Training for investigation and prosecution of

New and emerging Crimes

Introduction:

There is no universally acceptable definition of new and emerging crimes. As these crimes are still nascent and evolving, the definitions if attempted, need regular amendments. To distinguish the 'new and emerging' crimes from the 'traditional' the following discussion is essential.

i. 'Traditional Crime' (like homicide, robbery, theft/burglary, falsification of account books etc.) has declined sharply in recent decades in developed countries including US and UK. But new types of crimes—many of them enabled by computer technology—have begun to proliferate. Criminals are using technology to invent new types of crime, and are creating new methods for committing traditional crimes.

ii. New crimes, like "ransomware," (a type of online attack that blocks victims' access to their computers until they pay a ransom), "sextortion" (sexual exploitation, in some cases by blackmailing victims with the threat of disseminating sexual images of them) and synthetic identity the (taking pieces of information from multiple people to create an entirely new, fictional identity that can often be exploited for long periods of time) have become a billion-dollar-a-year enterprise. Moreover these new crimes like Phishing, trolling, malware, online scams, revenge porn and the child sexual exploitation largely remain unregistered and undetected.

iii. Technology is changing how some long-established types of crimes are committed today. For example, drug dealers are discovering they can move larger quantities of illegal drugs more easily and with less risk via "dark web" internet marketplaces and postal mail than they can by selling drugs on the streets. [1]

[1] The Changing Nature of Crime And Criminal Investigations, January 2018, Police Executive Research Forum, Washington, D.C. 20036

iv. Nearly every type of crime today has a digital component. Investigators today are encountering a wide array of digital data captured by a variety of devices—smart phones, laptops and tablets, GPS systems, Fitbits and other wearable technologies, closed-circuit television, and the growing body of “Internet of things” devices. Likewise, future technologies, such as driverless cars, virtual reality and implant technology, will pose new risks and opportunities for the police service.

v. Digital evidence being latent, volatile, time-sensitive and most often, foreign located, poses significant challenges to the Law Enforcement Agencies (LEAs). New technologies like Encryption often restrict/prevent police access to information as well as evidence in digital space. At times, even with the assistance of service providers and a court order, police may not be able to access encrypted data.

vi. Criminals are exploiting technology, and the tools to preserve anonymity online, more quickly than law enforcement is able to bring new techniques to bear. Just as criminals learn to exploit new technologies and invent new *modi operandi*, LEAs need to make use of technological innovation and develop new investigative measures to counter the threat of new and emerging crimes. To prevent, detect and combat the emerging crimes, the LEAs need to acquire critical new skills and build capacities in investigating officers and prosecutors.

vii. All these new and emerging crimes are largely transnational in jurisdiction and organized in nature. Recognizing the threats to global peace and security, United Nations General Assembly on 9 December 1998 resolved to establish a comprehensive international convention against transnational organized crime (TOC).

viii. The United Nations Convention against Transnational Organized Crime (UNTOC) was adopted by General Assembly on 15 November 2000. It entered into force on 29 September 2003. India signed and ratified UNTOC in 2011. UNODC is the nodal office wrt UNTOC implementation.

Types of New and Emerging Crimes/TOC:

i. The Conference of the Parties to the United Nations Convention on Transnational Organized Crime (UNTOC) identified cybercrime, identity-related crimes, human trafficking and human smuggling, the trafficking of small arms and light weapons, trafficking in cultural property, environmental crime (illegal logging, illegal mining, illegal fishing, the illegal wildlife trade etc.), piracy (an old form of crime which has re-emerged), organ trafficking, and fraudulent medicine as new and emerging crimes of concern.

ii. No exhaustive list of TOC is drawn by UNODC. Australian Criminal Intelligence Commission classifies Serious and Organised Crime (British and Australian equivalent of TOC) in the following manner.

   a. **Illicit Commodities**
      i. Trafficking of Drugs and psychotropic substances
      ii. Counterfeit Currency
      iii. Illicit pharmaceuticals
      iv. Firearm trafficking
      v. Environmental crime
      vi. Trafficking of Cultural Property
      vii. Intellectual property crime

   b. **CRIMES IN THE MAINSTREAM ECONOMY**
      i. Card fraud
      ii. Export/Import Frauds
      iii. Securities and financial market fraud
      iv. Bank Frauds including technology enabled frauds
      v. Insurance Frauds
      vi. Visa and migration fraud
      vii. Maritime Piracy
      viii. Revenue and taxation fraud

   c. **CRIMES AGAINST THE PERSON**
      i. Human trafficking and slavery
      ii. Maritime people smuggling
      iii. Child sex offences

   d. **Enabler Activities**
      i. Money Laundering
      ii. Cybercrime and technology-enabled crime
      iii. Identity crime
      iv. Criminal exploitation of business structures
      v. Public sector corruption
      vi. Violence

iii. New Crimes have been most prominently discussed in form of Cybercrimes, which have been divided broadly under three heads, namely:

a. **Pure Cybercrimes**

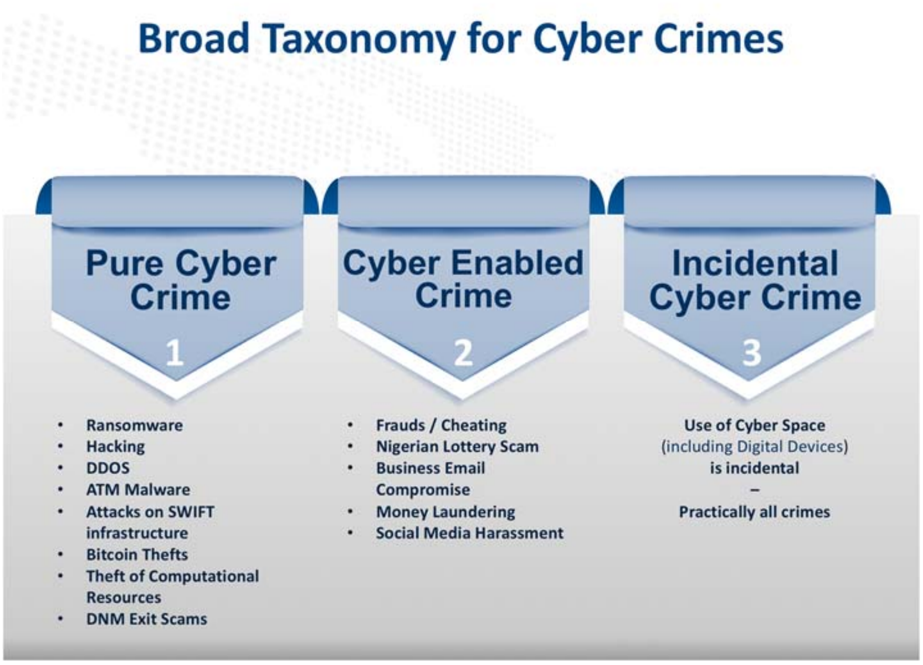
i. Ransomware
ii. Hacking
iii. DDOS
iv. ATM Malware
v. Attacks on SWIFT infrastructure
vi. Bitcoin Thefts
vii. Theft of Computational Resources
viii. DNM (Dark Net Market) Exit Scams

b. **Cyber Enabled Crime**

i. Frauds / Cheating
ii. Nigerian Lottery Scams
iii. Business Email Compromise
iv. Money Laundering
v. Social Media Harassment

c. **Incidental Cybercrime**

Use of some amount of cyber space (including Digital Devices) is incidental for commission of crimes / presence of evidence / presence of victims / presence of suspects – this covers practically all crimes.



Broad Taxonomy for Cyber Crimes

Pure Cyber Crime
1

- Ransomware
- Hacking
- DDOS
- ATM Malware
- Attacks on SWIFT infrastructure
- Bitcoin Thefts
- Theft of Computational Resources
- DNM Exit Scams

Cyber Enabled Crime
2

- Frauds / Cheating
- Nigerian Lottery Scam
- Business Email Compromise
- Money Laundering
- Social Media Harassment

Incidental Cyber Crime
3

Use of Cyber Space
(including Digital Devices)
is incidental
–
Practically all crimes

Roles and Special Skills required:

i. Cybercrime poses a significant challenge to law enforcement agencies worldwide. While it is perhaps no longer a novelty, the ways in which criminals exploit technology are evolving at an increasingly rapid pace, causing serious concern to law enforcement. The latest developments in technology are being adopted by cybercrime networks to shape new, unique and innovative modus operandi with little time lag. The information infrastructure is increasingly under attack by cyber criminals. The number, cost and sophistication of these attacks are increasing sharply. Most of these attacks are transnational by design, with victims spread throughout the world, necessitating multi-jurisdictional or transnational investigations.

ii. Traditional modes of training through books, boards, PowerPoint / PDF-based approach are not very suitable for advanced trainings to combat cybercrime. There is need for more practical training, something based on simulated environments. However, given the need of volumes, the proposed methodology should be scalable.

iii. The challenges of cybercrime trainings can be summarised as:

   a. Traditional PowerPoint/ PDF-based approach not very suitable
   b. Number of officers to be trained (volume)
   c. Inaccurate assessments of needs of Law Enforcement Agencies (LEAs)

iv. The expanding ubiquity, frequency, and severity of cybercrimes entail LEAs to think beyond the one-size-fits-all training strategy. In devising new counter-responses, continual advancement in knowledge and skill of cybercrimes is a core imperative.

v. Capacity-building for LEAs must be seen in the context of boosting the capabilities in these functional areas:

   a. To detect cybercrimes
   b. To receive complaints about cybercrimes
   c. To be a first responder to the complaints about cybercrimes
   d. To register criminal complaints about cybercrimes, with all details

e. To investigate cybercrime cases

f. To do forensic as well as data analytics related to cybercrime cases

g. To collect admissible evidence and launch prosecution in cybercrime cases

h. To prepare and launch public awareness campaigns to prevent cybercrimes

i. To work with researchers, academia and private sector to improve cyberspace security

j. To liaison with international LEAs and service providers

vi. In order to create a suitable training curriculum, we first need to identify what are the roles or professional categories that have duties related to cybercrime investigations and digital forensics, and identify what are the core skills they should possess. Below are the proposed series of roles and skills needed. The roles have been grouped on several tracks in order to structure the training curriculum.

a. Responders Track

b. Forensics Track

c. Investigations Track

d. Intelligence Track

e. Management Track

f. Judiciary / Prosecutors Track

These Tracks, Roles and Required skill sets are described in following paragraphs

I. Responders Track:

A. First Responder Officer can be a PCR Van officer or the Emergency Officer of the Jurisdictional Police Station. He is often the first to arrive on the scene of crime and needs to have an awareness of how technology affects crime, what is digital evidence and how it should be handled.

B. Duty Officer is the Frontline officer that receives and offers first line response to complaints involving crime using technology. He/She needs to assess complaints and respond appropriately to instances of crime using technology and make appropriate referrals where required and/or necessary.

Skills needed:

- Understanding what digital evidence is and what can be found by analysing digital evidence
- Crime scene attendance – identifying, gathering, preserving digital evidence with proper chain of custody.
- Knowledge of current legislation and policies related to crimes using technology including the legal authority to obtain telecommunications information such as subscriber data.
- Knowledge of information technology and how it is used including the internet, email, communication technology, online services including social networking.
- Knowledge of risks for the individual, organisation or investigation when using technology including the consequences of interacting with devices including an understanding of reliability of information and associated risks when relying on uncorroborated information (for example, email header, existence and pseudonyms), exposure of identity and other risks when operating online and risks associated with the volatility of electronic evidence.
- Knowledge of consequences to alteration of dates and time and others that may influence the criminal justice process.

II. Digital Forensics Track:

Digital Forensics Specialist: The main job of a Digital Forensics Specialist is to perform recovery and investigation of material found in digital devices. The Digital Forensics Specialist has a technical background and has to be able to apply knowledge of computer forensic principles in the identification and collection of digital evidence.

Skills needed:

- Advanced cybercrime awareness
- Advanced knowledge of legal and jurisdiction issues
- Processing of digital evidence while maintaining the chain of evidence
- Expert knowledge in one or more forensic areas
- Familiarity with different operating systems and applications and file structures
- Knowledge of relevant commercial and open source tools
- Knowledge of scripting/programming and database querying (SQL)
- Understanding of forensic artefacts and data carving
- Knowledge of both post mortem and live data forensics

- Data Recovery
- Mobile Phone Forensics

Advanced Skills:

- JTAG
- Chip Off
- Memory Forensics
- Malware Analysis and reverse engineering
- Cloud Forensics
- Decryption

III. Investigations Track:

A. **General Investigator** is the police officer that handles criminal cases in a wide variety of police operational units. This investigator handles increasingly more technological related issues regarding the cases that he is required to solve and needs good cybercrime and digital forensics awareness skills.

Skills needed:

- Responders track plus:

1. Technical skills:

- General Cybercrime awareness including types of cybercrimes and other tech enabled crimes.
- Internet basics – URL, DNS, Domain names and IP addresses ISPs.
- Email investigations and other communication technologies including time zones.
- Proxies and anonymous investigations
- Social media and Open Source Intelligence (OSINT)
- Anonymization techniques concepts
- Virtual Currencies concepts
- Digital crime scene examination skills including seizing of electronic evidence, chain of custody and presenting evidence in court
- Mobile applications;
- Malware;
- Preservation of Digital Evidence;
- Modus Operandi;
- Biometrics – Authentication methods;
- Social Engineering;
- Money laundering

2. Legal skills:

- Penal Codes, Procedure Codes, Evidence Acts, Special Laws (IPC, CrPC, IEA, IT Act etc.)
- Requesting and processing subscriber information and data from third parties
- Fundamental knowledge of legal and jurisdiction issues (LRs and MLAT Requests)
- How to present evidence in court;

B. **Cybercrime Investigator** is an investigator, who is specialized in cases involving high technology or very technical aspects such as cybercrime, cyber-attacks, etc. and needs very strong computer networks investigative skills.

Skills needed:

- General investigator pack plus:

1. Technical skills:

- Advanced computer technologies including network security and vulnerabilities, open system interconnect (OSI) and network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS]),
- Knowledge of data interception and traffic analysis methods and performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)
- Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files
- obfuscation/anonymisation techniques,
- common operating systems (file systems)
- network topologies
- virtualization
- logging and analysis

- web technologies
- data storage systems
- encryption methodologies
- Knowledge of content development
- Extract data from local devices
- Malware Analysis at a deeper level
- File formats
- Scripting
- Pattern Analysis for multimedia files
- Ability to engage private sector or other countries to find solutions

2. Legal skills:

- Penal Codes, Procedure Codes, Evidence Acts, Special Laws (IPC, CrPC, IEA, IT Act etc.)
- Requesting and processing information and data from third parties
- Knowledge of the impact of legislation on technology crime-related investigations
- Advanced knowledge of legal and jurisdiction issues
- Individual organizational policies and procedures
- Knowledge of international frameworks, protocols and conventions.
- Advanced knowledge on how to interact with international organizations

IV. Intelligence Track

Cybercrime Intelligence Officers/Analysts are identifying and producing intelligence on cybercrime from raw information; assembling and analyzing multi-source operational intelligence; preparing and presenting intelligence briefings; preparing planning materials for photographic reconnaissance missions; analyzing the results, preparing reports.

They are required to prepare graphics, overlays and photo/map composites; plotting imagery data using maps and charts; providing input to and receive data from computerized intelligence systems; maintaining intelligence databases, libraries and files.

Skills needed:

- Strategic and operational crime analysis
- Big data management and analysis
- Advanced cybercrime awareness
- Analytical and visualization tools

- Computer networking fundamentals
- E-discovery techniques
- Social networks and Open Source Intelligence (OSINT)

V. **Management Track:**

A. **Cybercrime / Digital Forensics Head of Unit (SP / DCP):** These professionals deal directly with cyber investigators and experts. They should take informed decisions in cybercrime cases or in other complex investigations involving cybercrime elements. Their role is to coordinate staff, allocate resources and prioritize policing activities. They should have detailed overview of the capacity, capabilities and needs of the unit and provide it with the relevant training and tools that enable or facilitate investigation and examination of the evidence. Another function is to represent the unit when dealing with external stakeholders.

They need at least a minimum of hands-on practical experience to evaluate operational and strategic activities and the ability to communicate effectively with their staff and external experts.

Skills Needed:

- Profound knowledge of cybercrime and cybercrime offences
- Advanced knowledge of legal and jurisdiction issues
- Knowledge of the institutional framework for international cooperation
- Knowledge of relevant investigating procedures
- High-level knowledge of investigating and forensic tools
- Knowledge of training needs and available resources
- Staff management skills
- Budget management skills
- Project proposal drafting skills
- Relationship management and soft skills
- Communication skills (incl. presentation skills)
- Ability to communicate the needs to higher hierarchy
- Foresight capabilities

B. **Heads of Police Forces (DGP)**are the Law Enforcement Managers, who are responsible for creating and executing strategic initiatives to increase efficiency of policing activities while dealing with obstacles such as legislation changes or staff turnover. They influence key external stakeholders and promote the organization in the media. They establish policies and procedures for the organization to follow and manage and allocate available resources.

This group should benefit from advanced awareness on cybercrime. The actors should be able to maintain an effective working relationship with the head of the cybercrime unit and represent cybercrime policing in the media. At a general level, the cyber related threats, legislation, opportunities and limitations must be understood.

Skills Needed:

- High level cybercrime awareness
- Knowledge of legal and jurisdiction issues
- Knowledge of the institutional framework for international cooperation
- Staff management skills
- Budget management
- Relationship management and soft skills
- Communication skills
- Knowledge management
- Abilities to speak about the unit externally
- High knowledge on polices and local environment regarding cyber
- Awareness on particularities regarding seizure and local procedures

VI. Judiciary Track

A. **Judges / Prosecutors** handle a wide variety of criminal cases. They should get an awareness of how crime can be facilitated by technology and what digital evidence is and how it can be used in a case.

Skills Needed:

- High level cybercrime awareness including concepts of the following nature:
    - General cybercrime awareness including types of cybercrimes and other tech enabled crimes.
    - Internet basics – URL, DNS, Domain names and IP addresses ISPs.
    - Email investigations and other communication technologies including time zones.
    - Proxies and anonymous investigations
    - Social media and Open Source Intelligence (OSINT)
    - Deep Web and Virtual Currencies concepts

- Knowledge of legal and jurisdiction issues
- Knowledge of the institutional framework for international cooperation

B. **Specialized Cybercrime Judge/Prosecutors** are specialized in prosecuting / judging technology enabled crime cases or specifically cybercrime cases. They need specialized cybercrime investigations and digital evidence skills.

Skills Needed:

- Profound knowledge of cybercrime and cybercrime offences
- Advanced knowledge of legal and jurisdiction issues
- Knowledge of the institutional framework for international cooperation
- Knowledge of relevant investigating procedures
- High-level knowledge of investigating and forensic tools
- Knowledge of training needs and available resources
- Staff management skills
- Relationship management and soft skills
- Communication skills

ii. New and emerging crimes, in addition to above, require the knowledge of following domains besides understanding of the *modi operandi* of the above crimes:

a. Criminal Intelligence Analysis and use of various analytic tools including OSINT
b. Use of INTERPOL tools and Databases in Criminal Investigations and fugitive tracking
c. Obtaining foreign located evidence (Mutual Legal Assistance)
d. Seeking Extradition of fugitive criminals
e. Admissible Recovery and seizure of digital evidence
f. Obtaining foreign located Digital Evidence
g. Tracing, attachment and confiscation of proceeds of Crime
h. Undercover Operations (wherever law permits)
i. Lawful Interception (Surveillance) including Telephonic, electronic and environmental surveillance

Training Methodology:

i. There is a strong need for a standardized recognized certification in fighting New Crimes like cybercrime. A large majority of the digital forensics specialists and cybercrime investigators are required to testify in court and so they are constantly being challenged on the basis of their certifications and professional knowledge. There is a need to setup a standardized certification that can be nationally accepted and recognized and which could be presented in courts to further testify for the strong cybercrime investigations, or digital forensics knowledge of the holder.

ii. There is a need to setup a certification system, based on the proposed training system described above. This training curriculum will provide law enforcement officers with three certifications:
   a. Certified in Cyber Fundamentals
   b. Certified Cyber Specialist
   c. Certified Cyber Expert

iii. In order to obtain the Fundamentals certifications, trainees will need to complete the introduction online modules for all the tracks and the classroom based modules from the Basic level for their specific track providing a general overview on cybercrime and other types of online investigations techniques and digital evidence.

iv. In order to obtain the Specialist certification trainees will need to complete all the Core trainings for the specific track they are following and two other modules of their choice, either from the same track or from the others, be it from Core or Intermediate/Advanced levels.

v. For the Expert certification, trainees will have to complete all the core modules for their track plus six other modules, either from the same track or from the other tracks, from Core or Intermediate/Advanced skill sets.

vi. This is a standardized, modular system and certifications need to also be offered to trainees, who have successfully completed training modules delivered by other organizations, law enforcement agencies or academies, as long as they can prove that the modules they completed fit within the framework of the standardized course curriculum and the topics and skills acquired are similar.

vii. This system provides a standardized approach with a curriculum that is modular and highly adaptable to each person`s needs and interests while still providing core fundamental skills needed for each track.

viii. The basic requirements for all the professional tracks should be fulfilled through the online module. **E-Learning modules** using electronic educational technology in learning and teaching, can be utilised for online personalised, interactive or virtual education, enabling dissemination of information and provide knowledge as tool for capacity building and optimizing resources.

ix. The **UNODC Global eLearning Platform,** launched in September 2014 is an example in this area. The UNODC Global eLearning Programme develops learning contents in collaboration with UNODC senior international experts in each specific thematic field. Current security and human threats such as transnational organized crime, illicit drugs, trafficking in persons and smuggling of migrants, and issues relating to border control, forensics and laboratories, controlled deliveries, security and travel documents, intelligence, HIV and AIDS and human rights are covered by 21 courses. During 2014 to 2016, as many as 24, 876 officers from 185 countries (428 from India) are taking benefit of the UNODC Global eLearning Platform.

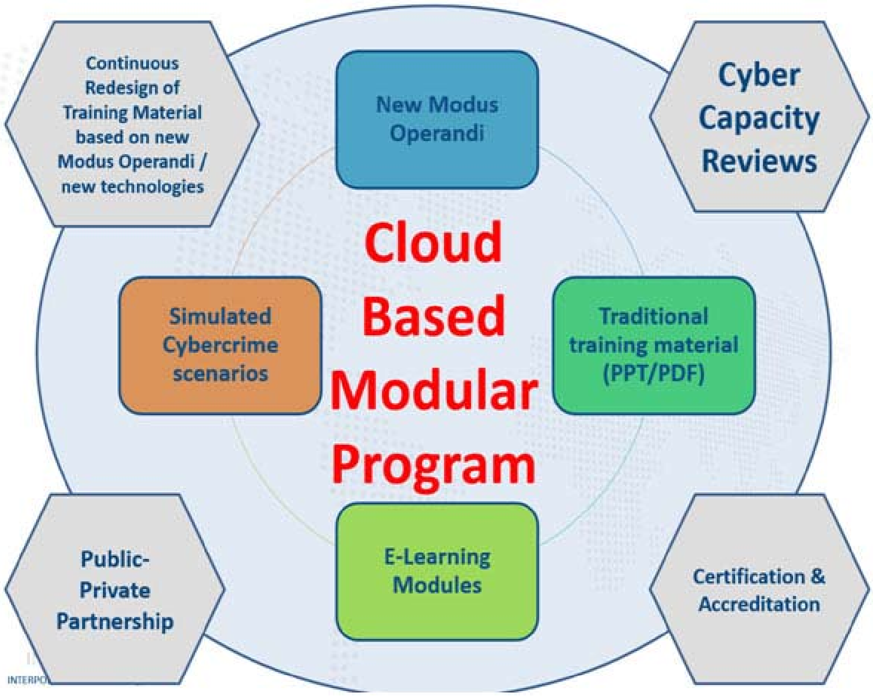
x. The **INTERPOL Global Learning Centre (IGLC)** is a web-based portal giving authorized users access to a comprehensive range of online learning products. The IGLC is aimed at the wider police community across the world. Its goal is to encourage the sharing of knowledge and best practice between INTERPOL member countries as well as providing the opportunity for interactive e-learning. IGLC contains a wide catalogue of e-learning courses as well as an online library of resources with a wealth of links to reports, documents and websites of law enforcement organizations. This is complemented by resources from other relevant bodies such as universities, police colleges, academies and training institutions.

xi. Distance education of Law Enforcement Officers and Prosecutors is also possible through A massive open online courses (MOOCs) and E Books.

xii. Cybercrimes introduce unanticipated risks and effects, creating greater urgency to equip investigators with new skillsets. One such area is the establishment of a cloud computing training platform that comprises a networked and nodal nature, parallel to that of cyber security.

xiii. Cyber Range or Simulated Cybercrime Scenarios are the key component of such a training model. Besides preparation of traditional modes of training through books, boards, power point/PDF-based approach, there is a strong need for more trainings based on simulated environments. This would mean creation of scenarios, including digital exhibits (logs, etc.) for extraction by trainees using forensic tools preloaded on the infrastructure, using appropriate procedures.

xiv. This platform can be pivotal to increase shared knowledge and skills for investigators and connect LEAs and stakeholders. This cloud-based training system could encompass functions depicted in the diagram[2]:


Continuous Redesign of Training Material based on new Modus Operandi / new technologies
New Modus Operandi
Cyber Capacity Reviews
Cloud Based Modular Program
Simulated Cybercrime scenarios
Traditional training material (PPT/PDF)
Public-Private Partnership
E-Learning Modules
Certification & Accreditation
INTERPO

[2] "National Capacity Strengthening to Combat Cybercrime", Madan Oberoi, July, 2016, http://www.digitalpolicy.org/national-capacity-strengthening-to-combat-cybercrime/

xv. New modus operandi: In cyberspace, criminals keep on adopting new modus operandi every day and therefore, simulation-based training methodology has to be contemporary. To develop new scenarios, it is important to keep abreast of new modus operandi and technology trends. This part would include:

   a. Knowledge exchange on current and emerging methods of operations (or modus operandi) of cybercriminals
   b. Within this platform, training courses could stress-test the computing skills of cybercrime experts to analyse and discern signals collected from hacker forums, internet relay chat rooms and messaging texts
   c. Attacks like phishing and tampering, advanced persistent threats, backend systems and reverse-engineering could be simulated.
   d. Combating cybercrime could take more than technical skills and require cross-disciplinary knowledge. Researchers must look at the best practices to stay ahead of hackers by understanding indicators of malware victimisation, the ecology of trust and motivation among hackers, online hacker communication and interaction styles
   e. Gaining practice in such knowledge exchanges could shed light on how hacker communities interact and share information, creating actionable intelligence for cybercrime investigations

xvi. Continuous redesign for training material: Feedback gathered from learner usage and experience must be utilised to design new knowledge capacity and material. The modules should be developed by subject-matter-experts, ensuring quality content is constantly updated. Training courses should be more reflective of real-world cases and incidents

xvii. In order to maintain engagement with users, tapping into learners' interests can be done through offering appropriate challenges and increasing motivation

xviii. Synchronised skill levels: This platform will allow new relationships with other nodes within the networks of the cybersecurity architecture. Effective collaboration and greater harmonisation will provide a more accurate and comprehensive assessment of cyber criminality, ensuring responses are coordinated, effective and timely response.

Partnerships:

i. **UNODC:** Established in 1997 through a merger between the United Nations Drug Control Programme and the Centre for International Crime Prevention, UNODC is a global leader in the fight against illicit drugs and international crime. The capacity-building assistance UNODC provides inter alia includes:

   a. Specialized training for practitioners and policymakers involved in healthcare, law enforcement, criminal justice and other priority areas

   b. A wide array of operational tools, guides and practical resources, including handbooks, manuals, software, databases, case studies, assessment instruments, training modules and other resources and reference tools.

   c. Collection, dissemination and promotion of best practices and lessons learned, and develops guidelines based on them.

   d. developing online networks and databases to support international cooperation and information-sharing.

   e. encouraging interagency coordination and crossborder operations, particularly in efforts to halt trafficking and other forms of transnational crime.

   f. fostering interdisciplinary dialogue and knowledge-sharing

ii. **INTERPOL**: INTERPOL is the world’s largest international police organization, with 192 member countries. Police training plays a key role in INTERPOL’s overall mission to promote international police cooperation. INTERPOL helps to build the capacity of police in our member countries, equipping them with the knowledge, skills and best practices needed to meet today's policing challenges. INTERPOL’s wide range of initiatives is designed to bridge the gap between national and international policing and help law enforcement agencies make maximum use of the services provided by INTERPOL. Partnerships with the public and private sectors ensure the continued relevance of our training courses and access to the latest thinking and expertise. Operational training courses cover specialized crime areas – such as terrorism, drugs and trafficking in human beings – as well as investigative support tools, such as forensic techniques and the use of INTERPOL's network and databases. Other programmes are aimed at senior officers with responsibility for international police cooperation, Police Leaders.

iii. **CEPOL**: CEPOL is an agency of the European Union dedicated to develop, implement and coordinate training for law enforcement officials. CEPOL’s official name is “The European Union Agency for Law Enforcement Training”. CEPOL’s headquarters are located in Budapest, Hungary. CEPOL brings together a network of training institutes for law enforcement officials in EU Member States and supports them in providing frontline training on security priorities, law enforcement cooperation and information exchange. CEPOL also works with EU bodies, international organisations, and third countries to ensure that the most serious security threats are tackled with a collective response. CEPOL’s current portfolio encompasses residential activities, online learning (i.e. webinars, online modules, online courses, etc.), exchange programmes, common curricula, research and science.

iv. **FBI**: The FBI also offers international training to foreign national police agencies via its International Law Enforcement Academies (ILEA), which deliver courses on leadership and investigative techniques, as well as specialized seminars on several security issues. The FBI heads facilities in Hungary, and offers seminars at national police academies located in Thailand, Botswana, and San Salvador.

v. Law enforcement collaborations with the private sector can be used to explore and design complex simulations of future communications technologies that are prone to criminal exploitation, improve cyber security skills at all levels and work with associated professions to make industry more resilient to cybercrime.

****