International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Organised Crime in the Digital Age

Dr. S. Krishnan[1], Mr Harsh Pratap[2], Ms Sakshi Gupta[2]

[1]Associate Professor, [2]LLB Student,
[1,2]Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India

ABSTRACT

Digital technology has transformed organizational life. Developments in communications, and in information storage and retrieval, to name just two areas, have greatly enhanced the efficiency with which legitimate organizations operate. Unfortunately, the benefits of digital technology are not lost on criminal organizations, which exploit digital technology to enhance the efficiency and effectiveness of their own operations. This paper will discuss the organized criminal exploitation of digital technology, by looking at a number of illustrative cases from Asia and around the world. It will discuss the various types of "conventional" organized crime that can be facilitated by digital technology, as well as terrorism, which itself can be regarded as a special kind of organized criminal activity. One fundamental question that the paper will seek to address is whether the activities of Asian organized crime have become substantively different as a result of technology, or whether traditional organized criminal activities in Asia are merely being conducted on a more efficient and effective basis. The paper will note the transnational nature of much organized criminal activity, and will discuss mechanisms for the control of organized crime in the digital age.

KEYWORDS: *Digital, Organised Crime, Malware, Hacking, cybercrime*

How to cite this paper: Dr. S. Krishnan | Mr Harsh Pratap | Ms Sakshi Gupta "Organised Crime in the Digital Age" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.152-169, URL: www.ijtsrd.com/papers/ijtsrd41185.pdf

IJTSRD41185

INTRODUCTION

"You are a Timex watch in a digital age", so says the smooth master criminal pitted against Bruce Willis' action-hero cop John McClane in *Die Hard 4.0* (known as *Live Free or Die Hard* in the US). The film begins on a relatively subdued note, with computer programmers hacking into government systems as a prelude for an all-out assault on the world's IT networks by disaffected Pentagon boffin Thomas Gabriel (Olyphant). It sets the tone for some of the techno-babble and unwieldy dialogue about cyber crime that blights the film's later stretches.

Drive-by downloads. Man in the Middle attacks. Fake installers. Rogue certificates. Bot zombies. Spyware, malware, Trojans. The list of cybercrime threats goes on. As the world becomes more connected, cybercriminals are becoming more adept, innovative and successful. How do organizations protect themselves in this high stakes game of corporate account takeovers, fraud and data and identity theft?

Digital crime is evolving, fast. As the real and online worlds converge, both the frequency and the variety of offences are increasing. Serious offences can now be committed with minimal physical resources. The spectrum of activity and players is broad, bewildering, and constantly changing: from hack attacks on banks, through online gambling rings and black markets, to old-fashioned, real-world violence for control of hi-tech digital tools.

In the decade since the term "cybercrime" was first coined, it has quickly emerged as one of the top four economic crimes, just behind asset misappropriation, accounting fraud and bribery and corruption.[1] The cyber-attacks on corporations globally, combined with confirmed threats to critical infrastructure in the U.S. and other countries, had former Secretary of Defense Leon Panetta warning of a potential "cyber-Pearl Harbour."[2]

Today's increasing proliferation of mobile devices and the new frontiers of ecommerce and social networking are raising the ante for security experts: more is at risk than ever before in the war against cybercrime. What has not been clear up to now is the extent to which these new types of crime are organised. Are there new types of online organisation, or are traditional crime groups entering the online world?

Cybercrime has become a billion dollar industry – therefore it is of no surprise that organized crime groups are increasingly seeking a share of the illicit profits. Attracted by the high rewards and low risk that many online criminal ventures provide, more and more organized criminal groups are focusing less on traditional criminal activities, and instead setting up online criminal networks. These groups

[1] PricewaterhouseCoopers LLP. Global Economic Crime Survey. November 2011.

[2] CIO Journal. The Wall Street Journal. "U.S. Defense Chief Warns of Digital 9/11." 11th October, 2012.

plan, organize and commit all forms of online crime – from fraud, theft and extortion, to the abuse of children.[3]

The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease, and range with which transactions can be conducted while also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities and multiplier benefits for illicit business. The dark side of the Internet involves not only fraud and theft, pervasive pornography and paedophile rings, but also drug trafficking and criminal organizations that are more concerned about exploitation than the kind of disruption that is the focus of the intruder community. In the virtual world, as in the real world, most criminal activities are initiated by individuals or small groups and can best be understood as "disorganized crime."

Globalization and technological innovation have not only impacted legitimate commerce, but they have simultaneously revolutionized crime. In response to these forces, organized criminals have adopted more-networked structural models, internationalized their operations, and grown more tech savvy. Criminals have become more elusive. They see international borders as opportunities while law enforcement views them as obstacles. Criminals have expanded their range of tools and targets as well. Meanwhile, law enforcement "plays by yesterday's rules and increasingly risks dealing only with the weakest criminals and the easiest problems," according to the Strategic Alliance Group, a partnership of seven law enforcement agencies from five nations.[4]

Yet there is growing evidence that organized crime groups or mafias are exploiting the new opportunities offered by the Internet. Organized crime and cyber-crime will never be synonymous – most organized crime will continue to operate in the real world rather than the cyber-world and most cyber-crime will continue to be the result of individuals rather than criminal organizations per se. Nevertheless, the degree of overlap between the two phenomena is likely to increase considerably in the next few years. This is something that needs to be recognized by business and government as an emerging and very serious threat to cyber-security. Accordingly, this analysis sets out to do three things:

- Explain why the Internet is so attractive to criminals in general and to criminal organizations in particular.
- Identify some clearly discernible trends that provide important clues about ways in which organized crime and cyber-crime are beginning to overlap.
- Identify a series of measures necessary for business to respond effectively to the growing exploitation of the Internet by organized criminals.

The Internet itself provides opportunities for various kinds of theft. Online thieves can rob online banks or illicitly gain access to intellectual property. The Internet offers new means of committing old crimes such as fraud, and offers new vulnerabilities relating to communications and data that provide attractive targets for extortion, a crime that has always been a staple of organized crime.

The anonymity of the Internet also makes it an ideal channel and instrument for many organized crime activities. The notion of a criminal underworld connotes murkiness or lack of transparency, where who is doing what is usually hidden from view. Secrecy is a key part of organized crime strategy and the Internet offers excellent opportunities for its maintenance. Actions can be hidden behind a veil of anonymity that can range from the use of ubiquitous cyber-cafes to sophisticated efforts to cover Internet routing.

ROLE OF ORGANISED CRIME IN THE DIGITAL AGE

Organized crime has always selected particular industries as targets for infiltration and the exercise of illicit influence. In the past, these have included the New York garbage hauling and construction industries and the Fulton Fish Market, the toxic waste disposal and construction industries in Italy, and the banking sector and aluminium industry in Russia. From an organized crime perspective, the Internet and the growth of e-commerce can be understood as the provision of a new set of targets for infiltration and the exercise of influence – a prospect that suggests that Internet technology and service firms should be particularly careful about prospective partners and financial supporters.

The organized crime groups use the Internet for major fraud and theft activities. Perhaps the most notable example of this – albeit an unsuccessful one – occurred in October 2000 and concerned the Bank of Sicily. A group of about 20 people, some of whom were connected to mafia families, working with an insider, created a digital clone of the Bank's online component. It then planned to use this to divert about $400 million allocated by the European Union to regional projects in Sicily. The money was to be laundered through various financial institutions, including the Vatican bank and banks in Switzerland and Portugal. The scheme was foiled when one member of the group informed the authorities. Nevertheless, it revealed very clearly that organized crime sees enormous opportunities for profit stemming from the growth of electronic banking and electronic commerce.

Indeed, organized crime diversification into various forms of cyber-crime or Internet related crime is closely related to a second discernible trend – organized crime involvement in what was once categorized as white collar crime. The activities of the US mob and Russian criminal organizations on Wall Street fall into this category: during the late 1990s there were numerous cases of criminal organizations manipulating micro-cap stocks using classic "pump and dump" techniques. While much of this was done through coercion or control of brokerage houses, the Internet was also used to diffuse information that artificially inflated the price of the stocks. Among those involved were members of the Bonnano, Genovese, and Colombo crime families as well as Russian immigrant members of the Bor organized crime group. As criminal organizations move away from their more traditional "strong arm" activities and increasingly focus on

[3] Cybercrime and Organised Crime. See http://www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/organized_crime/

[4] These law enforcement agencies include the U.S. Federal Bureau of Investigation (FBI); Drug Enforcement Administration (DEA); Immigration and Customs Enforcement (ICE); the United Kingdom's Serious Organised Crime Agency (SOCA); the Australian Crime Commission and Australian Federal Police; the New Zealand Police; and the Royal Canadian Mounted Police. See SOCA, "SOCA Working in Partnership Worldwide," http://www.soca.gov.uk/about-soca/working-in-partnership/international-partnerships. Intelligence Committee Futures Working Group, Crime and Policing Futures, Strategic Alliance Group, March 2008, p. 2. (Hereafter, Intelligence Committee Futures Working Group, Futures.)

opportunities for white collar or financial crime, then Internet-based activities will become even more prevalent.

This is not to suggest that organized crime will change its character. Its inherent willingness to use force and intimidation is well suited to the development of sophisticated cyber-extortion schemes that threaten to disrupt information and communication systems and destroy data. Indeed, the growth of cyber-extortion is a significant trend. Although extortion schemes — as the Bloomberg case[5] showed — are sometimes bungled, they can be done in ways that incur only modest risks (because of anonymity) and yield high pay-offs. Indeed, this might already be a form of crime that is significantly under-reported. Yet, it is also one that we can expect to see expand considerably as organized crime moves enthusiastically to exploit the new vulnerabilities that come with increased reliance on networked systems.

Another trend that we can expect to see is what might be termed jurisdictional arbitrage. Cyber-crimes – certainly when they are linked to organized crime – will increasingly be initiated from jurisdictions that have few if any laws directed against cyber-crime and/or little capacity to enforce laws against cyber-crime. This was one of the lessons of the Love Bug virus. Although the virus spread worldwide and cost business billions of dollars, when FBI agents succeeded in identifying the perpetrator, a student in the Philippines, they also found that there were no laws under which he could be prosecuted. Although more and more countries (including the Philippines) are passing legislation dealing with cyber-crime, there will continue to be what have been termed jurisdictional voids from which criminals and intruders can operate with impunity. Indeed, it is possible that some jurisdictions will increasingly seek to exploit a permissive attitude to attract business, creating both information safe havens (paralleling offshore tax havens and bank secrecy jurisdictions) that make it difficult for law enforcement to follow information trails and insulated cyber-business operations.

Further, the Internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place the opportunities for laundering money through over-invoicing and under-invoicing are likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases, laundering money by paying much more than the goods are worth. Online gambling also makes it possible to move money – especially to offshore financial centers in the Caribbean. Moreover, as e-money and electronic banking become more widespread, the opportunities to conceal the movement of the proceeds of crime in an increasing pool of illegal transactions are also likely to grow.

An instance can be made of what might be termed growing network connections between hackers or small-time criminals and organized crime. In September 1999, for example, two members of a group known as the "Phone masters" were jailed for two years and 41 months respectively. They had penetrated the computer systems of MCI, Sprint, AT&T, and Equifax. One of them, Calvin Cantrell had downloaded thousands of Sprint calling card numbers that were sold to a Canadian who passed them to someone in Ohio, from whom they went to an individual in Switzerland and subsequently to organized crime groups in Italy. As well as intruders working directly for criminals, these network connections between the two kinds of groups are likely both to deepen and to widen.

In another instance, 26 individuals – including reputed mafia organized crime family members – were indicted on charges of operating a sophisticated illegal gambling enterprise, including four gambling websites in a country in Central America. The District Attorney commented that 'law enforcement crackdowns over the years on traditional mob-run wire rooms have led to an increased use by illegal gambling rings of offshore gambling websites where action is available around the clock.' While gambling was illegal in the prosecuting jurisdiction, the websites took advantage of different legislation in other jurisdictions. Bets were placed in the country but processed offshore and the data 'bounced' through a series of server nodes to evade traditional law enforcement detection methods.[6]

In addition, of course, organized crime groups use the Internet for communications (usually encrypted) and for any other purposes when they see it as useful and profitable. Indeed, organized crime is proving as flexible and adaptable in its exploitation of cyber-opportunities as it is many other opportunities for illegal activity.

Criminals are relying on the increasingly interconnected world to form a networked community of heterogeneous, international groups, Europol said. These individuals groups are no longer defined by their nationality, geographic region, or type of criminal activity. Organized crime can now operate on an international basis, "with a business-like focus on maximizing profit and minimizing risk," said Rob Wainwright, director of Europol. "A new breed of organized crime groups is emerging in Europe, capable of operating in multiple countries and criminal sectors," said Wainwright.[7]

The volume of cybercrime activity, such as phishing and click fraud scams, is expected to increase, according to Europol. The increase "will closely mirror the growth of the attack surface, as the Internet becomes even more essential to everyday life," the report warned.[8]

Cybercrime is booming due to a lack of security awareness among European organizations and users, an official in the Europol said.[9] For example, people and organizations "expose" themselves as targets by making their data freely available on social networking sites. Unfortunately, the structure of such organizations makes them very difficult to be intercepted. Unlike traditional criminal groups, online groups generally operate on a 'stand alone' basis, with members rarely coming into direct physical contact with one another, and only meeting online. The organizations are usually run by a core group, which divides the different

[5] Michael Bloomberg, founder of Bloomberg L.P, an information services, news, and media company, worked with the FBI in a sting operation to apprehend cyber-extortionists, who were arrested in August 2000.

[6] Please see http://www.fbi.gov/newyork/press-releases/2012/four-gambino-crimefamily-members-and-associates-plead-guilty-in-manhattan-federal-court.

[7] Rashid, Fahmida Y., *Europol Warns Organized Cybercrime Is Booming*, Security Week, 19th March, 2013.

[8]'2013 EU Serious and Organised Crime Threat Assessment' Report Prepared by Europol, The Hague, 18th March, 2013.

[9] Interview with the official in Europal, 12th June 2019.

responsibilities of an operation (eg. spamming, web design, data collection) among the members. The members run their own outer networks to fulfill those responsibilities –rarely even having contact with each other online.

Organised criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. While some traditional criminal organisations are seeking the cooperation of e-criminals with the necessary technical skills, newer types of criminal networks operating only in the area of e-crime have already emerged.

The structure of these criminal organizations is different from traditional organised crime organisations. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centred on online meetings. These networks are structured on "stand alone" basis, as members rarely meet each other in person and sometimes do not even have a virtual contact with other colleagues. This sophisticated structure, together with access to the core operations granted only to trusted associates, prevents organised cybercrime groups from being detected and infiltrated by law enforcement.

Cybercriminals can work independently or as members of a large group. Some are mercenaries doing the bidding of more sophisticated criminals. Others act on their own behalf, such as a disgruntled employee with access to high-level identity and password information. A most disturbing development is that highly organized crime syndicates are playing a leading role in the explosion of cybercrime. According to the Federal Bureau of Investigation (FBI), these organizations operate like companies with specialists in each area of expertise:[10]

- Organization leaders assemble the team and choose targets
- Coders write the exploits and malware
- Distributors trade and sell stolen data
- Tech experts maintain the criminal enterprise's IT infrastructure
- Hackers search for and exploit vulnerabilities in applications, systems and networks
- Fraudsters woo potential victims with social engineering schemes like phishing and spam
- Hosted system providers offer illicit content servers
- Cashiers control drop accounts and provide names and accounts to other criminals for a fee
- Money mules complete wire transfers between bank accounts
- Tellers transfer and launder illicit earnings through digital currency services

According to Akamai Technologies, the top ten countries from which cyber attacks originate have not changed significantly in the recent past. China remains the source of the largest recorded attack traffic. Aggregately, nearly 38 percent originated from the Asia Pacific/Oceania region, just over 36 percent in Europe, 23 percent in North and South America, and just under 3 percent from Africa. It should be noted, however, that due to the anonymity provided by the Internet, the point of attack origination is not necessarily the same as the location of the cybercriminal.[11]

Cybercriminals are brazen social engineers, skilled in duping targets into providing sensitive information and security credentials, such as passwords or user IDs. According to the World Economic Forum, today, a relatively low-skilled individual can cause devastating consequences for governments and corporations remotely. Any device connected to a network of any sort, in any way, can be compromised by an external party.[12]

The networks themselves could involve from ten to several thousand members and could include affiliated networks in their structure. Regardless of the number of members and affiliates, virtual criminal networks are usually run by a small number of experienced online criminals who do not commit crimes themselves, but act rather as entrepreneurs. The leading members of the networks divide the different segments of responsibility (spamming, controlling compromised machines, trading data) among themselves. Some "elite" criminal groups act as closed organisations and do not participate in online forums because they have enough resources to create and maintain the value chains for the whole cycle of cyber-offences, and therefore have no need to outsource or to be engaged as outsiders into other groups.

Without a clearer understanding of the different types of perpetrators behind this evolving threat, we cannot develop effective strategies to tackle them. Worryingly, key aspects of organised digital crime remain under-researched, and a lack of data and an absence of robust analysis are hampering our ability to develop effective policy and law enforcement responses.

NETWORK OF THE DIGITAL ORGANISED CRIME

One needs to look at the structure of organised digital crime groups, how they are using information and communications technology to perpetrate their crimes, and how these new threats can be tackled. Many standard perceptions of digital organisation need to be revised, not least that all organised digital crime groups (ODCs) are 'networked' organisations, they are primarily 'trans-jurisdictional' associations, they mainly involve young, technically-literate individuals, and other kinds of crime groups are less significant drivers of digital offending.

There is no doubt that we are entering a "fourth era" of organised crime. In the past century, organised crime has passed through three distinct eras. First, the Prohibition era of the 1920s saw organised crime groups emerge, profiting from illicit alcohol, gambling and racketeering. In the 1940s, the chaos of World War Two and its aftermath enabled a second era based on the exploitation of the Black Market. A third era was discernible in the 1970s and 1980s with the globalisation of drug markets and the emergence of new, international crime empires.

Whilst almost all organized criminal groups will use some type of networked technology to organize themselves and their crimes, some are also using those technologies to commit cybercrimes. The actual nature of the organization of cybercrimes varies according to the level of digital and networked technology involved, the modus operandi and the

[10] Panda Security. The Cyber-Crime Black Market: Uncovered. 2011.

[11] Akamai Technologies, Inc., Volume 5, Number 2, The State of the Internet 2nd Quarter, 2012 Report.

[12] World Economic Forum. Global Risks 2012: Seventh Edition, January 2012.

intended victim groups, which also help to define the differences between them.[13]

The more traditional organized criminal groups tend not to be involved in committing cyber-dependent crimes, which are those crimes that disappear when the Internet is removed.[14] They are, however, increasingly using networked technologies to communicate with each other to organize crimes or seek intended victims, for example, to sell drugs over the Internet or darknet. These forms of cybercrime are either "cyber-assisted" (usually using communications technology), because without the Internet the offending would still take place but by other means of communication, or they are "cyber-enabled", when long-standing (usually localized) forms of offending, such as illicit gambling, frauds and extortion, are given a global reach by digital and networked technologies. If the Internet is removed, then the offending would revert from the global to the local form. They contrast sharply with "cyber-dependent" crimes such as hacking, distributed denial of service and ransomware attacks, and spamming which, as indicated above, disappear when the Internet is removed from the equation.

Cybercrime also varies according to the *modus operandi* of the offending involved, which is linked with the motivations and profile of the criminal actors. The organization of "cybercrimes against the machine" such as computer misuse offences by hackers, for example, are very different to "cybercrimes using the machine" such as, scams, frauds, and extortion. Both of these are also very different from "cybercrimes in the machine" such as child sexual abuse material, hate speech, terrorist materials (where the offence is actually in the computer content).[15]

The final factor that has to be considered when looking at cybercrime and its organization is who are the targeted victim groups. Some criminal groups deliberately target individual users, for example, by spamming deceptive emails to scam or defraud them. Other groups deliberately target businesses or governmental organizations, to commit larger scale frauds, obtain trade secrets or to disrupt their business flows (to extort or at the behest of a rival). Finally, other groups, usually State actors, deliberately target the infrastructures of other States to create distrust or discontent and/or to cause harm.[16]

Therefore, not only is the organization of criminals using networked technologies a very different issue to the way that criminals organize crimes online, but the latter also depends upon the level of technologies used, the particular criminal acts being committed, and also the intended victim groups.

Now, the convergence of the online and offline world, and the new opportunities presented by access to information, online networks and new forms of "electronic" value threatens a fourth era of organised crime, in which both traditional crime gangs and new types of organisation can prosper and grow.

In a survey conducted by Symantec Corporation, it was found that 65% of internet users had been a victim of some kind of cybercrime, including viruses and malware attacks, online scams, phishing attacks, hacking of social-networking profiles, credit card fraud and sexual predation. Cybercrime has become a more lucrative criminal industry then the illicit drugs trade, and generates over $US 100 billion dollars annually. There is no doubt - cybercrime is rife, and is spreading at an alarming rate.[17]

DIGITAL TECHNOLOGY AND CYBERCRIME: THE RISE OF AN UNDERGROUND ECONOMY

In the early days of cybercrime, the scene was mainly dominated by individuals or loosely connected groups of hackers committing attacks just for fun or to demonstrate their technical skills.[18] The development and growth of the digital economy dramatically changed both the criminal landscape and the motivation of offenders, transforming cyber-related crime into a complex and thriving criminal industry. As in the case of illicit financial flows in general, there are no reliable estimates on the criminal profits and the reputational losses and recovery costs that can go far beyond the direct harm. Most of the assessments come from the cyber-security companies and, thus, are being questioned concerning the reliability of crime statistics and losses estimates.[19] The uncertainty about crime profits and losses for businesses, however, does not mean that there is no general understanding that the aggregated criminal profits and direct and indirect losses for businesses are very high.

While we are aware of the growing number of cyber crime cases, from child pornography, hacktivism, to website defacements and data theft from computer systems, a more disturbing issue is what we often fail to see, the business side of cyber crime in the underground market. In 2011, the GIB CERT (Computer Emergency Response Team) of Russia estimated the global cyber crime market to be US$12.5 billion. Services that can be availed include the following: online fraud, spam service, Cyber Crime to Cyber Crime market (C2C), and DDoS attack service. Adding to these services are online pornography, online child abuse, identity theft, credit card fraud and cyber assassination. To commit cyber crime, your imagination is the only limitation.

[13] Wall, David (2017). "Crime, security and information communication technologies: The changing cyber security threat landscape and implications for regulation and policing". in: R. Browns word, E. Scotford and K. Yeung (Eds.), *The Oxford Handbook of the Law and Regulation of Technology*, Oxford University Press. pp. 1075-1096.

[14] Wall, David (2015). "Dis-organized Crime: Towards a distributed model of the organization of Cybercrime", *The European Review of Organized Crime*, No. 2(2), 71-90; Lavorgna, Anita and Sergi, Anna (2014). "Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies". *International Journal of Law, Crime and Justice*. No. 42(1), 16-32.

[15] Wall, David (2017). "Crime, security and information communication technologies: The changing cyber security threat landscape and implications for regulation and policing". in: R. Browns word, E. Scot ford and K. Yeung (Eds.), *The Oxford Handbook of the Law and Regulation of Technology*, Oxford University Press. pp. 1075-1096.

[16] Ibid.

[17] Hyman, Paul, *Cybercrime: It's Serious, But Exactly How Serious?*, Communications of the ACM, Vol. 56 No. 3, pp. 18-20.

[18] Secure Works, 2010. 2010. "The Next Generation of Cybercrime: How it's evolved, where it's going." Executive Brief, secureworks.com.

[19] Jardine. 2015. "Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime." Chatham House, Global Commission on Internet Governance. Paper Series: NO. 16 — July 2015. Available at https://www.cigionline.org/sites/default/files/no16_web_1.pdf

To date, it is close to impossible to put a definite figure on the size and coverage of the underground market and the services it provides. Computer crime is no longer just about a hacker who has the expertise to successfully compromise a system and steal data for profit. The emergence of powerful search engines makes the cyber crime issue more challenging and complicated to prevent. The mentioned websites are considered to be an information highway where any person with or without technical knowhow can download and learn hacking techniques easily.

Adding to the list is the availability of cyber crime tools that can be purchased through the dark web. These are websites not accessible using the usual web browsers like Google Chrome, Firefox and Microsoft Internet Explorer, but can only be accessed using specially crafted browsers like TOR Browsers. Interested individuals can buy and download highly sophisticated tools, newly released exploits and payloads, malwares and other malicious software useable for any type of cyber crime activities.

Cybercriminals are increasingly structuring their operations by borrowing and copying business models from legitimate corporations. Cybercrime business models were similar to those of high-technology companies in the early 1990s because digital criminality was still in its infancy. But since the early 2000s, cybercriminals have developed patterns imitating the operations of companies such as eBay, Yahoo, Google, and Amazon. One factor indicating the current maturation of the cybercrime industry is the degree of professionalization of IT attacks, e.g., fraudulent activities like classic phishing, which is becoming the greatest identity-theft threat posed to professional businesses and consumers. Another factor is the increasing specialization of perpetrators, which means that cybercrime involves the division of labour. Other factors include the sophistication, commercialization, and integration of cybercrime.

Crimes committed with the aid of technology allow bank robbers to steal money from banks without limits and without the risk of getting caught during the execution of the crime. Credit cards are being compromised not only by tens or by the hundreds but by hundreds of thousands. A highly knowledgeable hacker can steal the entire database of a bank containing bank accounts and credit card information, which are then sold like a normal commodity both offline and online. Debit and ATM cards are favorite targets of these cybercriminals. Once acquired, the information is used to clone cards and sent to money mules around the world to make cash withdrawals from ATM machines.

To add insult to injury, investigating and prosecuting cybercriminals is nothing similar to the way the law enforcement agencies deal with traditional crimes. Extracting and gathering digital evidence, not to mention presenting it in court, makes it more difficult for our law enforcement agencies to file a case and convict cybercriminals.

There is no doubt that cyber crime is a big threat to social and economic security world over. The continuing sophistication of technology is polluting the minds and morals of our children. Cybercriminals are gaining grounds and taking advantage of the underground market, while we fall prey and helpless every time we connect ourselves to the internet. Norton's 2016 cyber crime report showed that 689 million people in 21 countries experienced cyber crime including identity theft, money stolen from bank accounts and credit cards. And since 2015, victims spent US$126 billion globally dealing with internet crime.

According to the FBI, cyber crime represents an underground economy of $114 billion that is highly organized, employs expert hackers and operates like a legitimate global economy. Cyber crime is on the rise among American businesses and is costing the U.S. economy very badly. Cyber crime knows no boundaries. Everyone is a target. Governments, organizations, business and individuals are probable victims.

Technological developments, research, innovation, and the transformation of value chains into value networks has driven the globalization of the legal sector and has affected their organisations, making them more decentralized and collaborative with regard to external partners. In the same way, innovation has fuelled the creation of new patterns in criminal ecosystems with regard to product placement, subcontracting, and networking. Cybercriminals employ schemes similar to the legitimate B2B (business-to-business) models for their operations, such as the highly sophisticated C2C (criminal-to-criminal) models, which make stolen data and very effective tools for committing cybercrime available through digital networks. Computer systems' vulnerabilities and software are exploited to create crime ware: "malware specifically developed with the intention of making a profit and which can cause harm to the user's financial well-being or valuable information. These crime ware tools like viruses, Trojans and keyloggers, offer criminal groups the flexibility to control, steal and trade data.

Though the primary targets of the cybercriminals are more wealthy developed countries, which heavily depend on information technologies, and there is a common notion that many crimes originate in countries in Asia, Africa, and Eastern Europe[20], the underground economy itself exists independently of national borders. The development of the cybercrime industry is driven by the monetary value of data and services[21], traded on the specific internet platforms and via communication channels, which are used as underground marketplaces.[22]

This value represents an illicit commodity, intangible and easily transferrable across borders. Specific criminal activities have been developed and are being constantly improved in order to obtain data or increase the value of services: phishing, farming, spoofing, sophisticated malware, and tools to obtain information from commercial databases. Online criminality includes a broad spectrum of fragmented and highly specialized economic activity, where both the skills and data are offered for sale: various criminal groups specialize in developing specific tools such as exploits,

[20] Europol 2015. "The Internet Organised Crime Threat Assessment (iOCTA)." September 30. https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

[21] For example, according to KPMG research, in 2014 the prices for stolen credit card credentials ranged from US$0.25 to US$100 per item. Debit card information cost approximately US$9.55 per item, stolen usernames and passwords US$5.60 per item.

[22] Europol 2014. "The Internet Organised Crime Threat Assessment (iOCTA)." September 29. https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta; Fallmann. Hanno, 2010. "Covertly probing underground economy marketplaces." Vienna University of Technology Secure Systems Lab. http://www.iseclab.org/papers/dimva2010_underground.pdf.

writing code for malicious software, or leasing the tools for automated attacks.

The underground economy is structuring its operations by copying business models from legitimate sectors. Technological developments, research, innovation, and the transformation of value chains into value networks have driven the globalization of the legal sectors and have affected business structures, making them more decentralized and collaborative with regard to external partners. In the same way, the development of digital technologies is fuelling the creation of new models of labor division, subcontracting, product placement, communications, and networking in the criminal ecosystem of the digital underground economy.

Schemes for doing illegal business resemble legitimate business-to-business (B2B) models. Highly sophisticated C2C (criminal-to-criminal) operations aim to make stolen data, crime tools, and professional skills for committing crimes available through digital networks.[23] The vulnerabilities of software and systems are exploited to create so-called “crime ware,” that is, “malware specially developed with the intention of making a profit and which can cause harm to the user’s financial well-being or valuable information”.[24] Crime ware in the form of viruses, Trojans, key loggers, toolkits, and exploit kits offers cybercriminals the flexibility to steal and control data, to create and manage malicious programs, and to run networks of interconnected computers infected with malware.[25]

Cybercrime has undergone a revolutionary change, going from being product-oriented to service-oriented because the fact it operates in the virtual world, with different spatial and temporal constraints, differentiates it from other crime taking place in the physical world.[26] As part of this change, the cybercrime underground has emerged as a secret cybercrime marketplace because emerging technological changes have provided organized cybercriminal groups with unprecedented opportunities for exploitation.[27] The cybercrime underground has a highly professional business model that supports its own underground economy.[28] This business model, known as CaaS, is “a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner”.[29] Thus, CaaS is referred to as a do-it-for-me service, unlike crime ware which is a do-it-yourself product.

The different actors in the cyber underground use a variety of tools and mechanisms to obtain information, garner resources, and launch attacks. In addition to one-off exploits and attacks targeting a particular vulnerability or a particular system, which we explore in depth in later sections, many attacks often involve the use of a botnet. Attackers create a botnet by luring unsuspecting users to download malicious code, which turns the user’s computer into one of the “bots” under the command of the bot server. After installation, the infected bot machine contacts the bot server to download additional components or obtain the latest commands, such as denial-of-service attacks or spam to send out. With this dynamic control and command infrastructure, the botnet owner can mobilize a massive amount of computing resources from one corner of the Internet to another within a matter of minutes. It should be noted that the control server itself might not be static. Botnets have evolved from a static control infrastructure to a peer-to-peer structure for the purposes of fault tolerance and evading detection. When one server is detected and blocked, other servers can step in and take over. It is also common for the control server to run on a compromised machine or by proxy, so that the botnet’s owner is unlikely to be identified.

Botnets commonly communicate through the same method as their creators’ public IRC servers. Recently, however, we have seen botnets branch out to P2P, HTTPS, SMTP, and other protocols. Using this real-time communication infrastructure, the bot server pushes out instructions, exploits, or code modifications to the bots. The botnet, therefore, can be instructed to launch spam, DDoS, data-theft, phishing, and click fraud attacks. As such, botnets have become one of the most versatile attack vehicles of computer crime.

A profitable industry needs to reinvest illegal profits in legitimate business, a fundamental role in cyber-criminal organizations covered by the “money mules”, individuals who are knowingly or unknowingly used to launder a crime syndicates’ illegal gains. Money mules are used to anonymously transfer money from entities, typically through anonymous wire transfer services such as Western Union, Liberty Reserve, U Kash and WebMoney. Virtual currency services such as Bitcoin offer a valid instrument for money laundering preventing that law enforcement will be able to intercept the payment made to finance illegal activities.

Usually, each sale transaction is fragmented into smaller batches to elude controls operated by law enforcement. Cyber criminals’ organizations are structured like businesses. They develop a detailed business model and monetization strategy “because even an illegal company needs to ‘pay the bills’ in order to function on a day-to-day basis”. Money Management is vital aspect, as organizations have to track the resources used and the earns for their utilization, they do this utilizing commercial business process management tools, financial systems and many

[23] Ben-Itzhak. 2008. “Organized cybercrime.” ISSA Journal (October). https://dev.issa.org/Library/Journals/2008/October/Ben-Itzhak-Organized%20Cybercrime.pdf; Tropina, Tatiana. 2013. “Organised Crime in Cyberspace.” In Transnational Organized Crime. Analyses of a Global Challenge to Democracy. Bielefeld, Transcript Verlag, edited by Heinrich-BöllStiftung and Regine Schönenberg, pp. 47–60.

[24] ESET. 2010. “Cybercrime Coming of Age.” White paper, January. http://go.eset.com/us/resources/white-papers/EsetWP-CybercrimeComesOfAge.pdf.

[25] Kharouni, Loucif. 2012. “The Crimeware Evolution.” Trend Micro Incorporated Research Paper 2012. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-thecrimeware-evolution.pdf.

[26] M. Yar, “The novelty of ‘Cybercrime’: An assessment in light of routine activity theory”, *Eur. J. Criminol.*, vol. 2, no. 4, pp. 407–427, 2005.

[27] K.-K. R. Choo, “Organised crime groups in cyberspace: A typology”, *Trends Organized Crime*, vol. 11, no. 3, pp. 270–295, 2008.

[28] K. Hughes, “Entering the World-Wide Web”, *ACM SIGWEB Newslett.*, vol. 3, no. 1, pp. 4–8, 1994.

[29] A. K. Sood and R. J. Enbody, “Crimeware-as-a-service—A survey of commoditized crimeware in the underground market”, *Int. J. Crit. Infrastruct. Protect.*, vol. 6, no. 1, pp. 28–38, 2013.

other instruments to manage everything from software development to accounts payable.

According to The Aegenis Group, the black market value of a payment card account number was estimated to be between $4 and $6 in the 2007–2008 period.[30] Magnetic stripe data for a payment card carries a price tag between $25 and $35, depending upon the credit limit and type of card. Full information sufficient to open a bank account, including birthday, address, and Social Security number, goes for approximately $200 to $300. Other personal data, such as driver license numbers, Social Security cards, and PayPal or eBay accounts, are often seen for sale on the black market. Drivers' licenses and birth certificates go for about $100. A PayPal or eBay account goes for $5 to $10. Thus, a piece of malware that exploits an unpatched vulnerability can fetch anywhere between $20,000 and $40,000 a pop, depending on the consequences. Bot army building software (e.g., the exploits and bot agent code) goes for approximately $5,000–$10,000 on the black market.[31]

The rising black market value of personal data and data-stealing malware has created a cottage industry of criminals (the information dealers mentioned earlier) that focus on trading financial information. The incidents at TJX and Hannaford Brothers illustrate just the tip of the iceberg; the magnitude of the problem is not yet well understood by the general public.

A vulnerable website particularly that of a financial institution or an online e-commerce site, is often the most direct route to valuable data. Because the web server runs software that issues SQL commands to retrieve and modify the internal database (e.g., sensitive customer information), a successful SQL injection attack that fools the web server into passing arbitrary SQL commands to the database can fetch whatever data it chooses.

A well-known women's clothing store was recently informed by their web application firewall vendor that an SQL injection error in their web application could lead to the compromise of their entire customer database, including credit card numbers, PINs, and addresses.

It is almost routine now for security vendors who engage in web application scanning to discover not one, not two, but many SQL injection attack vulnerabilities in existing web applications. With the advent of Web 2.0 and its still-esoteric secure code development practices, we should not be surprised that many web applications are vulnerable to data theft attacks.

Organized crime groups have long realized that digital data theft represents a gold mine for them. It is known that some of these groups have both automated and manual means to scan the Internet continuously, looking for vulnerable sites.

Many Internet crimes today can be traced back to some form of malware. For example, spyware, installed on a user's machine, can steal private information on the hard disk, such as Social Security numbers, credit card information, and bank account information. Injected iFrames, a form of malware that typically lives on the server, can capture user login information and other proprietary communications between the browser and the server. Bot-building malware, once installed on a user's machine, wakes up once every so often to participate in botnet activities unbeknownst to the user.

The most popular means of malware distribution today is via the Web. Users browsing the Web who come in contact with a malware distribution or hosting site may subject their computers to a malware infection. Many such infections produce no visual clues and therefore are not easily identifiable without special detection tools. A disturbing trend is that we are seeing more and more legitimate websites unwittingly participating in malware distribution. Malware injected on the website (e.g., the injected iFrames mentioned earlier) can transparently redirect a user's browser to a third-party site that hosts malware. Google reports that 6,000 out of the top one million ranked websites (according to Google's page rank algorithm) have been listed as "malicious" at some point. Many are legitimate sites that are compromised at one point or another. Social networking sites and high-volume e-commerce sites have all been hot targets for malware distribution.

A significant step toward greater viability by the cyber underground economy is the ability to turn financial frauds into actual, usable *cash*. This is a nontrivial step that involves extracting cash from legitimate financial institutions. One of the most valuable assets in the cyber underground is so-called "drop" accounts where money can be routed and withdrawn safely. These are often legitimate accounts owned by parties that are willing to play the cashier role discussed earlier in exchange for a cut of the take.

Let's say Johnny the hacker has full account information for 20 Bank of America customers. Johnny could set up a bank transfer from these compromised accounts (to which he has access) to another Bank of America account owned by Betty, the cashier acting on his behalf. Betty then goes to her local bank and cashes out her entire account. She wires 50% of Johnny's deposit to a predetermined location, which will be picked up by Johnny, and keeps the remaining 50%.

Being a cashier carries a nontrivial level of risk. Experienced cashiers rarely stay put, often having at their disposal a number of different accounts opened with fraudulent credentials. A good cashier can often demand a market premium. Without the drop accounts and the cashiers, the underground economy would be nothing more than an academic study.

Given that the internet is an important driver of economic growth, it is clear that government actors need to take steps to ensure that criminal actors do not offset these gains.[32] The speed of post-strike interventions is critical to reducing harms – the time lag between implementing new criminal strategies and the effective countering of those strategies leads to economic losses. However, given the disadvantages of being attacked, and the costs required to minimise the impact of such attacks, the problem that law enforcement, organisations and governments will continue to face is the 'cost-to-pay-off' analysis vis-à-vis cybercrime. As it is the sovereign responsibility of the state to protect its citizens, it is arguably reasonable to demand that government provide the necessary policing responses to economic cybercrime, although these responses must inevitably compete with

[30] Interview with an official in The Aegenis Group, 12th January 2021.

[31] Ibid.

[32] Manyika, J & Roxburgh, C (2011). "The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity". McKinsey Global Institute.

other agendas and priorities. As noted earlier, the police are not required to be the sole player in the law enforcement landscape; rather, it is more about identifying specific roles and responsibilities in that landscape, as well as the role of other agencies, and the promotion of partnership and other collaborative arrangements. The crux of the challenge lies in the speed and volume of economic cybercrime, the global nature of the internet, and the scale at which this allows crimes to be committed. Subsequently, responsibilities for global protection and the pursuit of offenders lie with a plethora of national governments, requiring strong and effective collaborative networks.[33] Differences in political regimes and economic success raise the risk of 'free-rider' governments that refuse to participate in a global protection regime against online criminal actors. This is an issue that has been rising up the political agenda, though it is somewhat undermined by the politics surrounding allegations of state-sponsored hacking for economic and political intelligence and to cause damage. In this context, frauds against individuals and SMEs are normally subordinated.

DIGITAL ORGANISED CRIME AND COVID-19

On 10 September 2020, in Germany, more than 30 internal servers of the University Hospital of Düsseldorf were hit by a cyber attack, which crippled the hospital's systems and caused emergency patients to be turned away.[34] In the midst of the global crisis arising from the COVID-19 pandemic, the hospital was forced to route patients to other facilities for care. German authorities subsequently launched an investigation to determine whether the death of a re-routed patient had resulted from delays to her treatment because of the cyber attack[35]; if this was found to be the case, the death of the patient would be the first known fatality directly caused by a ransom ware attack. This attack was not an isolated incident. During the pandemic, malicious cyber actors are also known to have targeted the Paris hospital system; medical clinics and healthcare agencies in the US; the World Health Organization (WHO); COVID-19 treatment and vaccine research institutions; and other healthcare entities.[36]

Such incidents are reminders of the constant threat that cybercrime and other malicious cyber activity presents to countries' national, economic and human security. And these threats are nothing new. Cybercrime was already accelerating rapidly and evolving in most parts of the world before the COVID-19 pandemic, and the virus has only served to provide perpetrators with new opportunities and vulnerabilities to exploit for a variety of motivations. The stakes are perhaps higher now, in terms of how such crimes will impact national governments as they struggle to blunt the spread of both a deadly infectious disease and its resulting economic effects. Thus, cybercrime has been thrust into the spotlight as a threat to which more attention needs to be paid, across all sectors in all societies. In the long term, there are a number of questions about how the rise of cybercrime linked to the pandemic will impact developments that were already under way before the onset of the pandemic. In particular, COVID-19-related cybercrime, and the global attention being paid to it, may have lasting implications for global cybercrime cooperation and for internet governance more broadly.

With pandemic disrupting businesses and with remote working becoming reality, cyber criminals have been busy exploiting vulnerabilities. Year 2020 saw one of the largest numbers of data breaches and the numbers seem to be only rising.

According to Kaspersky's telemetry, when the world went into lockdown in March 2020, the total number of brute force attacks against remote desktop protocol (RDP) jumped from 93.1 million worldwide in February 2020 to 277.4 million 2020 in March—a 197 per cent increase.[37] The numbers in India went from 1.3 million in February 2020 to 3.3 million in March 2020. From April 2020 onward, monthly attacks never dipped below 300 million, and they reached a new high of 409 million attacks worldwide in November 2020. In July 2020, India recorded its highest number of attacks at 4.5 million. In February 2021—nearly one year from the start of the pandemic—there were 377.5 million brute-force attacks—a far cry from the 93.1 million witnessed at the beginning of 2020. India alone witnessed 9.04 million attacks in February 2021. The total number of attacks recorded in India during Jan & Feb 2021 was around 15 million.[38]

A data breach, irrespective of the modus operandi, has grown many folds in India. However, the disturbing trend in India has been firms' failure to acknowledge that a breach has happened, which then makes individual users wonder if their data is safe at all. Take the instance of the recent data breach at the payment firm Mobikwik. It was reported that the data breach incident has affected 3.5 million users, exposing know-your-customer documents such as addresses, phone numbers, Aadhaar card, PAN cards and so on. The company, till now, has maintained that there was no such data breach. It was only after the regulator Reserve Bank of India (RBI) asked Mobikwik to get the forensic audit conducted immediately by a CERT-IN empanelled auditor and submit the report that the company is working with requisite authorities.[39]

For users in India in case of data breaches they are in a fix as India does not have a specific legislation dealing with user data breach cases or penal actions relating to the same. The Personal Data Protection Bill, which is proposed to deal with such cases of data breaches, has been pending in the Lok Sabha since 2019. "The lack of clear regulatory frameworks and policy execution impacts our country's overall cyber hygiene. For Cyber security researchers who uncover breaches, policy reforms are needed as many face threats of legal prosecution without legislative protection. Enacting cyber security legal policies will give all stakeholders a frame of reference and guide them towards building a more resilient digital economy. Incident reporting should also be

[33] Ibid.

[34] Wired, "Hackers Are Targeting Hospitals Crippled by Coronavirus," 2020, https://www.wired.co.uk/article/coronavirus-hackerscybercrime-phishing (Accessed 15 June 2020).

[35] Ibid.

[36] MalwareBytes, "Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book," 2020, https://blog.malwarebytes.com/socialengineering/2020/03/cybercriminals-impersonate-worldhealth-organization-to-distribute-fake-coronavirus-ebook/, (Accessed 15 June 2020)

[37] Shivani Shinde and Neha Alawadhi, "India becomes favourite destination for cyber criminals amid Covid-19", *Business Standards*, 6th April, 2021.

[38] Ibid.

[39] Ibid.

made mandatory," said Pankit Desai, co-founder & CEO, Sequretek, an AI based cyber security firm.[40]

Cybercrime was a persistent and often transnational threat before the COVID-19 pandemic hit. The ubiquity of technology and the growing rates of internet connectivity, coupled with the continued development of new technologies that allow for anonymity, have made cybercrime a low-risk, high-reward venture for a wide spectrum of state and non-state actors.[41] Legacy technology used by critical infrastructure and a lack of adequate investments in cyber security in certain parts of the world have also exacerbated the problem.[77] The professional services firm Accenture found that the average cost of cybercrime for companies (across 11 different countries and 16 different industry sectors) increased by some 12 per cent in 2018, to a new high of $13 million, from $11.7 million in 2017.[42] The same study also estimated that the total economic value at risk from cybercrime around the globe may be as high as $5.2 trillion in the five-year period 2019–23.[43] It found that the techniques used by non-state and nation-state actors to commit cybercrimes were evolving, with perpetrators increasingly using 'people-based attacks' such as phishing or other forms of social engineering attacks.[44] The boundary between state actors and non-state cybercriminals was also increasingly blurring, as states abetted and in some instances directly employed non-state cybercriminals and/or their tools to advance their objectives.[45]

Law enforcement has struggled to keep up with this dynamic threat, resulting in a significant global cyber enforcement gap that allows cybercriminals to operate with near impunity. For example, the think-tank Third Way estimated in 2018 that only three in 1,000 reported cyber incidents in the US saw the arrest of one or more perpetrators.[46] While the extent of the entire global enforcement gap is unknown, the rates of arrest are not much better in a broad range of countries. There are numerous technical, operational and strategic challenges that have contributed to this gap[47], including significant hurdles related to the collection, handling and transfer of electronic evidence.[48] The fact that cybercrime investigations often require intensive cooperation within and across borders presents particularly thorny challenges. This gap has resulted in a perception among certain publics that, while governments have the legal authority to bring malicious cyber actors to justice, law enforcement will rarely be able, or willing, to try to do so. This may be, in part, due to the lack of capacity and capability among criminal justice actors on cybercrime and digital evidence. This leads to decreased public trust in the ability of law enforcers to secure justice for victims, which can hinder reporting.[49]

While cybercrime was continuing to increase and transform before the COVID-19 crisis, some data now indicate that the pandemic has only made things worse, at least at certain points. Europol (the European Union Agency for Law Enforcement Cooperation) noted that with a record number of people staying in their homes and relying even more on the internet for daily activities including work, education and leisure, 'the ways for cybercriminals seeking to exploit emerging opportunities and vulnerabilities have multiplied'.[50] According to one study published in March 2020, 88 per cent of US organizations had encouraged or required employees to work remotely.[51]In addition, social media usage rates have spiked.[52] Such shifts have created a large pool of individuals, businesses and even public officials who are increasingly using online communication, often with less stringent cyber security measures in place than would be employed in an office environment. This provides cybercriminals with an unprecedented number of victims to target.[53]

As well as having a growing number of potential targets, cybercriminals have customized their tactics, techniques and procedures (TTP) to the COVID-19 crisis, often exploiting people's fears about the pandemic to their advantage. INTERPOL (the International Criminal Police Organization) found an increase in the detected number, reported by global law enforcement entities, of malware and ransomware campaigns using the COVID-19 pandemic to access and infect computers.[54] Among the many examples of how cybercriminals are exploiting fears about the virus to conduct business are phishing campaigns or malware distribution through websites that have the appearance of being legitimate sources of information about COVID-19.[55]

Social engineering has been key to the success of many cybercriminals seeking to exploit the pandemic. While this was already a technique used by cybercriminals before COVID-19, the cyber security company Fire Eye found that: 'COVID-19 is being adopted broadly in social engineering approaches because it has widespread, generic appeal, and there is a genuine thirst for information on the subject that encourages users to take actions when they might otherwise

[40] Interview with Pankit Desai, Co-Founder and CEO,Sequretek, 31st January, 2021.

[41] Norton, "Coronavirus Phishing Emails: How to Protect Against COVID-19 Scams," 2020. https://us.norton.com/internetsecurity-online-scamscoronavirus-phishing-scams.html (Accessed 15 June 2020).

[42] Ibid.

[43] Ibid.

[44] R. Smithers, "Fraudsters use bogus nhs contact-tracing app in phishing scam," 2020. https://www.theguardian.com/world/2020/may/13/ fraudsters-use-bogus-nhs-contact-tracing-app-inphishing-scam (Accessed 30 May 2020).

[45] Ibid.

[46] M. Yar, "The novelty of 'cybercrime' an assessment in light of routine activity theory," *European Journal of Criminology*, vol. 2, no. 4, pp. 407–427, 2005.

[47] Ibid.

[48] N. Kumaran and S. Lugani, "Protecting businesses against cyber threats during covid-19 and beyond," 2020, https://cloud.google.com/blog/products/identitysecurity/protecting-against-cyber-threats-during-covid19-and-beyond (Accessed 17 June 2020)

[49] Ibid.

[50] Europol, "Pandemic Profiteering: How Criminals Exploit COVID-19 Crisis," 2020, https://www.europol.europa.eu/publicationsdocuments/pandemic-profiteering-how-criminalsexploit-covid-19-crisis (Accessed 15 June 2020).

[51] Ibid.

[52] M. Cross and D. L. Shinder, *Scene of the cybercrime*. Syngress Pub., 2008.

[53] Ibid.

[54] Wired, "Hackers Are Targeting Hospitals Crippled by Coronavirus," 2020, https://www.wired.co.uk/article/coronavirus-hackerscybercrime-phishing (Accessed 15 June 2020)

[55] Ibid.

have been circumspect.'[56] Business email compromise (BEC) attacks, in particular, are expected to continue to increase in frequency during the current crisis. These are a type of fraud that typically targets anyone who performs legitimate fund transfers. In April 2020 the US Federal Bureau of Investigation (FBI) noted that there had been an increase in BEC targeting municipalities purchasing COVID-19-related equipment and medical supplies.[57]

The above factors are reported to have resulted in an overall acceleration of cybercrime as the COVID-19 crisis took hold. As early as April 2020, the FBI reported that complaints of cybercrime had increased up to fourfold compared with the months prior to the pandemic.[58] By mid-2020, the US Secret Service estimated that $30 billion in COVID-19 relief funds would be lost to cybercrime.[59] The UN Under-Secretary-General and High Representative for Disarmament Affairs told an informal meeting of the UN's Security Council that there had been a 600 per cent increase in 'malicious emails' during the crisis.[60] In addition, the member states of Europol reported an increase in the number of attempts to access illegal websites featuring child sexual exploitation material.[61] However, some data indicate that the dramatic spikes in cybercrime recorded at the beginning of the COVID-19 crisis may be starting to level off.[62]

Broadly speaking, the types of threat actors that are conducting malicious cyber activity in the COVID-19 era are thought to be similar to those conducting such activity before the outbreak of the virus. Criminals, criminal organizations, nation states and state-backed actors are perpetrating malicious cyber activity with a variety of motivations during this crisis.[63] For many non-state criminals and criminal organizations, the proliferation of potential victims has been a boon for their financially motivated cybercrime businesses. For states and state-backed actors, the motivations are often quite different. Advanced persistent threat groups (APTs) receiving direction and/or support from states are targeting critical infrastructure, including hospitals and vaccine development labs. It is widely suspected that they are motivated by a desire to gain access to valuable information about COVID-19 response efforts and research.[64] WHO reported in April 2020 that it had seen a fivefold increase in cyber attacks, with at least some of these incidents believed to be linked to hackers connected to the Iranian government.[65] The UK, the US and Canada have publicly accused APTs associated with the Russian government of targeting vaccine research and development organizations.[66] Similarly, US authorities have accused actors affiliated with the Chinese government of being behind cybercrime and other forms of malicious cyber activity perpetrated against organizations conducting research related to COVID-19.[67]

While the threat actors remain largely the same, the risks posed to certain sectors during the COVID-19 crisis by a cybercrime incident or cyber attacks may be even greater. In particular, although the healthcare sector was already a major target for cybercrime before the pandemic – particularly through ransomware attacks, where victims' data or systems are held hostage until victims pay a ransom, as happened in the 2017 WannaCry attack on the UK's National Health Service[68] – a disruption or complete shutdown of a hospital treating patients, or of a research institution working to find a vaccine and treatments, could be tremendously destabilizing to entities already under unprecedented strain.[69] For a hospital, a successful attack could mean days or even weeks of being offline, and there is a risk that recovery efforts could inhibit a medical facility's ability to provide rapid, life-saving care to patients, as already demonstrated in the case of the attack on the University Hospital of Düsseldorf in March 2020.[70] INTERPOL has already reported a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response.[71] Cybercriminals are striking at healthcare providers and medical facilities as a means of targeting a sector that has lagged behind in its cyber security capacity – at a time when an institution may be most willing to pay a ransom in order to recover quickly from an attack. In addition, insurance companies have, in some cases, been reported as having advised entities in the healthcare sector to pay a ransom instead of incurring the substantial recovery costs in the event of an attack, despite law enforcement guidance in certain countries against doing precisely that.[72] While targeting the healthcare sector is not a novel approach for cybercriminals, the stakes for such attacks may be significantly higher in the context of the current pandemic.[73]

[56] Hiscox, "The hiscox cyber readiness report 2019," 2019, https://www.hiscox.co.uk/cyberreadiness (Accessed 9 May 2020)

[57] Ibid.

[58] UK's National Cyber Security Centre (NCSC) and the US' Department of Homeland Security (DHS) Cyber security and Infrastructure Security Agency (CISA), "Advisory: COVID-19 Exploited by Malicious Cyber Actors," 2020, https://www.ncsc.gov.uk/news/covid-19- exploited-by-cyber-actors-advisory (Accessed 15 June 2020).

[59] D. R. Cressey, "Other people's money; a study of the social psychology of embezzlement". Free Press, 1953

[60] S. Gallagher and A. Brandt, "Facing down the myriad threats tied to covid19," 2020, https://news.sophos.com/enus/2020/04/14/covidmalware (Accessed 9 May 2020).

[61] Ibid

[62] Ibid.

[63] F. Shi, "Threat spotlight: Coronavirus-related phishing," 2020, https://blog.barracuda.com/2020/03/26/threatspotlight-coronavirus-related-phishing (Accessed 9 May 2020).

[64] Ibid.

[65] N. Kumaran and S. Lugani, "Protecting businesses against cyber threats during covid-19 and beyond," 2020, https://cloud.google.com/blog/products/identitysecurity/protecting-against-cyber-threats-during-covid19-and-beyond (Accessed 17 June 2020).

[66] Ibid.

[67] Ibid.

[68] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, and A. Seeam, "Pervasive ehealth services a security and privacy risk awareness survey," in 2016 *International Conference On Cyber Situational Awareness, Data Analytics And Assessment* (CyberSA). IEEE, 2016, pp. 1–4..

[69] Ibid.

[70] Alex Sroxton, "German authorities probe ransomware hospital death", *Computer Weekly*, 18th Sept, 2020.

[71] Davey Winder, "Cyber attacks against hospitals have significantly increased as Hackers seek to Maximise profits", *Forbes*, 8th April, 2020.

[72] Ibid.

[73] Ibid.

Taken together, these factors have put cybercrime in the spotlight during the COVID-19 crisis as a threat impacting countries and their people around the world. Combating this threat will require strong cooperation within and across borders. Already, a number of cooperation mechanisms have been set up since the outbreak of the coronavirus in order to deal with the rising cybercrime challenge that transcends national borders. For example, the COVID-19 Cyber Threat Coalition was established to bring together cyber security practitioners who have volunteered their time to share cyberthreat intelligence.[74] Another entity, the CTI League, connects the cyber security community to law enforcement agencies, with the particular purpose of protecting life-saving sectors from cyber attacks during the course of the COVID-19 crisis. The League produces intelligence feeds, analyses attacks, and works with relevant agencies to 'take down' cybercriminals.[75] Governments are also enhancing and establishing new mechanisms to boost cooperation between criminal justice actors. In the US, the FBI established a COVID-19 Working Group in March 2020; this comprises hundreds of personnel, and is dedicated to boosting the investigation of and response to COVID-19-related crime.[76] In June, Europol announced the launch of the European Financial and Economic Crime Centre (EFECC) to support EU member states and EU institutions on issues related to financial and economic crime, noting that law enforcement authorities would need more support to follow the 'money trail' as part of their investigations into cybercrime and other forms of crime.[77] Multilateral organizations such as INTERPOL and the UN are also boosting their efforts to educate participating countries on COVID-19-related cybercrime.[78]

DIGITAL ORGANISED CRIME – INDIAN PERSPECTIVE

Cyber crime has become an organised criminal network in the country with groups hiring hackers and establishes best business practices and professional business to increase the efficiency of their attacks against enterprises and consumers. This new class of professional cyber-criminal spans the entire system of attackers, extending the reach of enterprise and consumer hearts and fuelling the growth of online crime.

Mr. Tarun Kaura, Director for solution product management for Asia Pacific at Symantec said they had extensive resources and a highly skilled technical staff, who operate with such efficiency that they maintain normal business hours and even take the weekends and holidays off.[79] Some cyber criminal attackers even create call centre operations to increase the impact of their scams, he added. With a young demographic, millions of mobile connections, rapid adoption of cloud and increasing integration of ICT in critical infrastructure, India continued to be a top source as well as destination for cyber attacks, he noted. "Once considered the spam capital of the world, India had seen a steady decrease in the amount of spam originating from its borders", he said[80], adding, the country however continued to rank as the third top source of overall malicious activity, including spam, malware and polishing hosts. The United States and the United Kingdom were the top two sources.[81]

There seems to be a trade-off between two kinds of cybercrime, the one cyber-dependent and the other cyber-enabled. Cyber-dependent crime occurs when technical penetration of an individual computer or a network of computers is integral to the commission of the crime; in other words, the crime would not be able to happen without this penetration. Cyber-enabled crime occurs when the scale of criminal activity is greatly increased by computer technology, but the actual crime is a variant of existing criminal behaviour; scamming would fall into this category.[82] Also, cyber-enabled crime is rampant in the physical world (one need only think of street con-artists), but has been enlarged in geographic scope and in the size of potential profits thanks to online markets.

The trade-off is due to the fact that contexts that see higher levels of cyber-dependent crime (such as advanced economies and countries with high levels of computer literacy) are also those where a greater awareness of cyber security exists among ordinary computer users. There is therefore less scope in these contexts for unsophisticated online scams to be successful. In contrast, when a country offers low yields from cyber-dependent crime (owing perhaps to a weak currency and/or limited household earning potential), there is greater room for deceiving unaware internet users through cyber-enabled scams. India is particularly vulnerable in this regard, with new digital payment systems being introduced to reduce the amount of untaxed or 'black' money in circulation. While beneficial for the country and economy as a whole, e-payment technologies pose a serious hacking risk. It has been estimated that mobile transactions in the country will be worth one trillion dollars by 2023.[83] Unless there is a marked improvement from 2020 levels of cyber-security awareness on the part of Indian smartphone users, the South Asian nation will become perhaps the world's biggest target for online scams. This is because the widespread penetration of English-language devices will render India vulnerable to international cybercriminals. In contrast, China, despite its comparably huge population, would most likely be shielded by strong internet controls built on pre-existing surveillance systems, as well as having a more inaccessible language.[84]

Most cybercrimes feature at least some degree of victim participation, making it difficult to draw a clear distinction between cyber-enabled and cyber dependent criminality. Perhaps a useful definition might be that if a crime is committed with one-off victim participation against a well-protected target, and is reliant thereafter solely on technical means, it is a cyber-dependent crime. If a measure of ongoing human interaction is present, and levels of security are poor, it is cyber-enabled.

The Indian context features a few examples of cybercrimes with low human interaction, but the majority of offences registered in the country, or originating from it, involve

[74] Joyce Hakmeh and Emily Taylor, Allison Peters and Sophia Ignatidou, "The Covid-19 pandemic and trends in technology", Chantham House, 16th February, 2021.

[75] Ibid.

[76] Ibid.

[77] Ibid.

[78] Ibid.

[79] Charles Cooper, "Is the Mafia Taking Over Cyber Crime? Not Really", *Symantec*, 15 August 2018.

[80] Ibid.

[81] Ibid.

[82] Rick Sarre, Laurie Yiu-Chung Lau and Lennon YC Chang, "Responding to cybercrime: current trends", *Police Practice and Research*, 19, 6, 2018, pp 515–516.

[83] Ayeshea Perera, Why India's financial system is vulnerable to hacks, BBC, 15 November 2019.

[84] Ibid.

extensive use of deception against a human target. The technical sophistication of these crimes is low, while the level of human interaction is high (lowtech/high-interaction). This brings one to the trade-off mentioned earlier: cyber-dependent crimes are characteristic of societies with a high level of digitization and a technologically aware population. Those who commit such crimes expect that they will have to overcome strong suspicions and make many attempts before they can smooth talk or phish their way into a victim's bank account. So, they rely on a technology-heavy approach with minimal human interaction. They conduct research into the psychological and technical profiles of their anticipated victims, as in the case of Tecnimont SpA, to score an instant success.

Cyber-enabled crimes, on the other hand, (with the exception of online child sexual exploitation, for example) usually depend on the susceptibility of their victims to being deceived.[85] The less advanced the level of digitization in a society, the easier it is to defraud people who have only recently purchased a smartphone or computer but have little understanding of how it could compromise their private information. Such crimes are less discriminating and adopt a mass-based approach in which the perpetrators make multiple synchronized efforts to defraud victims, aware that only a small percentage of these efforts need to actually pay off in order to turn a profit.

A large-scale cybercrime enterprise provides a good illustration of how legitimate and illegitimate components of a business model can mix, with the former covering up for the latter. During the first decade of this century, one such enterprise, Innovative Marketing Inc (IMI), which originated from the United States, became a prototype of the kind of online scams that are now growing increasingly widespread in India.

The case of IMI is similar to what later transpired in one of India's biggest call-centre scams, the Mira Road scam (discussed later). Like Ukrainian programmers who worked for IMI, some of the Indians working in junior capacities for call centres that scam Westerners may not know that they are part of a criminal enterprise. Even if they have their suspicions, they keep silent about these and prefer not to seek clarifications that could potentially threaten their source of livelihood. A cybercrime operation that is multi-layered, with different levels of awareness and culpability, fits with what researchers have discovered about the global trade in data: an entire 'parallel economy' exists to service scamming. The division of labour between different functional specialists occurs here just as it does in legitimate businesses. In 2019, law-enforcement agencies across Eastern Europe broke up a network called GozNym, named for its use of a combination of Nymaim malware and the Gozi ISFB banking trojan.

Although police spokespersons described GozNym as a consolidated entity, some of its members appear to have been freelancers recruited through online chat forums. The main trait they shared was their use of the Russian language. But that in itself did not imply centralized control. It seems that those arrested had worked according to a loosely structured model, behaving more like external consultants than gang members. That being said, many network members still remain at large, so the complete picture on GozNym is not yet clear.

An ordinary person is suffering as fraudsters can easily access her digital wallet, internet banking and newly created UPI identity. There's no solution for such frauds, as there is no central authority to respond to cybercrime.

State Police handles Cybercrime-related matters, but fraudsters are sitting miles away, sometimes outside the state or union territory and many a time outside India. So, what recourse can an individual take if she has been duped online or harassed by scamsters via encrypted VOIP calls? While such crime can be reported on the national portal set up by the ministry of home affairs, ultimately it falls within the state police's domain. And, there is little to no co-ordination between police authorities across state lines. The police of that state could shield the local mafia, and the police where the crime occured would have little authority over the matter.

Another issue is tracing money sources. When it comes to vishing crimes, fraudsters use bank accounts of people who are either not aware of the entire operation or agree to such scams for a share. The Netflix series Jamtara was one such example of organised vishing crime. However, there are plenty of Jamtara like towns in India. Another type of attack is lottery schemes where vishing techniques are used by sending videos on WhatsApp, and users are duped into calling an unknown WhatsApp number. When users call this number, an initial deposit is requested from users to collect the lottery amount. Fraudsters request an initial payment of Rs 25,000-30,000.

Open source intelligence analysis reveals geolocation of criminals to be remote villages in states of Maharashtra, Jharkhand, Bihar, Chhattisgarh, West Bengal and the modus of operandi is to target consumers of another state. Since there is no central cybercrime coordinating or responding agency in India, resources with the states police departments are also limited.

Organised cybercrime is mushrooming in India at an exponential pace. Hence to tackle and respond to such frauds services providers, such as telcos, insurances companies, banks will have to bundle security services with leading security companies. Since not everyone in India could pay extra for digital security, the government also needs to step in.

Studies have found that unlike job-seekers of the 1980s and 1990s, who were prepared to accept any kind of work and had few qualms about some jobs being beneath them, today's Indian youth carry a sense of entitlement. They are prepared to remain unemployed rather than accept a job that they feel does not match their educational qualifications. This attitude has driven many into temporary work in the call-centre business, where they get to practise salesmanship skills as a prelude to entrepreneurship, which is increasingly regarded as a respectable way of earning a living. Even so, it must be emphasized that the role of Indian nationals in digital crime is weighted towards that of foot soldiers and recruited enablers (data thieves who do not have the technical skills to remotely penetrate a network, but must have physical access to its systems). The country has struggled to produce quality software from its own research-and-development base. Consequently, it lacks the local talent

[85] Soumyo D Moitra, "Cybercrime: Towards an assessment of its nature and impact", *International Journal of Comparative and Applied Criminal Justice*, 28, 2, 2004, p 106.

needed to move very high up the value chain of cybercrime, from cyber-enabled to cyber-dependent.

Most indications are that cybercrime in India originated not with out-of-work computer programmers, as it did in Eastern Europe, but with frustrated employees of the off shoring sector. It was only later, in the mid-2010s, that IT graduates started to get into cybercrime once finding jobs became difficult. Initially clustered around large IT hubs, such as Pune and Gurugram, cyber-enabled scams spread to the countryside. The reason was sociological: as the lure of working in ITes companies diminished (especially for client-facing roles), vacant positions were increasingly filled by domestic migrants from the rural hinterland. These new employees had even fewer skills than their predecessors, but they discovered the techniques and profitability of social engineering. At a time when scams targeting Western countries were beginning to pop up in large Indian cities, migrants from rural areas were able to observe the success of telephone-based fraud. They subsequently brought these techniques back to their home towns and villages. This time, however, instead of defrauding foreign nationals, they targeted Indian citizens. The most notorious examples of copycat cyber-criminality were clustered in the district of Jamtara, in Jharkhand, a province of central-eastern India.

After interviewing several low-level employees of call centres who were likely to be engaged in illegal activity (i.e. phone scams), Indian journalist Snigdha Poonam summarized their dystopian and self-exculpatory logic in the following terms: ‘As young men with no prospects, they are the biggest victims – and the whole world is a big scam.’95 Through her investigative reports, Poonam found that the unemployment crisis in India was acute and many youths were so desperate for work that they did not bother to ask questions of a potential recruiter. They had no loyalty to their employers, and did not expect any in return. It was easy in this situation for a low-tech cybercrime industry to take root in the country, despite the best efforts of the government to preserve the integrity of data and the reputation of the ITes sector. Cyber-enabled crime in India became a two-level business.

Multiple government schemes enabled for Digital Payments must have a strong mechanism to report frauds. Similarly, companies linking digital payment methods enabled by the government such as UPI must have some liability in case frauds happen due to security weaknesses in their systems. Programmes to make consumers are aware of security-related risks must be launched, informing users of new cybercrime trends and making her aware of such practices. The regulatory bodies such as RBI, NPCI need to expand their security monitoring capability and update their security guidelines to tackle threats.

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

India has made significant investments in establishing the National Critical Information Infrastructure Protection Center (NCIIPC) in accordance with section 70A of India’s IT (Amendment) Act, 2008. Its aim is to regulate and raise information security awareness among the critical sectors of the nation rather than technology interventions. It started off with only five sectors, though other countries like the US, the UK, the UAE, etc. have considered more than ten sectors as Critical National Infrastructure (CNI), that are essential for society and economy. Non-critical systems/sectors are taken care by CERTIN. While India’s National Cyber Security Policy (NCSP) published in 2013 set the tone for formulating a comprehensive effort for protection of CII, there is still no clarity with regard to coordination mechanism between organizations such as of NCIIPC, NTRO and CERT-IN, among other agencies mentioned in the policy, specifically with regards to protection of critical Infrastructure.

With the current geopolitical situation prevailing in India, we should strengthen our IT laws to check the growing crime on the World Wide Web. India should participate in as many international conventions and MLAT treaties and increase the number of MoU’s with international agencies to curb cybercrime menace from adversaries. We need to work on bringing laws rather than guidelines, which are enforceable and deterrent in nature. Cybercrimes should be treated as acts against national security if needed. Policies need to be rephrased and effective legal frameworks need to be put in place as part of the overall strategy to counter cyber offences. There is a need to issue practical policies on protecting the critical infrastructure of the nation and clearly define roles and responsibilities of each agency mentioned in the policy. It is essential to address private CII operators about whom they should be accountable to in the event of cyber-attacks. The center has to identify and operationalize sectoral CERTs to tackle cyber threats in specific sectors. The need for standards on critical infrastructure protection (CIP) needs a detailed roadmap. Certainly, the public and private partnership is crucial for sharing cyber security information, but there should be an approach to facilitate the coordination between security firms and initiate new campaigns on recommendations towards technology verge.

Centers like “Cyber Swachhta Kendra” are steps towards the right direction in creating a secure cyber ecosystem. But it would need a lot more background work to create a realm of tools that citizens trust and use to protect their sensitive data. Though we have forensic science laboratories (FSL) to conduct digital forensic investigations, the center should also facilitate crime investigation labs focusing on specific domains under cyber security, viz., dark web monitoring, open source intelligence, crime against children and women and other malware attacks. As a first level of defense in cybercrime and cyber security, implementing a security operations center (SOC) with adequate people, process and technology are essential to strengthen the institutional framework. Initiatives taken by the Government of India under the Ministry of Home Affairs formulated two new divisions17 to thwart cyber fraud and check radicalization, namely, Counter Terrorism and Counter Radicalization (CTCR) Division and Cyber and Information Security (CIS) Division. The objective of CTCR is to devise strategies and prepare action plans for combating terrorism, whereas CIS has been created for monitoring online crimes and counter threats like online frauds, dark net, hacking, identity theft, etc.

DIGITAL ORGANISED CRIME – INTERNATIONAL PERSPECTIVE

Cyber organized criminals have engaged in a variety of cybercrimes, including fraud, hacking, malware creation and distribution, DDoS attacks, blackmail, and intellectual property crime such as the sale of counterfeit or falsified trademarked products (e.g., apparel, accessories, shoes, electronics, medical products, automobile parts, etc.) and the labels, packages, and any other identifying designs of these products.[86] These types of cybercrimes cause financial, psychological, economic, and even physical harm (especially counterfeit electronics and automobile parts, as well as falsified medical products, defined by the World Health Organization as "deliberately/fraudulently misrepresent their identity, composition or source"), and have been used to fund other forms of serious crime, such as terrorism.

Criminal groups that engage in cyber organized crime also provide services that facilitate crimes and cybercrimes (crime as a service), such as data and identity documents (e.g., financial and health data, passports, voter registration identifications); malware (i.e., made to order or known malware - e.g., Zeus, a banking Trojan, designed to surreptitiously capture users' banking details and other information needed to log in to online accounts); distributed denial of service (DDoS) attacks and botnet services; keyloggers; phishing/spear phishing tools; hacking tutorials; and information about vulnerabilities and exploits and instructions on how to take advantage of these.[87] For instance, the Shadowcrew, "an international organization of approximately 4,000 members … promoted and facilitated a wide variety of criminal activities [online] including, among others, electronic theft of personal identifying information, credit card and debit card fraud, and the production and sale of false identification documents" (*United States v. Mantovani et al*., criminal indictment, 2014).

Organized criminal groups have also profited and/or otherwise benefited from illicit products and services offered online. For example, the creator of the Butterfly Bot advertised this malware online as capable of taking control of Windows and Linux computers.[88] The creator of the Butterfly Bot also sold plug-ins that modified the functions of the malware, and also offered to create customized versions of the malware for paying customers.[89] Various online criminal networks deployed the Butterfly Bot, the largest application of this malware resulted in the Mariposa botnet, which infected 12.7 million computers around the world.[90]

Cyber organized criminals also provide *bulletproof hosting* services, which enable criminals to utilize servers to commit cybercrime and does not remove criminal content from these servers.[91] Because of low trust in criminal transactions online and the existence of scammers, *escrow services* provided by cyber organized criminal groups are high in demand. These escrow services enable the funds criminal customers pay for illicit goods and services to be sent only after they confirm that the goods or services they paid for were received in good order.[92]

Illicit goods and services are primarily purchased with *crypto currency* (i.e., "a digital currency that utilizes cryptography for security reasons").[93] There are numerous crypto currencies on the market (e.g., Bitcoin, Litecoin, Dogecoin, Ethereum, and Monero, to name a few). While most darknet markets primarily use Bitcoin, other crypto currencies (e.g., Ethereum and Monero) are being utilized, and in some cases, preferred over Bitcoin.[94] Certain darknet sites use what is known as a 'tumbler', which sends 'all payments through a complex, semi-random series of dummy transactions … making it nearly impossible to link … [a] payment with any … [crypto currency] leaving the site'.[95]

Furthermore, cyber organized criminals also provide *money-laundering* (i.e., "the process whereby criminals conceal and legitimate illicit funds") as a service.[96] The proceeds from the services provided by cyber organized criminals are also laundered. Money-laundering involves three stages: placement of illicit proceeds in financial system (*placement*), concealment of the origin of illicit funds (*layering*), and reintroduction of funds into the economy with concealed origin (*integration*). Money is laundered utilizing *digital currency* (i.e., unregulated currency only available virtually); prepaid credit and debit cards (even Bitcoin-based cards); gift cards; money mules' bank accounts; fake name/shell company bank accounts; PayPal accounts; online gaming

[86] Albanese, Jay (2018). Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. Presentation at *International Academic Conference: Linking Organized Crime and Cybercrime.* A conference hosted by Hallym University and sponsored by the United Nations Office on Drugs and Crime (UNODC), 8 June 2018; Broadhurst, Roderic (2018). Malware Trends on 'Darknet' Crypto-markets: Research Review. *Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology*; Europol (2018). *Internet Organised Crime Threat Assessment 2018.* Maras, Marie-Helen (2016). *Cybercriminology*. Oxford University Press.

[87] Broadhurst, Roderic (2018). Malware Trends on 'Darknet' Crypto-markets: Research Review. *Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology*; Maras, Marie-Helen (2016). *Cybercriminology*. Oxford University Press.

[88] Mariposa Botnet "Mastermind" Jailed in Slovenia. *BBC News,* 24 December 2013.

[89] FBI (2010). *FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators.*

[90] Mariposa Botnet "Mastermind" Jailed in Slovenia. *BBC News,* 24 December 2013.

[91] National Cyber Security Centre, 2017, p. 8.

[92] Ibid.

[93] Maras, Marie-Helen (2016). *Cybercriminology*. Oxford University Press,p.337.

[94] Broadhurst, Roderic (2018). Malware Trends on 'Darknet' Crypto-markets: Research Review. *Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology*; Europol (2018). *Internet Organised Crime Threat Assessment 2018*; US Department of Justice (2017). *AlphaBay, the Largest Online 'Dark Market' Shut Down.*

[95] *United States v. Ross William Ulbricht*, Criminal Complaint, 2013, p. 14

[96] Maras, Marie-Helen (2016). *Cybercriminology*. Oxford University Press,p.337.

sites (via virtual gaming currency); and illicit gambling sites.[97]

According to Europol, cyber organized criminals are also utilizing semi-automated crypto currency exchanges (known as *swappers*) and decentralized (peer-to-peer) exchanges, which do not require the identification and verification of users (pursuant to Know Your Customer requirements for regulated financial institutions) to launder criminal proceeds. Moreover, cyber organized criminals have found new and creative ways to launder money, such as Uber "ghost journeys" (i.e., drivers receive funds from money launderers to accept ride requests from Uber accounts at a prearranged price without the launderers actually using the service), and fake Airbnb rentals (i.e., money launderers pay Airbnb owners without staying at their property).[98] Furthermore, cyber organized criminals engage in *micro laundering* "a process whereby criminals launder large amounts of money by engaging in numerous small transactions". Online, these types of transactions can occur on commercial sites, auctions sites, and even employment sites.[99]

Furthermore, cyber organized criminals have utilized information and communication technology (ICT) to facilitate various forms of traditionally offline organized crime activities, such as the smuggling of migrants and trafficking in persons, wildlife, drugs, firearms, and cigarettes trafficking. For instance, the smuggling of migrants, which is defined under Article 3(a) of the United Nations Protocol against the Smuggling of Migrants by Land, Sea and Air of 2000, supplementing the Organized Crime Convention as "the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident", has been facilitated by smugglers' use of ICT to advertise, recruit, communicate with, and ultimately sell their services to migrants

DEVELOPMENT OF SECURITY IN TECHNOLOGICAL WORLD AND LEGAL FRAMEWORK

UNICRI is working on the field of cybercrime to achieve a better understanding of the phenomenon, in order to formulate ad hoc prevention policies, develop security methodologies and techniques, and strengthen the capacities of the actors involved in investigating and prosecuting cybercrimes.[100]

Cybercrime and Cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on Cyber security[101] addresses cybercrime as one major challenge underlines this. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services.[102] Enhancing Cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.[103]

In 1994, the United Nations Manual on the Prevention and Control of Computer Related Crime noted that fraud by computer manipulation; computer forgery; damage to or modifications of computer data or programs; unauthorized access to computer systems and service; and unauthorized reproduction of legally protected computer programs were common types of computer crime.[104] While such acts were often considered local crimes concerning stand-alone or closed systems, the international dimension of computer crime and related criminal legislation was recognized as early as 1979. A presentation on computer fraud at the Third INTERPOL Symposium on International Fraud, held from 11 to 13 December 1979, emphasized that 'the nature of computer crime is international, because of the steadily increasing communications by telephones, satellites etc., between the different countries.'[105]

Although organised criminals have been exploiting opportunities presented by information and communications technologies since at least the 1980s, our report suggests that it is only now that we are at a tipping-point for the power and reach of organised digital crime. The internet is now a key facilitator for organised crime, and criminals are ruthlessly exploiting the increasing ubiquity of mobile devices, wireless internet, and radio frequency identification (RFID) technologies (like Oyster Cards and contactless bank cards).

Though new digital crime empires are not yet consolidated, we can disrupt and prevent them, providing that we re-shape our assumptions about what digital crime is, who its perpetrators are, and address the true nature of the threat.

[97] Europol (2018). *Internet Organised Crime Threat Assessment 2018*; Maras, Marie-Helen (2016). *Cyber criminology*. Oxford University Press,p.337; McMullan, John and Aunshul Rege (2010). On Line Crime and Internet Gambling. *Journal of Gambling Issues*, Vol. 24, 54-85.

[98] Busby, Matta. (2018). Cyber laundering: from ghost Uber rides to gibberish on Amazon. *The Guardian*, 17 May 2018.

[99] Maras, Marie-Helen (2016). *Cyber criminology*. Oxford University Press,p.337.

[100] United Nations Interregional Crime and Justice Research Institute. See Website: http://www.unicri.it/special_topics/cyber_threats/cyber_crime/

[101] UNGA Resolution: Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[102] With regard to development related to developing countries, see: ITU Cyber security Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cyber security/docs/itu-cyber security-workprogramme-developing-countries.pdf.

[103] See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cyber security, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cyber security, including combating spam, available at: www.itu.int/ITU-D/cyb/cyber security/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cyber security/cyber security.pdf.

[104] United Nations, 1994. UN Manual on the Prevention and Control of Computer Related Crime.

[105] INTERPOL, 1979. Third INTERPOL Symposium on International Fraud, Paris, 11-13 December, 1979.

A very large proportion of digital crime is carried out not by lone actors but by organised groups. In fact, 80 per cent of digital crime may now originate in some form of organised activity.

There are six main types of organised groups, which appear to be reflected in about four-fifths of current digital crimes. Traditional organised crime hierarchies feature here alongside newer types of crime networks. They exist on a spectrum, dependent on their level of organisation, and whether their activity is purely aimed at online targets, uses online tools to enable crimes in the "real" world, or mixes online and offline targets.

BAE Systems Detica and The John Grieve Centre have unveiled a major piece of research revealing that 80 per cent of all digital crime now originates from organised crime groups. On and offline crime worlds are converging and perpetrators are now just as likely to be street gangs, drug traffickers or established crime families as those traditionally associated with digital crime such as ID fraudsters or hacking syndicates.[106]

Kenny McKenzie, Head of Law Enforcement at BAE Systems Detica said: "Organised criminal activity has now moved from being an emerging aspect of cyber crime to become a central feature of the digital crime landscape. Our report shows that more and more criminal activities now rely upon the online world and that a significant proportion – 80 per cent - of the volume of serious crime now occurring online has clear associations with groups which display various levels of collective co-ordination, purpose and capacity… As digital crime continues to grow, increased partnership between law enforcement and technical experts – as well as the private sector – will be critical."[107]

For law-enforcement agencies, some of the more concerning developments are the evidence of hybrid organisations which combine on and offline offending and where new and old forms of criminality converge. New and unpredictable opportunities for crime are opening up as a result.

Digital crime is widely assumed to trans-jurisdictional, in contrast to more localised organised crime. But even the most traditional crime networks have long stretched across borders, and while organised digital crime can operate from anywhere it is again a mistake to assume this is always the case.

In fact, organised digital crime networks operate at varying levels of proximity. Close circles of family and friends continue to be significant, as are local and regional networks. Interpol has identified distinct regional hubs operating in northwest, northeast and southwest Europe, while at the global or transnational level networks exist centred on: the Americas; China, India and the Far East; and Nigeria and West Africa.

The popular image of the "cyber criminal" – the youthful 'computer geek' scheming remotely in his bedroom, is far removed from the 'mafioso' with an extended family network and propensity for face-to-face violence. However, contrary to what one might anticipate, digitally-enabled crime goes far beyond hacking, and our assumptions about the youth and skill level of digital criminals are skewed. More organised digital crime members are over 35 years old (43 per cent) than are under 25 years old (29 per cent).[108] This is partly a result of wider computer literacy, but also a "deskilling" of digital crime with the availability of "crime ware" which can be easily distributed or purchased online. These toolkits offer everything from ready-made viruses to exploit the vulnerabilities of individual systems to "botnets" which control large networks of hijacked computers. As many as 80 percent of all viruses may now originate in this way. Low tech tools such as pre-pay phones, library computers, and even old fax machines are also playing an increasing role in digital crime.

Another erroneous assumption is that organised digital crime relates only to distributed, non-hierarchical 'networks' with no links to traditional crime families – who are often perceived to lack the technical expertise, rely on physical and geographical proximity and the use of force, and target a different set of victims.

Legal measures play a key role in the prevention and combating of cybercrime. Law is dynamic tool that enables the state to respond to new societal and security challenges, such as the appropriate balance between privacy and crime control, or the extent of liability of corporations that provide services. In addition to national laws, at the international level, the law of nations – international law – covers relations between states in all their myriad forms. Provisions in both national laws and international law are relevant to cybercrime.

When asked to report legislation relevant to cybercrime, countries referred to a number of laws, including: criminal codes; laws on high-tech crime; criminal procedural codes; laws on wiretapping; evidence acts; laws on electronic communications; laws on security of information technologies; laws on personal data and information protection; laws on electronic transactions; cybersecurity acts; and laws on international cooperation.

In today's globalized world, the law consists of a multitude of national, regional and international legal systems. Interactions between these systems occur at multiple levels. As a result, provisions sometimes contradict each other, leading to collisions of law, or fail to overlap sufficiently, leaving jurisdictional gaps.[109]

Cybercrime is by no means the first 'new' form of crime to engage multiple jurisdictions and laws. Illicit trafficking flows in drugs, people and weapons, for example, frequently originate and end in different hemispheres, passing through many countries in between. Nonetheless, cybercrime acts can engage legal jurisdictions within the timeframe of milliseconds. Computer content, for example, can be legally stored on a computer server in one country, but downloaded through the internet in multiple countries, some of which may consider the content to be illegal.[110]

[106] Eshel, Tamir, *Organised Crime In The Digital Age*, Defence Update, 28th March, 2012.

[107] Dunn, Jophn E., *Cybercrime dominated by organised gangs, academic study finds World in "Fourth era" of organised crime*, TechWorld, 28th March, 2012.

[108] Interview with a Delh-based police official, 23rd December, 2020.

[109] Sieber, U., 2010. Legal Order in a Global World. In: Von Bogdandy, A., Wolfrum, R. (eds.) Max Planck Yearbook of United Nations Law, 14:1-49.

[110] Sieber, U., 2008. Mastering Complexity in the Global Cyberspace. In: Delmas-Marty, M., Pieth, M., and Sieber, U. (eds.) Les chemins de l'harmonizationpénale. Paris, pp.127-202 (192-197).

There are three main scenarios when it comes to identifying the applicable instrument for international cooperation. First, relevant procedures can be part of international agreements, such as the United Nations Convention against Transnational Organized Crime (UNTOC)[111]and its three protocols, or regional conventions, such as the Inter-American Convention on Mutual Assistance in Criminal Matters[112], the European Convention on Mutual Assistance in Criminal Matters[113] and the Council of Europe Convention on Cybercrime.[114] The second possibility is for procedures to be regulated by bilateral agreements. Such agreements in general refer to specific requests that can be submitted and define the relevant procedures and forms of contact as well as the rights and obligations of the requesting and requested states. Australia, for example, has signed more than 30 bilateral agreements with other countries regulating aspects of extradition. Some negotiations of such agreements have also addressed cybercrime as a topic, but it is uncertain to what extent the existing agreements adequately govern cybercrime. If neither a multilateral nor a bilateral agreement is applicable, international cooperation generally needs to be founded on international courtesy, based on reciprocity.

The main international instrument for judicial cooperation in criminal matters is the United Nations Convention against Transnational Organized Crime (UNTOC). This convention contains important instruments for international cooperation, but was not specifically designed to address cybercrime related issues. Nor does it provide specific provisions dealing with urgent requests to preserve data.

It's far more likely that the crimes of the future will assume a shape that's difficult for us to imagine at the moment. The Internet has developed a new set of specialized tools that make running an illegal operation easier than ever before. Organized crime has always meant having your fingers in lots of different pies, so it's natural that the Web would appear a new and fruitful frontier to be divided up, using as many parallel scams as possible. To accomplish that, old-school syndicates will need highly educated recruits.

The decentralized nature of international law, particularly in the sphere of criminal law enforcement, may explain the Convention's accommodation of flexible harmonization to achieve law enforcement goals aimed at the timely eradication of cybercrime. Having a sense for "what will fly" in the international body politic, heavily dependent upon cultural understandings and differences, must always be a practical and necessary concern.

However, cybercrime prosecutions will most certainly raise issues relating to concurrent jurisdiction and/or the application of domestic law to foreign nationals. While the particular offense conduct may be properly circumscribed, the means of investigating and prosecuting the conduct will not be predictable.

In its present form, the Convention allows state intrusions into the sphere of individual privacy rights to gather evidence for use in subsequent criminal prosecutions without adequate guarantees of procedural due process. In this way, the Convention on Cybercrime could become a blueprint for future international endeavours to harmonize penal law enforcement.

[111] Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: Smith, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

[112]Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

[113]European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

[114]Council of Europe Convention on Cybercrime, ETS 185.