Response in an Enterprise Environment.
- ✓ File system Structure and Analysis

Certification (Optional)

At the end of the course, certificates endorsed by the eminent body in cybersecurity shall be issued to the participants. The certified trainees will be able to handle the cybercrime cases as per IT Act.

C) *Cyber Crime Awareness*

In this globalization era, individuals face a multiplicity of challenges in recognizing IT security concerns and respond accordingly. Current technology has given us access to a huge amount of information on network, web, mobile & tasks like e-governance, banking services, etc. Taking time to assimilate on how to stay protected in our ever-expanding digital lives is one step we can take to become more cyber aware. The more aware we are, the more precociously we can bounce back when the cyber-attacks occur. This course aims to develop skills to secure cyberspace from various cyber threats. Experts herein share their knowledge on the principles, state of the practice and strategies for secure cyberspace.

This course has 17 sessions including 10 practical labs that provide a better understanding of crime investigation.

Topics

- Introduction to Cyber Security
- Cyber Security Threats
- Phishing & Preventive Techniques
- ATM/Debit/Credit Card Security
- Social Media Security
- E-mail Security
- Social Engineering
- Password Management
- Malware & Ransomware
- Data backup and Recovery Techniques
- System Patch Management
- Usage of Public WiFi
- Secure Communication over the Internet
- Laptop/Desktop Security (Anti-virus, Firewall)
- Mobile Security
- Cyber Laws & Internet Ethics
- Cyber Security best practices and recommendations

Key Learning Objectives

- ✓ Provide the roles & responsibilities of each individual on Cyber Security space.
- ✓ Gain a comprehensive knowledge of Cybercrime threats and solutions
- ✓ Protecting sensitive information of organizations
- ✓ How to avoid information disclosure in social networks?
- ✓ React when an incident happens
- ✓ Protecting personal devices and information
- ✓ Understanding of applicable cyber laws
- ✓ Best practices to avoid Cyber Security issues

Certification (Optional)

At the end of the course, certificates endorsed by the eminent body in cybersecurity shall be issued to the participants. The certified trainees will be able to handle the cybercrime cases as per IT Act.