CYBERCRIME
A New Frontier of Organized Crime

NATIONAL INITIATIVE
AGAINST ORGANIZED CRIME
PAKISTAN

NATIONAL INITIATIVE
AGAINST ORGANIZED CRIME
PAKISTAN

POLICY BRIEF

CYBERCRIME
A NEW FRONTIER OF ORGANIZED CRIME

*by **Kashif Noon***

Kashif Noon, lead researcher at NIOC, has developed this policy brief which was peer-reviewed by the head of the cybercrime wing of the Federal Investigation Agency. It has been issued after the approval of the NIOC Advisory Board and with the support of NIOC Secretariat.

NIOC
NATIONAL INITIATIVE
AGAINST ORGANIZED CRIME
PAKISTAN

ADVISORY BOARD

Tariq Parvez
President Advisory Board, NIOC:
Former Director General Federal Investigation Agency

Zahid Hussain
Member NIOC AB:
Eminent journalist particularly specializing in countering terrorism

Samina Ahmed
Member NIOC AB:
Senior Adviser Asia and Project Director, South Asia for the International Crisis Group

Zubair Habib
Chairman CPLC Karachi, Member NIOC AB:
For community outreach.

Jawaid Akhtar QPM
Member NIOC AB:
Police Officer. retired as the Deputy Chief Constable of West Yorkshire Police

Fasi Zaka
Member NIOC AB:
Communications expert. To steer the advocacy campaign.

NIOC DIRECTORATE

Tariq Khosa
Director

Muhammad Amir Rana
Secretary

Muhammad Ali Nekokara
Deputy Director

Hassan Sardar
Admin & Finance Manager

CONSULTANTS

Ammar Hussain Jaffri
Communication Strategist

Kashif Akram Noon
Lead Researcher

Outline

CYBERCRIME: A NEW FRONTIER OF ORGANIZED CRIME

Foreword

Evolutionary explanations suggest that criminal behaviours have evolved over time. This evolution not only added new practices and means to the acts of crime, but also provided complex dimensions to the criminal psychology. Meanwhile, the battle between criminals and law enforcers also continues with cybercrime being a new front. Internet has already changed the lives of millions and continues to do so. But it is also a tool in the hands of criminals to invent new criminal practices including in business, and to cause harm to governments, communities and citizens.

Though Internet and cyberspaces are a recent phenomenon, yet unlike other developments these are moving forth at lightning speed. We have seen the era of Morse code and are now witnessing the world rife with big data analytics and technologies. There is a growing talk of cryptocurrencies and cyberterrorism. Many heinous crimes happen on the dark or deep web. This widening scope of criminal activities needs to be understood and swiftly countered including through robust law enforcement approaches. That also calls for flexible but strong law enforcement approaches which are able to adapt to ever-changing world of cybercrimes. Cyberspace is also a cross-cutting tool, and criminal enterprises are adopting and using it to circumvent law enforcement.

In this context, the National Initiative against Organized Crime (NIOC) decided to conduct research and develop a policy paper on the issue of cybercrime. We believe that law enforcement agencies in Pakistan need support in handling this emergent threat in the realm of organized crime, including in terms of insight in the perspectives of policy and practice.

Kashif Noon, consultant and lead researcher at NIOC, developed this policy brief in collaboration with Mohammad Ali Nekokara, Amir Rana, Ammar Jaffri and Hassan Sardar. The Advisory Board led by Tariq Parvez, and other members including Zahid Hussain, Samina Ahmed, Zubair Habib, Jawaid Akhtar and Fasi Zaka provided strategic advice for conducting the research.

Special thanks are extended to the officials of Federal Investigation Agency (FIA) for their support in completing this work. It is hoped that this policy brief will add to the body of knowledge on cybercrime in Pakistan and will help policymakers and law enforcement departments to use the information and analysis for curbing the emerging threat.

Tariq Khosa

Director

National Initiative against Organized Crime (NIOC)

Introduction

The traditionally held distinction between different variants of crime, such as against person, property, or society, is getting blurred. A key reason for that is that the world is increasingly becoming virtual and is largely driven by data and information. Information has always been valuable including for criminals, mainly in terms of assessing law enforcement measures and evading them. The first-ever recorded recognition of coded concealment of information came in 50 BC, when Julius Caesar introduced Caesar cypher, or code, for encrypting military communication. Since then, governments and organizations have been practicing the protection of classified information. The information has been bought and sold at the state-level espionage. While in the past it was considered an indirect source of wealth, information has now become a wealth in itself. Data in the age of Internet has become equivalent to dollars. Most of the world's richest contemporary companies are data-based Internet giants. The world's richest man owns Amazon, an online retail service. Information and data have become tangible assets, and have transformed the traditional concepts of wealth. The world is also fast embracing 'e-commerce' as the most preferred mode of trade, sale and retail. The global growth in e-commerce has been exponential; a 2019 estimate put it at around $3.46 trillion.1 Similarly, online and social media interactions are fast replacing in-person meetings, and banking is increasingly shifting to e-banking. Everything is getting the prefix "e". Many predict that the time is approaching when more than half of the new businesses will run on Internet of Things (IoT), ranging from smart toasters to Internet-connected dog collars; mundane everyday use items are already connected to the Internet.2 Therefore, Internet and web based life is the new normal, which some people call the "fourth industrial revolution".

In the late 1970s, the first ever computer virus "creeper" was created to make free long-distance phone calls. The event was termed as the horizon of cybercrime, and was followed by the creation of first antivirus "reaper".3 The Morris worm or Internet worm of November 1988, which was transmitted through the Internet, gained the attention of the world and media for the first time.4 Since then, cybercrime has grown exponentially. New formats of cyber attacks have been developed. A community of organized criminals/hackers has evolved. They are virtually organized criminals

[1] Jessica Young, "Global ecommerce sales to reach nearly $3.46 trillion in 2019," Digital Commerce 360, November 13, 2019, https://www.digitalcommerce360.com/article/global-ecommerce-sales

[2] Matt Burgess, "What is the Internet of things? Wired explains," Wired, February 16, 2018, https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

[3] Infosec Institute, "Evolution in the world of cybercrime," June 28, 2016, https://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/#gref

[4] Ibid.

without faces and identities, who also coordinate their attacks virtually. In the age of virtual wealth, they are getting high dividends.

The Arsenal of Cyber Criminals

The most widely used weapons in the arsenal of cyber criminals are ransomware, point of sale attacks (PoS), botnets, phishing, cyber warfare and network travelling worms.

1. **Ransomware**: This malware (a software with built-in mala fide program) encrypts all files on a victim's computer and then demands ransom to restore the files, which is payable through bitcoins.[5] It is usually sent as an email attachment to the victim's computer in the guise of a legitimate source with legal assurances. Once the attachment is opened the malware starts its attack and encrypts all data. Suddenly the victim is unable to access its data. The ransom is demanded as a flash on the screen, generated by the malware. The University of Calgary has so far paid the largest ransom of 20,000 USD in bitcoins in response to such attack.[6]

2. **Point of sale attacks**: The plastic currency is increasingly becoming a preferred mode of payment. Instead of carrying cash in wallets, consumers prefer to make payments through debit or credit cards, which are also easy and secure to keep. The teller at the point of sale passes the card through a linear slot in the small machine, which is a computer vulnerable to malwares. These devices can temporarily memorize the information on the cards, including passwords. The attacking malware accesses this data and the card information is then used or sold on the dark web. In the biggest cybercrime PoS attack in 2013, a hacker was able to steal over 70 million credit card numbers from customers.[7]

3. **Botnets**: According to a major antivirus company 'Norton', botnets are the 'workhorses of the Internet'. They are legitimately used as a connected group of computers performing repetitive tasks for keeping the websites running. There is a program called 'spider' which crawls the Internet, looking for loopholes in the cyber security of a machine. It hacks a

Silk Road Case Trial

This particular Silk Road case was an online black market that was shut down twice by the FBI between 2013 and 2014. In February 2015, Silk Road's founder Ross Ulbricht was convicted of various crimes, including several attempted murders-for-hire. Silk Road ran its operations on the *dark web*, which makes up a small percentage of the *deep web*.

[5] Josh Fruhlinger, "Ransomware explained: How it works and how to remove it," CSO Online, June 19, 2020, https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[6] Infosec Institute, "Evolution in the world of cybercrime," June 28, 2016.

[7] Erica Johnson, "What are the main vulnerabilities of POS systems," Heimdal Security, June 3, 2019, https://heimdalsecurity.com/blog/pos-systems-vulnerabilities

computer and uses it to shut down websites, email spam to millions of users, replace banner ads on a targeted website, and to perform similar malicious acts.[8] Botnets tend to send millions of spam emails, pull the websites down for ransom, or harm the victim financially or even emotionally. These botnets, due to their efficiency, are a favorite tool of cybercriminals. Some of the biggest botnets attacks in recent years have been Grum, Kraken, Mariposa, Mirai and 3ve.[9]

4. **Phishing**: Phishing is the oldest and yet the most prevalent cyber-attack. It began in the 1990s. It uses disguised email as a weapon, which is always from a trusted source. The criminal masquerades as a trusted entity of some kind and seeks victim's banking information or asks to pay an amount to access something as 'lottery'. They attract the victim by baiting them; hence the word phishing [fishing] is used. Perhaps one of the most consequential phishing attacks in history happened in 2016, when hackers managed to get Hillary Clinton campaign chair John Podesta to offer up his Gmail password.[10]

5. **Denial of services (DoS) attacks:** A DoS attack is expression of 'malice' in cyber world. This kind of attacks usually targets big companies, where users get the message that services provided by that company are denied, causing losses to customers.

6. **Auto teller machine (ATM) skimming:** Auto teller machines (ATMs) are increasingly replacing cheque-based banking. Even in remote areas, ATMs are installed. ATM skimming is done by placing a device in the swipe, capturing the magnetic strip information on the card. Then often CCTV cameras placed in the booths are hacked and digital passwords are captured. This information is then used to transfer funds or for online purchases. Sometimes cloned cards are also created.

The Deep Web and the Dark Web

The *deep web* is a portion of the Internet, a collection of encrypted websites, which is hidden from the normal search engines like Google. The *dark web* on the other hand is a portion of the Internet that is intentionally hidden from search engines, and uses masked IP addresses. It is accessible only with a special web browser. The *dark web* is part of the *deep web*.[11] Indeed, the *deep web* is a generic term that

[8] Norton, "What is a botnet," https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

[9] EC-Council, "9 of the biggest botnet attacks of the 21st century," June 24, 2020, https://blog.eccouncil.org/9-of-the-biggest-botnet-attacks-of-the-21st-century

[10] Josh Fruhlinger, "What is phishing? How this cyber attack works and how to prevent it," CSO Online, April 7, 2020, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

[11] Dictionary.com, "The deep web vs dark web: do you know the difference?" https://www.dictionary.com/e/dark-web

not only includes the *dark web*, but also "mundane content like registration-required web forums and dynamically-created pages like your Gmail account."[12]

When people discuss the seedy underbelly of the Internet where they can buy drugs, weapons, child pornography, murders-for-hire – basically any illicit item or service of that sort – they are indeed talking about the *dark web*. Greenberg notes that while the *deep web* is vast and accounts for 90-something percent of the Internet, the *dark web* only accounts for about .01 percent. The *dark web*, sometimes referred to as *darknet*, is accessed by Tor (The Onion Router) or I2P (Invisible Internet Project), which use masked IP addresses to maintain anonymity for users and site owners. This way, people who use the *dark web* for illegal purposes can't be traced.

The *dark web* is not all about illicit deals and seedy undertakings but is used for an array of purposes. For one, journalists use the *dark web* to protect anonymity of their sources. Similarly, others may use it simply because they believe strongly in their right to privacy. Max Eddy for *PC Magazine* reports that "Tor was originally developed by the US Department of Defense," and while now Tor is a nonprofit run by volunteers, it is funded by the likes of the US government and the National Science Foundation. On Vox, Timothy B. Lee explains: "Government[al] support for Tor has continued in recent years as part of the State Department's internet freedom agenda, which seeks to help people in repressive regimes gain access to information censored by their governments." For instance, Facebook recently launched a version of its site on the *dark web* to "make it easier to access the site from countries that restrict the service, such as China and Iran."[13]

The wide variety of arsenal available for cyber criminals and organized cybercrime, and the operational areas of deep web and dark web raise two very important issues of cyber security and cyber law enforcement. While the former deals with the individuals and markets, the latter is related to governments.

A Bit about Bitcoins

In order to understand bitcoins, it is pertinent to first understand blockchains. A blockchain is a virtual chain of data ledgers or records, known as blocks. Each block is "a digital ledger in which transactions are recorded chronologically and publicly".[14] Data is stored in computers across the world. When space for data storage is full, a block automatically seeks and gets linked with another block for data storage. In this way, the process goes on. When used for transfer of money, blockchains are able to transfer even the 'tinniest' fractions, which cannot be done efficiently

[12] Andy Greenberg, "Hacker lexicon: What is the dark web?," Wired, November 19, 2014, https://www.wired.com/magazine

[13] Dictionary.com, "The deep web vs dark web: do you know the difference?" https://www.dictionary.com/e/dark-web

[14] Coinmetro, "Blockchain: Explained in plain English," https://blog.coinmetro.com/blockchain-explained-in-plain-english

through regular electronic funds transfer methods. All cryptocurrencies use the blockchain technology.

The motivation behind the creation of bitcoins was apparently altruistic, i.e. to democratize the global financial system and ostensibly reduce inequalities. A bitcoin is anonymous money but at the same time it can be inspected by anyone at any time. It was invented and made public in 2008 by a Japanese person with pseudonym Satoshi Nakamoto. Bitcoin is not regulated or owned by anyone. The idea is to use cryptography to control the creation and transfer of money, rather than relying on central banks. Since the success of bitcoin, over 3,000 other virtual currencies have been introduced with varying degrees of success and popularity, such as Ethereum, Litecoin, Monero and Dash. Bitcoins derive their value partly from their scarcity, which is defined by a cryptographic lottery. One can buy bitcoins on online cryptocurrency exchanges or can earn them through a process known as 'mining'. Bitcoin mining programs compute an encryption function called 'hash' on a set of random numbers. Coins are awarded to whichever miner happens to compute a number below a certain threshold. This lottery favors those with the biggest and fastest machines, and currently there are about 17 million bitcoins in circulation. The total number of bitcoins in (virtual) circulation will never exceed 21 million because of the way the system was designed. Bitcoins and other cryptocurrencies are the most popular mode of transactions in the cybercrime world including ransomware or dark web.

Cyberterrorism

While the terrorists are adopting new strategies and tactics, there is a grave risk of terrorism evolving into cyber terrorism. Most of the governments have web-based critical infrastructures, such as transport networks, communication networks, power grids and even nuclear facilities. A USIP study in 2004 had noted: "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objective'[15]. There have been many reports of such attacks in the Western world.

Cybercrime and Digital Economy

The United Nations Conference on Trade and Development (UNCTAD) used to publish an annual report on 'information economy'. It renamed the report as 'digital economy' in 2019. That clearly indicated the advent of digital economy and replacement of 'information' with 'digital'. Global Internet Protocol (IP) traffic (a proxy measurement of data flow) was 100 GB per day in 1992, and in 2017 it reached 45,000 GB per second. The UNCTAD 2019 report estimated that by 2022 the

[15] Gabriel Weimann, "Cyberterrorism: How real is the threat?," United States Institute of Peace (USIP), Special Report 119, December 2004, https://www.usip.org/sites/default/files/sr119.pdf

Internet traffic would be around 150,700 GB per second. This simple comparison indicates the growth of digital data flows at a breakneck speed.[16] The combined value of digital economy is estimated to be $7 trillion.[17] The primary challenge to this exponentially growing economy is from cybercrime. Forbes magazine estimated in 2019 that in five years the global economy would lose $5.2 trillion to cybercrime.[18] The threat is acute, therefore responses need to be designed accordingly. Pakistan has a low ranking on Global Digital Evolution Index; 56 out of rank score of 60, i.e. fourth from the bottom. The Ministry of Planning, Development and Reforms estimated the size of Pakistan's digital economy to be around $3.5 billion.[19] Therefore, Pakistan is at the cusp of entering digital economy.

There are three key elements of the global and national digital economies:

a) Financial technology (Fintech)
b) Ecommerce
c) Personal information/privacy data

Fintech is used by banks and financial institutions. Ecommerce is used by different retail outlets and is becoming a growth sector in Pakistan's urban economy. In case of social media applications, personal data and information is 'sold' by the otherwise free platforms. This personal data and a preference profile is used for aggressive advertisement and marketing. With growing digitalization of the economy, 'identity theft' will perhaps become a rising format of crime. Recently Google had to pay $13 million in damages for breach of privacy in a class action law suit.[20] Similarly the social media giant Facebook is facing a lawsuit of $35 billion.[21] Therefore, threat from cybercrime spans a wide spectrum, ranging from corporation and banks, etc., to individuals.

Patterns of Cybercrimes in Pakistan

Pakistan is on the cusp of digital economy revolution. While cybercrime in the world has surpassed drug trafficking, in terms of earnings,[22] Pakistan will not enter the world of digital economy without

[16] See United Nations Conference on Trade and Development's (UNCTAD) *Digital Economy Report 2019*, which can be downloaded here: https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466

[17] Ibid.

[18] Steve Culp, "Cybercrime: A major threat to trust in the digital economy," Forbes, March 25, 2019, https://www.forbes.com/sites/steveculp/2019/03/25/cybercrime-a-major-threat-to-trust-in-the-digital-economy/#2ab5e1a02cb7

[19] Major portion of this industry is essentially related to IT manufacturing, assembly etc. It does not reflect the real digital economy which would be based on innovation.

[20] Clare Duffy, "Google agrees to pay $13 million in Street View privacy case," CNN, July 25, 2019, https://edition.cnn.com/2019/07/22/tech/google-street-view-privacy-lawsuit-settlement/index.html

[21] Josh Constine, "$35B face data lawsuit against Facebook will proceed," Techcrunch, October 18, 2019, https://techcrunch.com/2019/10/18/facebook-35-billion-lawsuit

[22] National Response Centre for Cyber Crime, "Cyber Crime," http://www.nr3c.gov.pk/cybercrime.html

associated risks of cybercrime. The use of digital currency and online purchasing is not yet common in Pakistan, mainly because people are conservative and less educated, and thus hesitant to purchase on line. A recent study reveals that out of 300 respondents 171 expressed reluctance for online transactions.[23] Pakistan's electronic crimes Act 2015 defines categories of offences. The table below represents the percentage of these cyber offences committed according to National Response Center for Cyber Crime, after a year since the Law was enacted:

Type of Offence	Percentage
Illegal data interference or system damage	7%
Illegal access to computer systems	6%
Illegal access, interception and acquisition of computer data	5%
Computer related trade mark and copyright offences	1%
Sending or controlling sending of spam	2%
Mobile/Computer related fraud and forgery	15%
Computer related acts involving hate material	7%
Computer related acts in support of terrorism offences	5%
Breach of Privacy or data protection measures	7%
Computer related identity offences (impersonation and identity theft)	17%
Computer related solicitation and 'grooming' of children	0%
Computer related acts causing personal harm (including social media related issues	28%
Computer related production, distribution or possession of child pornography	0%

(Reproduced from: The Incidence of Cyber Crimes in Pakistan (2016), full-text pdf can be downloaded here: https://www.researchgate.net/publication/304215702_The_Incidence_of_Cybercrime_in_Pakistan)

The study also quoted National Center for Cyber Crime to claim that amongst the 28% reported crime causing personal harm, 60% were Facebook related.[24] Since the year 2016 when this study was conducted, there has been an exponential increase in the number of Internet users in the country. It reached 47.5 million mobile Internet users and 2 million fixed broadband subscribers in 2018. More than 90% of these users started using the Internet in the last 4 years after introduction of 3G and 4G connections.[25] The cybercrime rates have also increased almost similarly.

[23] Kashif ur Rehman and Muhammad Ashfaq, "Examining online purchasing behavior: A case of Pakistan," (2011 International Conference on Social Science and Humanity), *IPEDR,* Vol. 5, IACSIT Press, Singapore.

[24] Ufaq Manzar, Sama Tanveer, and Sanwal Jamal, "Incidence of Cyber Crimes in Pakistan" (Bachelor's thesis, 2016); can be downloaded here: https://www.researchgate.net/publication/304215702_The_Incidence_of_Cybercrime_in_Pakistan

[25] Aamir Attaa, "State of social media and cyber crime in Pakistan in 2018," Pro-Pakistani, 2018, https://propakistani.pk/2018/02/06/state-social-media-cyber-crime-pakistan-2018

In 2017, ATM card skimmers from China stole the data of 579 debit cards. They were later apprehended from Karachi and their compatriot was arrested by Chinese Authority.[26] In 2018, Pakistan was hit by another major cybercrime attack in which data from 19,864 cards belonging to customers of 22 Pakistani banks was put on sale on the dark web.[27] Bank Al-Islami alone lost $6 million in just 23 minutes. It was essentially a point of sale (PoS) attack. Most transactions were traced to Brazil and US. Bitcoins and other cryptocurrencies are illegal in Pakistan. The authorities arrested two individuals belonging to Lahore in remote Shangla district of Khyber Pakhtunkhwa, where they were using bitcoins for money laundering.[28] In a similar incident, a bitcoin trader was arrested from Peshawar.[29] These incidents indicate that the trend of cybercrime is increasing in Pakistan.

Cybercrime as Organized Crime

The incidents and developments cited earlier suggest that cybercrime is increasingly becoming a new form of organized crime. The transactions on the data of stolen cards were made from as far as Brazil, US and China. This indicates the extent of the 'organization' of cybercrime is as global as the Internet. A research study asserted that cybercriminals, albeit organized, are 'non-violent' whereas other organized crimes adopting new technologies retain the element of 'violence'.[30] This contradistinction seems valid. Therefore, in case of Pakistan it will be useful to treat cybercrime as a form of organized crime itself as well as a tool adopted by the perpetrators of traditional organized crime. The adaptation mechanisms of traditional organized crime are presented in the following table.

Traditional organized crime	Adopting mechanisms
Terrorism and terrorist financing (TF)	1. Organizing cyber attacks on key government websites and systems 2. Recruitment through Internet (ISIS's favored method) 3. Hate and propaganda spread 4. Using cryptocurrencies and dark web for TF

[26] Geo News, "Hundreds of Pakistanis lose millions in major ATM skimming fraud," December 4, 2017, https://www.geo.tv/latest/170648-hundreds-of-karachiites-lose-millions-in-major-atm-skimming-fraud

[27] Farooq Baloch and Iftikhar Firdous, "Pakistani banks hit by biggest cyber attack in country's history," Samaa TV, November 6, 2018, https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history

[28] "Two held in Shangla for money laundering through bitcoin," *Dawn*, January 23, 2020, https://www.dawn.com/news/1529970

[29] Sajjad Haider, "FIA arrests man for trading Bitcoins in Peshawar," Samaa TV, March 8, 2019, https://www.samaa.tv/news/2019/03/fia-arrests-man-for-trading-bitcoins-in-peshawar

[30] Marjie T. Britz, "A new paradigm of organized crime in the United States: Criminal syndicates, cyber-gangs, and the worldwide web," *Sociology Compass* 2, no. 6 (2008): 1750-765.

Traditional organized crime	Adopting mechanisms
	5. Money heists using cyber methods (phishing, credit cards fraud etc., for funding terrorism)
Drug trafficking	1. Using Internet for the sale of drugs 2. Using dark web effectively for placing larger orders, etc. 3. Using cryptocurrencies for transactions
Human trafficking and smuggling	1. Using Internet-based traps by human smugglers (including websites) which seem legitimate 2. Using encrypted communication in human smuggling networks 3. Advertising for prostitution and other forms of trafficking

Law Enforcement Challenges

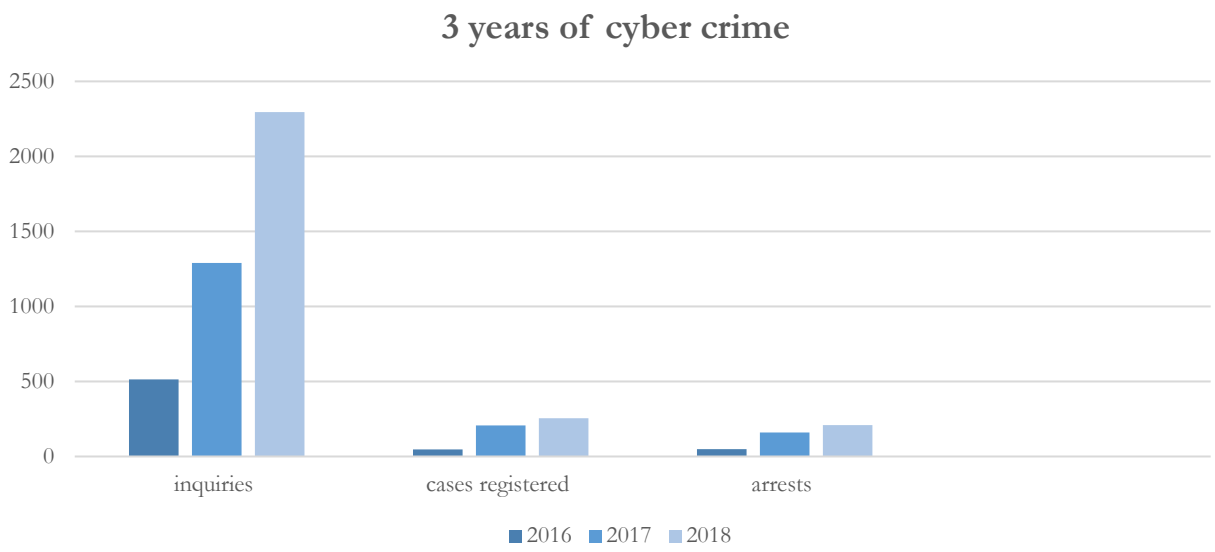
Prevention of Electronic Crimes Act 2016, criminalizes all mala fide acts using the Internet and other electronic means. The law is broad and also includes provisions for enabling international cooperation. However, there are three aspects which need to be considered carefully for understanding the law enforcement challenge posed by cybercrime:

a) Cyber security
b) Individual/personal information
c) Investigation and prosecution

This differentiation has been made on the basis of responsibility paradigm. The responsibility for cyber security rests with the companies, banks and retail enterprises. They have to invest in cyber security to ward off PoS and DoS types of attacks. They have to install all necessary safety measures in that regard.

In Pakistan, the most frequently reported cybercrime is related to personal domain, especially to female victims. This causes personal harm and often results in traumas and familial conflicts. The careless use of social media has resulted in criminal acts, like 'cyber harassment', 'cyber bullying' and 'trolling'. This aspect needs to be dealt at personal level by being careful, especially about the use of Internet by children. A careful approach in the use of Internet and especially social media can easily be managed at individual levels. All social media apps have settings to prevent any unwelcome advances and parental control settings. More awareness is needed to instill careful behaviors in the Internet users.

Pakistan's Federal Investigation Agency (FIA) has a designated National Response Center for Cyber Crimes, which has been trying to curb the evolving cybercrime. The following table shows a growth trend in reported cases, arrests and prosecutions.

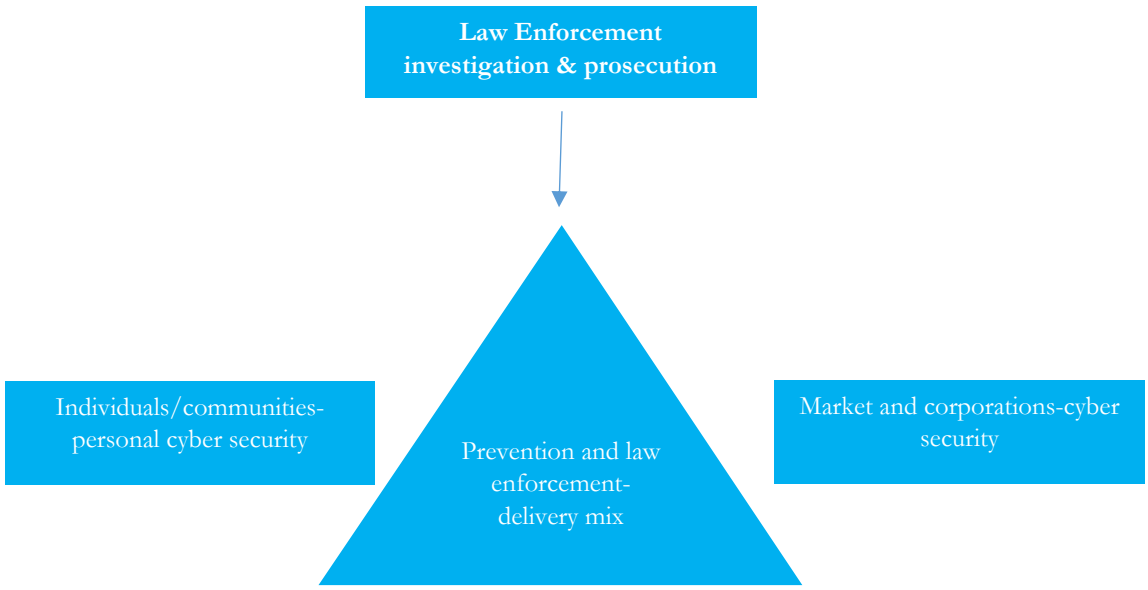


(Source: *Dawn*, October 23, 2018, https://www.dawn.com/news/1440854)

Therefore, it is imperative to understand that cybercrime transcends the corporate, personal and public sector law enforcement domain. It is also rising exponentially, further compounding the law enforcement challenge.

Conclusion

Colebatch and Larmour (1993) suggested a model of service delivery, where all actors would come together to deliver a service. The actors include: a) market; b) individuals and communities; and c) bureaucracy/hierarchy. This model can be borrowed for delivering a response to cybercrime, as described in the following diagram.



The following measures are important to make this approach functional and effective:

- Launching of a mass awareness campaign on cyber security and related issues;
- Making it mandatory for firms and corporations to invest in cyber security; and
- Building capacity of law enforcement agencies (mainly FIA and National Response Center for Cyber Crimes) in terms of fast changing landscape of cybercrime in Pakistan.

NIOC
NATIONAL INITIATIVE
AGAINST ORGANIZED CRIME
PAKISTAN

About NIOC

National Initiative against Organized Crime (NIOC) is the first-ever initiative in Pakistan, which was launched in November 2019 in collaboration with the Global Initiative's Resilience Fund. It is led by a group of committed professionals and experts with law enforcement, media and other public service backgrounds. Through developing an empirical evidence-base and conducting hand-on consultations, NIOC aims to build community resilience and influence public policy to combat organized crime including terror financing, drug trafficking, human trafficking and cybercrime. With a complex governance structure having multiple layers of stakeholders, the criminal justice system and law enforcement apparatus require better coordination and capacity building. NIOC tries to identify the gaps and suggest improvements in the system.

www.nioc.pk

niocpk

niocpk

niocpk