खण्ड VII
वर्ष 2021

Volume VII
Year 2021

Rajasthan Police Academy
सत्यमेव जयते
Security, Justice & Peace

रक्षिण्

RAKSHIN

A Journal of Rajasthan Police Academy

ISSN 2230-8288

Online Safety and Police Response to Cyber Crimes

Editor-in-Chief

Guest Editor

Editorial Board

Annual Subscription

India	Abroad
For individual: Rs. 150	For individual : £15
For institution : Rs. 200	For institution : £20

Disclaimer

No part of the 'Rakshin' journal may be used or reproduced in any form without permission from the Editor. Neither the Editor, nor the publisher assumes responsibility for the articles or opinions in the papers printed. The views expressed in signed articles an other materials are personal opinions of the contributors and not of the Rajasthan Police Academy.

Address
C/o The Director, Rajasthan Police Academy, Nehru Nagar,
Jaipur-302016 Rajasthan Tel. 0141-2303222, 2302131,
FAX: 0141 -2301 878
www.rpa.rajasthan.gov.in

रक्षिण्

RAKSHIN

खण्ड VII
वर्ष 2021

Volume VII
Year 2021

विषय-सूची /CONTENTS

Message from DGP Rajasthan

Editorial by Editor-in-Chief

1. **Cybercrime**
Dr. Arjun Singh, Associate Professor, School of Computing & IT
Manipal University, Jaipur

2. **Online Safety and Role of Police – Myriad challenges call for radical interventions?**
Ranjeet Rane, Technology Policy Researcher and
Varun Menon, Associate, Reserve Bank Innovation Hub (RBIH)

3. **Frauds in Cyber Space – Knowledge and Mitigation Strategies**
Dr. Rajveer Singh Shekhawat, Dean, Faculty of Engineering & Director,
School of Computing & IT, Manipal University, Jaipur

4. **Cyber - Sextortion/Catfishing – an evolving form of Cyber - Crime in Mewat region. Understanding the need for a multi-agency concerted effort to counter the menace.**
Tejaswani Gautam IPS, S.P. Alwar and
Vikas Sangwan IPS, ASP, (North), Alwar

5. **Online Gender Based Violence during Covid-19 Lockdown – A Longitudinal Study**
Dr. Amrita Duhan IPS, S.P., Pratapgarh (Rajasthan)

6. **Vulnerability of Cyberspace**
Ranjeeta Sharma, IPS, Astt. Superintendent of Police, Jodhpur

7. **Deepfakes and Detection Mechanisms During COVID 19**
Dr. Ananth Prabhu G, Dr. Anush Bekal, Harisha K, Sahyadri College of
Engineering & Management, Mangaluru, Karnataka

8. **Tools for Law Enforcement for Monitoring Tor Traffic**
Dr. Emmanuel S. Pilli and Pulkit Chandel
Department of Computer Science & Engineering
Malviya National Institute of Technology, Jaipur

9. **Book Review: Essentials of Online payment security and Fraud Prevention**
Digant Anand, IPS, DCP (West), Jodhpur Commissionarate

Contributors / लेखकगण

Dr. Amrita Duhan IPS, is Superintendent of Police, Pratapgarh, Rajasthan

Dr. Ananth Prabhu G, is Professor and Principal Investigator Digital Forensics and Cyber Security CoE, Sahyadri College of Engineering & Management, Mangaluru, Karnataka

Dr. Anush Bekal, is Associate Professor & Head, Department of Electronics and Communication, Sahyadri College of Engineering & Management, Mangaluru, Karnataka

Dr. Arjun Singh, is Associate Professor, School of Computing & IT, Manipal University Jaipur

Dr. Emmanuel S. Pilli, is Associate Professor, Department of Computer Science & Engineering, Malviya National Institute of Technology, Jaipur

Digant Anand, IPS, is Deputy Commissioner of Police, Jodhpur (West)

Harisha K, is Assistant Professor and Co-Principal Investigator, Digital Forensics and Cyber Security, CoE Sahyadri College of Engineering & Management, Mangaluru, Karnataka

Pulkit Chandel, is M.Tech. Computer Science & Engineering, (III Semester), Department of CSE, Malviya National Institute of Technology, Jaipur

Dr. Rajveer Singh Shekhawat, is Dean, Faculty of Engineering & Director, School of Computing & IT, Manipal University, Jaipur

Ranjeet Rane, is Technology Policy Researcher

Ranjeeta Sharma, IPS, is Astt. Superintendent of Police, Jodhpur

Tejaswani Gautam IPS, is Superintendent of Police, Alwar, Rajasthan

Varun Menon, is Associate, Reserve Bank Innovation Hub (RBIH)

Vikas Sangwan IPS, is Assistant Superintendent of Police, (North), Alwar

Message from DGP Rajasthan

I am pleased to note that the latest edition of Rakshin focuses on one of the most germane issues being handled by the law enforcement agencies. Computers and IT were purposed to achieve high performance levels in every sphere of human activity. But today, the increasing use of technology for activities which cause financial loss, social embarrassment or loss of functionality is a worrying trend and a high-priority concern for the police.

The anonymity and ability to operate remotely offered by technology provide a major advantage to the new-age criminals. Technology today influences our lives today in more ways than we actually perceive or appreciate. While the spectrum of services now available through or dependent on IT is expanding swiftly, the low public awareness levels towards safe usage have exposed the vulnerability of a large section of the society to the cyber thugs. The police face the challenge of upgrading their own professional competence to outsmart such criminals, not only to detect such crimes but also to implement effective preventive strategies.

Alive to the situation, the effort of Team-Rakshin in spreading the light of awareness on contemporary aspects of this unremitting problem, is a mark of our resolve to work relentlessly in ensuring peace and safety in society, in both the physical as well as the cyber realms. I convey my best wishes towards this publication.

(M.L. Lather)
Director General of Police
Rajasthan

Editorial

Cyber Crimes are the most challenging and fastest growing crimes today. Incidents of credit card frauds, phishing, sextortion & so on are becoming everyday news item. The use of cyber space has extended to human trafficking & arms trade also. Activities on Dark Web remain a serious concern for all law enforcement agencies.

In this background there arises a need for law enforcement agencies to not only be aware of the existence and methodology of such crimes but also to identify, track, and locate the cyber criminal(s) by appropriate use of technology and apprehend them from their hideouts for the purposes of investigation.

Other key concerns for police are protecting the citizens from becoming a victim of financial cyber-crimes, protecting the nations critical infrastructure and corporate organizations from data theft and ransomware.

While the State and its agencies continuously strive for minimizing the gap between the capabilities of law enforcement and the technology and techniques used by cyber criminals, through systemic up gradation and better training for police officers, the chasm remains as law enforcement agencies struggle to keep pace with technology changes.

With research and publication on relevant issues becoming a priority area at the Academy, need was felt to bring out an issue of 'Rakshin' that focussed on Online safety and Police response to cyber crimes. The current issue, dwells upon many such related issues and intends to bolster the understanding of our readers, with the ultimate objective of promoting online safety & induce critical thinking on this subject.

The articles in the current issue relate to subjects like role of police in online safety, frauds in cyberspace and mitigation strategies, cyber sextortion, a study of online gender based violence during Covid times, the vulnerability of cyberspace, investigating Tor traffic and the challenge of deepfakes.

A common outcome of various articles is the need for building capacity to check the menace of Cyber Crimes and to increase public awareness especially regarding safety measures to prevent such crimes.

I sincerely thank all the distinguished members from the Academia, researchers from team RBI and Police officers for their contribution to this issue and wish them all the very best in their endeavours.

I also thank Dr. Rajveer Singh Shekhawat of the Manipal University Jaipur for his key support as the Guest editor of this issue & making this issue a reality.

As we tread on the path of learning, research and excellence in training, we solicit support from the fraternity of learners, researchers and practitioners for our cause.

We would appreciate suggestions and comments from our readers and welcome contributions for future issues of our journal 'Rakshin'.

Rajeev Sharma, IPS
Editor-in-chief,Rakshin&
Director,Rajasthan Police Academy

Rakshin, Volume VII - Year 2021

Cybercrimes: An Introduction

Dr. Arjun Singh, Associate Professor, School of Computing & IT
Manipal University, Jaipur

Abstract:

With the growing use of computers in society, cyber crime has become a major issue. Humans are now dependent on the internet for all of their needs as a result of technological developments. People now have access to everything while sitting in a single area thanks to the internet. The internet allows people to do whatever they want, including social networking, online shopping, online schooling, online jobs, and everything else they can think of.

Cybercrime is different from other kinds of societal offences. This is because it has no limits, and cyber criminals are anonymous. Everyone is affected, from the government to industry to the ordinary population. Because of the growing use of technological tools, cybercrime is on the rise in India. This article aims to provide a thorough introduction of cybercrime, its many kinds, Amendments, and an analysis of cybercrime in India. Furthermore, we examine different strategies for combatting cyber crime in India.

Keywords: *DoS, Intrusions, cyberbullying, cloning, email spoofing, SMS spoofing, Cyber laws*

Introduction:

Cybercrime is a sweeping word that refers to criminal conduct in which computers or computer networks are utilized as a tool, a goal, or a location for criminal activity. It can range from electronic wracking to denial-of-service assaults. It is a broad word that encompasses crimes like phishing, credit card fraud, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children through chat rooms, scams, cyber terrorism, virus generation and or dissemination, spam, and so on.

It also includes traditional crimes in which computers or networks are utilized to facilitate illegal conduct. Cybercrime is on the rise, and it is increasingly fashionable to make money by making fraudulent phone calls or to get revenge by hacking into other people's accounts.

Types of Cybercrimes

Cybercrime encompasses a wide range of actions. Cybercrime may be broadly classified into three types:

- Cybercrimes against persons like Harassment occurs using internet.
- Cybercrimes against property like computer or network resources hacked.
- Cybercrime against the government, such as Terrorism via the internet.

A. Crimes against persons

Cyberbullying

Cyberbullying refers to the use of computer technology to create a physical threat that causes anxiety, such as the internet, e-mail, phones, text messages, webcams, websites, or movies.

Distribution of Obscene Material

This includes obscene exposure/pornography (essentially child pornography) and maintaining a website that contains these illegal items. These filthy elements may damage the adolescent's psyche and tend to deprave or corrupt their mind.

Defamation

Defamation can be understood as the wrongful and intentional publication of something either in the written or oral form about a person to harm his reputation in the society. For a statement to be considered as defamatory, the following essential elements must be fulfilled.

- There must be the publication of the defamatory statement, which means coming to the knowledge of a third party.
- The statement must refer only to the plaintiff
- The statement must be defamatory in nature.

Defamation can be divided in two categories-

I. Libel A statement that is defamatory and is published in a written from.

ii. Slander A defamatory statement spoken that means a verbal form of defamation.

Hacking

It refers to illegal control/access to a computer system, and the act of hacking fully destroys all data and computer programs. Hackers frequently target telecommunications and mobile networks.

Cracking

It is one of the most severe cybercrimes to date. Cracking indicates that a stranger has gained access to your computer systems without your knowledge or approval and messed with sensitive personal data and information.

E-Mail Spoofing

A spoofed e-mail is one that falsely portrays its origin. It demonstrates that its origin is distinct from where it truly originates.

SMS Spoofing

SMS spoofing is a technique that allows us to change the sender information on a text sent via the short message service (SMS) system. SMS text messages are used by cell phones, personal digital assistants, and similar devices and are typically just known as text messages.

When you send a spoof text, they replace the originating mobile number (sender ID) with alphanumeric text. In simpler words, SMS spoofing allows you to change the sender's display number. As it allows you to change the originator details, it's also regarded as "SMS originator spoofing."

Carding

False ATM cards, that is debit and credit cards, are used by criminals to obtain monetary benefits by fraudulently withdrawing funds from the victim's bank account. In this form of cyber crime, there is always illegal usage of ATM cards.

Cheating & Fraud

It indicates that the individual doing cybercrime, such as stealing passwords and data storage, did it with a guilty conscience, which leads to fraud and cheating.

Child Pornoraphy

It involves using computer networks/ mobiles to create, distribute, or access materials that sexually misuse juvenile children.

Assault by Threat

It refers to threatening a person with fear for their life or the lives of their family over a computer network, such as E-mail, videos, or phones.

B. Crimes against Property

As international trade expands, firms and consumers are increasingly adopting computers to generate, transport, and retain information in electronic form rather than conventional paper papers.

Some offences affect the person's property

Intellectual Property Crimes

IP crime is more generally known as counterfeiting and piracy. Counterfeiting is, wilful trademark infringement, while piracy involves, wilful copyright infringement. These are very similar and often overlapping crimes. IP crime is not a new phenomenon but due to globalization and advances in technology counterfeiting and piracy has become big business.

4 Cyber Squatting

It refers to when two people claim the same Domain Name, either by asserting that they registered the name first and have the right to use it before the other or by doing anything close to that before. For example, www.yahoo.com and www. yaahoo.com are both similar names.

Cyber Vandalism

Vandalism is the intentional destruction or damage of another person's property. Thus, cyber vandalism refers to the destruction or damage of data when a network service is terminated or disrupted. It may encompass any physical harm done to any person's computer within its scope. These crimes may include the theft of a computer, a computer component, or a peripheral connected to the computer.

Hacking Computer System

Hacktivism affects popular websites such as Twitter and blogging platforms by gaining unauthorized access to or control of the machine. There will be data and computer loss as a result of the hacking activities. Furthermore, research suggests that such assaults were not primarily meant for financial gain or to harm the reputation of a certain individual or organization.

Transmitting Virus

Viruses are programs that attach themselves to a computer or a file before spreading to other files and computers on a network. They generally have an impact on the data on a computer by changing or destroying it. Worm assaults have a significant impact on people's computerized systems.

Cyber Trespass

A person is guilty of computer trespass if s/he intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer network, computer program, or data. Computer trespass is directed generally towards computer hackers.

Internet Time Thefts

Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person knowledge. You can identify time theft if your Internet timehas to be recharged often, despite infrequent usage.

C. Cybercrimes against Government

Certain offences are committed by groups of people who seek to threaten foreign governments by exploiting internet facilities. It includes the following:

Cyber Terrorism:

Cyber terrorism is a big source of concern both at home and throughout the world. Terrorist assaults on the Internet typically take the shape of distributed denial of service attacks, hate websites and hate e-mails, attacks on critical computer networks, and so on. Cyber terrorist operations undermine the nation's sovereignty and integrity.

Cyber Warfare

It refers to malicious hacking and espionage for political purposes. It is a type of information warfare that is sometimes compared to conventional warfare; however, this comparison is debatable due to both its accuracy and political motive.

Distribution of pirated software

It entails transferring pirated software from one computer to another to erode government data and records.

Possession of Unauthorized Information

Terrorists may easily obtain any information via the internet and use that information for political, religious, social, or ideological purposes.

Analysis of Cybercrimes in India

With over 560 million internet users, India is the world's second-biggest online market, after only China. It is expected that by 2023, the country will have over 650 million internet users. According to recent NCRB data, 27, 248 incidents of cybercrime were recorded in India in 2020.

According to the FBI's study, India ranks third among the top twenty cyber crime victims. The central government's national cyber crime reporting platform (cybercrime.gov.in), launched last year, has received 33,152 complaints, resulting in the filing of 790 FIRs. According to a 2020 study, Indian customers lost more than 18 billion US dollars due to cybercrime.

Origin of Cyber Crime

Criminals used telephone lines to conduct crimes regularly around the start of the 1970s. Phreakers were the culprits. Cyber crime did not exist until the 1980s. One individual had access to another person's computer to locate, copy, or modify personal data and information. Lan Murphy, better known as Captain Zap, was the first person to be convicted guilty of cyber crime in 1981. He had hacked the American telephone company to alter its internal clock, allowing consumers to make free calls during peak periods.

Cyber Laws

The Information Technology Act of 2000 was enacted with the primary goal of creating a conducive environment for business usage of I.T. The IT Act defines the offenses that have been rendered criminal. The Indian Penal Code, 1860, has also been modified to include cybercrime inside its jurisdiction.

The following are the numerous internet-related offenses that have been made criminal under the IT Act and the IPC:

Cybercrimes under the IT Act

Tampering with Computer source documents - Sec.65

Hacking with Computer systems, Data alteration - Sec.66

Publishing obscene information - Sec.67

Un-authorized access to protected system Sec.70

Breach of Confidentiality and Privacy - Sec.72

Publishing false digital signature certificates - Sec.73

Cyber Crimes under IPC and Special Laws

Sending threatening messages by email - Sec 503 IPC

Sending defamatory messages by email - Sec 499 IPC

Forgery of electronic records - Sec 463 IPC

Bogus websites, cyber frauds - Sec 420 IPC

Email spoofing - Sec 463 IPC

Web-Jacking - Sec. 383 IPC

E-Mail Abuse - Sec.500 IPC

Cyber Crimes under the Special Acts

Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act

Online sale of Arms Arms Act

Conclusion

We live in a digital era, and cyberspace is not restricted to one's limits; rather, it encompasses the entire globe. As a result, cybercrime is on the rise in all nations, including India. The most difficult aspect of cybercrime is its dynamic character due to the continuing growth of digital technologies. As a result, new cybercrime tactics and approaches emerge. Thus, cybercrimes should be treated as seriously as any other type of crime in our society, such as theft, rape, or murder.

References:

- Alazab, M., & Broadhurst, R. (2015). The role of spam in cybercrime: Cybercrime Risks and Responses, 103- 120. https://doi.org/10.1057/9781137474162_7
- Alsmadi, I. (2019). Cyber intelligence. The NICE Cyber Security Framework, 75-90. https://doi.org/10.1007/978-3-030-02360-7_5
- Bernik, I. (2014). Cybercrime. Cybercrime and Cyberwarfare, 1- 56. https://doi.org/10.1002/9781118898604.cp
- Boes, S., & Leukfeldt, E. R. (2016). Fighting cybercrime: A joint effort. Cyber-Physical Security, 185-203.https://doi.org/10.1007/978- 3-319-32824-9_9
- Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.
- DCMS: Cybersecurity breaches survey 2019. (2019). Network Security, 2019(4), 4. https://doi.org/10.1016/s1353-4858(19)30044-3
- Doyle, C. (2011). Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws. DIANE Publishing.
- Grimes, R. A. (2017). Hacking the hacker: Learn from the experts who take down hackers. John Wiley & Sons.
- Grispos, G. (2019). Criminals: Cybercriminals. Encyclopedia of Security and EmergencyManagement, 1- 7. https://doi.org/10.1007/978-3-319-69891-5_80-1
- Gupta, S. (2019). Ethical hacking terminologies. Ethical HackingLearning the Basics. https://doi.org/10.1007/978-1-4842-4348-0_1
- Howard, P. N., & Gulyas, O. (2014). Data breaches in Europe: Reported breaches of compromised personal records in Europe, 2005- 014. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2554352
- Krausz, M., & Walker, J. (2013). The true cost of information security breaches and cybercrime. IT Governance Publishing.
- Moore, M. (2016). Cybersecurity breaches and issues surrounding online threat protection. IGI Global.
- Rajan, A. V., Ravikumar, R., & Shaer, M. A. (2017). UAE cybercrime law and cybercrimes An analysis. 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security). https://doi.org/10.1109/cybersecpods.2017.8074858
- Shea, J. M. (2012). Combating computer viruses. Gareth Stevens Publishing LLLP.

*****

Rakshin, Volume VII - Year 2021

Online Safety and Role of Police – Myriad challenges call for radical interventions?

Ranjeet Rane, Technology Policy Researcher and
Varun Menon, Associate, Reserve Bank Innovation Hub (RBIH)

Abstract

The past decade has seen a steady growth in the access to internet in the country. The mix of affordable devices and low data tariffs facilitated the on boarding of first time users to different platforms like social media portals, payment gateways and smartphone applications almost seamlessly. This technology adoption has brought in its wake the scaling up of cybercrime in the country as well. The nature and scope of these malicious activities are ever evolving and Law Enforcement Agencies are faced with myriad challenges. In this article the authors have attempted to understand the different concepts associated with online safety and the role that Police leadership can play in respond to new forms of crimes, social disorder and disinformation campaigns.

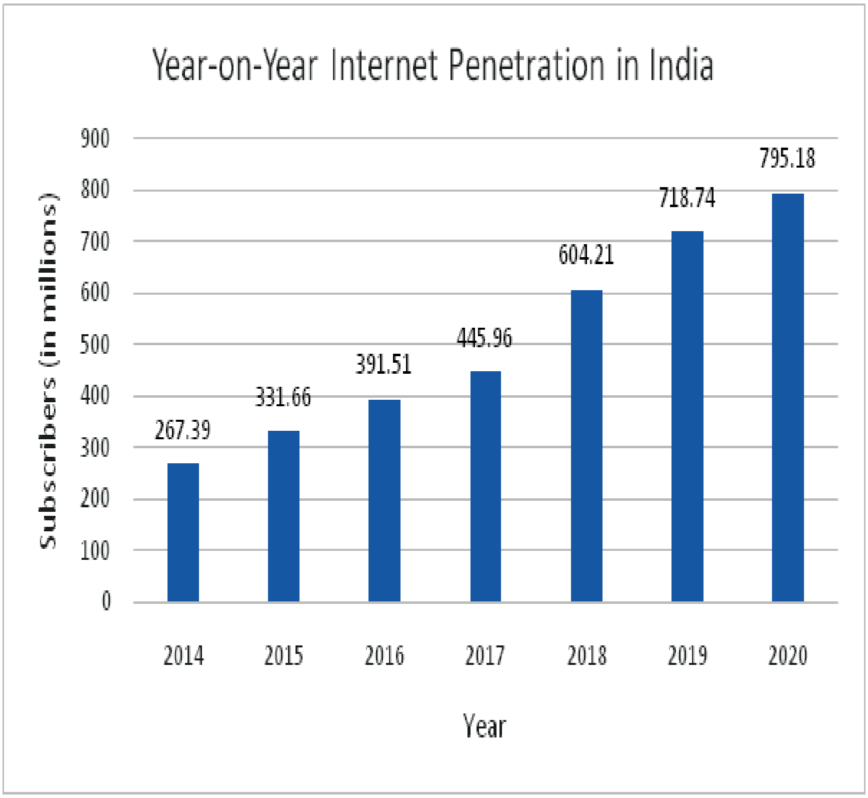
Keywords:
Cybercrime, Online Safety, Cyber Policing, Disinformation, Cyber Policing.

Introduction

As the COVID-19 pandemic began impacting lives and livelihood from the beginning of 2020, there was another pandemic of sorts that was slowly but surely making its impact felt on the lives of citizens. Much like the COVID19 pandemic, this information or cyber pandemic affected people of different age groups, socio-economic status and levels of digital know how in different ways. While for some it meant becoming victims of payment scams, for others it was getting exposed to the dark underbelly of cyber stalking or even been targeted by phishing emails for some.

Another worrying aspect was that of rampant misinformation campaigns, that included the entire ambit of fake news, rumours on chat applications, hateful content and pseudo-scientific remedies to tackle the COVID19 infection. As lock-down's forced citizens to move to online platforms for almost everything, the lack of awareness and digital know how manifested into a malice of sorts. While the pandemic may have been an immediate trigger for these concerns to show up in higher numbers, it was in making for over a decade.

Driven primarily by affordable mobile devices, low cost internet connections and mushrooming of local language content, the penetration of internet access in India has grown many foldsin the past decade. A snapshot of the same is presented in Fig 1.



Source: (Telecom Regulatory Authority of India 2014-2020)

This growth bought in its wake a steady rise in the instances of cybercrime, particularly those that led to financial loss of some degree. The nature of the loss made it an urgent issue to address for law enforcement agencies and policy makers alike. A slew of measures spanning legal amendments and technical regulations were mandated to address this issue. However, the safety and security of citizens is not restricted only to financial frauds in the cyber space.

There are other facets to ensuring online safety of citizens at large. In the ensuing sections, we will look to define these facets, discuss the existing legal and other provisions available to address the harm perpetuated through them and then delve upon the alternative approaches that can be adopted in particular by the law enforcement agencies.

What constitutes Online Safety?

The internet is a vast network and can be extremely over whelming for anyone using it for the first time. Owing to this, discussions around online safety usually tend to revolve around children, young adults and senior citizens. However, the idea of online safety spans across age groups, gender and socio-economic status. This is a problem that has manifested itself in different forms for different individuals and continues to baffle law enforcement agencies as well. The first step in this regard would therefore be to unwrap the different concepts under the larger umbrella of online safety and then proceeding to address each one of them.

Cyber Bullying

As is the case with real world bullying, cyber bullying also involves the use of intimidation tactics by one or more individuals through the use of electronic communication to bully anindividual or group, typically by sending messages of an intimidating or threatening nature(Ministry of Home Affairs 2018). It encompasses intimidation and emotional harassment. There may be a threat of defamation by exposing intimate details about the target individualas well as possible social exclusion. Children have been known to be targeted on social media platforms, chat applications and even on forums by such bullies(Lal and Jha 2020). However, the problem is not limited to children alone, women and individuals of the LGBTQ community have come out vocally against such harassment off late. As per data from the National Crime Record Bureau (NCRB), cases of cyber bullying filed under Sec 354D of the Indian Penal Code (IPC) has shown a steady increase year on year. The worrying aspect here is that most of the cases do not get reported and this data may only be an indicator of the underlying problem.

Online sexual abuse and exploitation

The scope of this criminal activity is very wide, starting from sexual harassment over chatting applications (sexting) it can include acts like aggressive sexual solicitation, blackmailing and financial extortion, production and consumption of child pornography as well as commercial exploitation and human trafficking (Ministry of Home Affairs 2018). There are legal provisions against such crimes which are invoked time and again against the perpetuators, however the issue at hand is that the internet offers a high degree of anonymity for those with the right set of tools and this is exploited by criminals to evade detection and arrests. Furthermore, evidence of such activities is difficult to gather as it may be stored on devices located out of the country. After financial frauds, this issue has got the highest attention from a law enforcement perspective, however as cyber criminals come up with newer ways to exploit victims, LEA personnel would need to up skill themselves as well.

Cyber Radicalisation

A grim constant on theever-expanding list of cyber issues, radicalisation using the internet has always been on the radar of LEA personnel for radicalisation towards terrorism and allied activities. The ISIS is known to have recruited individuals from across the globe to carry out terrorist attacks using internet chat rooms and social media platforms (Shukla 2020). Off late, political agents are utilizing such platforms to spread hateful content and push for ideological polarisation, leading to violent events such as riots or lynching (Bhushan 2018). Localised events may go unnoticed but the threat to social cohesion is real.

Online Crime/Frauds

This category has been in the spotlight owing to the high degree of financial loss associated with it. It includes in its ambit, insertion of malicious software, exposure to inappropriate content, identity theft, data breach, consumption of pirated media, and payment frauds with varying modus operandi. There are provisions in the Information Technology (IT) Act and the IPC that can be invoked to penalise different offenses. The wide ambit of malicious activities covered in this category have been addressed in a piecemeal manner over the past decade. State capacity is a serious issue in tackling these crimes and hence, cyber criminals appear to be a few steps ahead of the LEA when it comes to these crimes(Kini 2018).

Prevalent Techno-Legal provisions to address Online Safety

The Information Technology Act (2005) was aimed at comprehensively addressing the issue of cybercrime for citizens and organizations alike. The Act defines different types of crimes and lays down the penal provisions against them. This act has been the main stay in the fight against cyber criminals and ensuring online safety of citizens. The Supreme Court of India in 2015, struck down some provisions of the act like the section 66A with the intention to enable Freedom of Speech over social media platforms(Sriram 2015). The act in its current form is now seeming inadequate to address issues of online safety particularly those involving use of digital payment channels.

Other legal provisions that are frequently used in conjuncture with the IT Act are as follows:

Sec 384 IPC- *Punishment for extortion. - Whoever commits extortion shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.*

Sec 503 IPC- *Criminal intimidation.-Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which* *he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intim-idation.*

506 IPC- *Punishment for Criminal Intimidation-Whoever commits the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years or with fine, or with both.*

If threat be to cause death or grievous hurt, etc.- And if the threat be to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or imprisonment for life, or with imprisonment for a term which may extend to seven years, or to impute, unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

Sec 354D IPC - *Stalking (includes Cyber Stalking, Cyber Bullying of Women)- Any man who-follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; ormonitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking.*

Sec 469 IPC - *Forgery for purpose of harming reputation-Whoever commits forgery, intending that the document or electronic record forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.*

Sec 91 CrPC *which has been used buy LEA to gather technical evidence such as call data logs, IP addresses, transactions records etc.*

Technical measures primarily are focused on access to information from servers or data centres located outside of Indian geographical boundaries and chat transcripts across end to end encrypted chat platforms. The data requests from social media platforms have been routed through complex multilateral agreements and timely assistance to LEA from such platforms has been a bone of contentions. Similarly, lack of effective co-ordination between telecom service providers, banks, payment gateways and aggregator platforms mean that cyber criminals continue to recycle fake documents to acquire new SIM cards and create fake identities to carry out their actions. The debate about end to end encryption been made absolute by chat applications has also been active in public discourse over the past two years. Towards this the recently released guideline for intermediaries' mandate that due diligence and grievance redressal mechanisms under Part II of the rules be followed by the intermediaries. The due diligence to be observed by the intermediaries include

(i) informing the users about regulations and rules, terms and conditions and privacy policy for usage of its services

(ii) prevent access to unlawful information within 36 hours upon an order from the government or the Court

(iii) retain user information collected during registration for 180 days after withdrawal or cancellation of registration. The digital media publishers and intermediaries must provide for grievance redressal mechanisms.

The intermediaries are required to assign a grievance officer to address complaints against violation of rule which must be acknowledged within 24 hours and disposed of within 15 days. Part III of the rules describes the code of ethics and safeguards for digital media publishers.

Moving beyond the status quo

The issue of online safety of citizens is assuming importance with every passing day. It may even be prudent to raise this to the same level as physical safety because our online identities are now a manifestation of our physical self. The status quo as it stands has piecemeal provisions to cater to the problem at hand. While some do not look at the issue in a holistic manner – gender neutrality is missing in some of the provisions, others have been outpaced by technological developments – hacking as a concept is now obsolete in the face of personal data residing on multiple devices across geographies simultaneously.

A one-size-fits-all approach will

not work in face of such dynamics. The need of the hour therefore is to leverage a mix of legal interventions, technology adoption and specialized recruitment/training to be able to provision online safety as a public good for citizens. This would put online safety as non-rivalrous and non-excludable good provisioned for citizens at large. Such an approach will ensure that the access to preventative and remedial measures are equitably available to citizens.

On the legal side, it may be prudent to fast track the long due harmonisation of legal provisions to ensure that they are in tune with the current scenario. This would entail amending existing laws, scrapping redundant provisions and inserting sunset clauses where an anticipated change in technology may call for a review of existing provisions. Framing news laws may be avoided unless no other alternative is available. The upcoming Personal Data Protection law will also play a significant part in how the legal provisions, particularly the penal ones are shaped to act as a deterrent. Owing to fast paced nature of such crimes, the laws should focus on ensuring surety of punishment over severity.

Technological advancement in crime needs to be effectively countered with technological advancements on the law enforcement side as well. Automation of repeated tasks will go a long way in bringing much needed efficiency and ensure that the scare and highly trained manpower is utilised for work requiring expert intervention. The entire process starting from reporting, issuing of CrPC notice, evidence documentation, identification of fraudulent documentation / phone/account numbers, blacklisting such details and making all of this data searchable will help to cut through the long wait times, give citizens an interface to record and track their complaints without ever having to interact with LEA personnel and help private organisations, sector regulators and nodal agencies to have access to data for evidence based policy formulation in future.

Existing recruitment processes of LEA need to factor in the changing dynamics of the cyber world. All levels of recruitment need to facilitate intake of individuals with well-defined cyber skill sets, these may not always be of technical, but legal, psychological, and cyber forensic to name a few. A suggested measure is to provision for a mandatory 1% intake of cyber specialists across all entry points with immediate effect and gradually increase this to 5% over the span of a decade. This will help shape up a cadre of in-house personnel who while been trained and conditioned for policing duties, will primarily be assigned for tasks related to cyber issues.

The role played by Police personnel across all rank and file will be crucial in ensuring that the citizen of the country feel secure online. This will necessitate some targeted interventions spanning short to long term outcomes.

Way forward for LEA (Role of Police in Future)

As immediate interventions, the existing social media awareness campaigns been run by different police units need to be co-ordinated across a single forum, this will allow for a common message to go out, albeit with modifications in content to suit regional and linguistic differences. The pooling of resources will allow for hiring of professional agencies with expertise in communication and influencing choice through application of behavioural nudges. The outcomes from such campaigns need to be tangibly defined and tracked through an independent audit. Feedback received should then be utilized to make these campaigns more effective.

As advised earlier automation of record keeping processes needs to be initiated preferably under the existing Indian Cyber Crime Coordination Centre (I4C) and expedited in a mission mode over the next two years to enable a comprehensive cyber fraud registry. The Cyber Co-ordination (Cy-cord) centre setup by the Ministry of Home Affairs can be leveraged for this intervention. The data collated from the recently launched helpline and reporting platform for preventing financial loss due to cyber fraud can also be funnelled into this registry. This will ensure that small value – high volume frauds are handled at prevention level, saving crucial time and manpower in investigation and prosecution phases.

There is also a need to undertake multi phased sensitisation of police personnel with regards to engagement with victims of cyber bullying, stalking and other aforementioned criminal acts. Victim shaming can deter such individuals from seeking justice through proper channels. Recent surveys have shown that victims do not report such incidences, the reasons behind this hesitancy needs further research and actionable interventions in the medium term.

Citizen facing service delivery like passport verification, issuance of NoCs, permissions for processions etc. need to be automated at the earliest. The e-Pass feature run seamlessly during lockdowns in 2020 can be replicated at scale for these requests. There have been numerous recommendations about this intervention but very little action. Freeing up police force from such administrative tasks (The Bureau of Police Research & Development (BPR&D) had identified 45 such tasks in 2017)will allow personnel to focus on up skilling and training to tackle new age challenges.

There is a need for negotiating a clear set of guidelines with social media and other intermediaries so that swift data sharing can be achieved. Radical measures like asking for private keys for e2e encrypted communication will be stoned walled through court proceedings, leading to further delays. Training of police personnel to ask for data in required format, automating the submission of these requests and mapping compliance of platforms through a public facing dashboard will nudge better compliance. In the long term, the BPR&D can release data request reports similar to those released by the intermediaries today. This will increase transparency and aid policy formulation in future.

Conclusion

Provisioning of a safe cyber experience is undoubtedly a daunting task for all the stakeholders involved. There is a general sense of acknowledgement to address this issue, however the level of coordinated effort and long-term planning and execution that will ensure that citizens can be assured of certain degree of online safety independent of their age, gender or socio-economic background is still lacking.

As technology adoption leap frogs the laws and regulations that have been in place for more than half a century, the need for a systematic overhaul is evident now more than ever. The upcoming Personal Data Protection law could be the first step towards this. Police organisations would also need to initiate the process to imbibe cyber policing capabilities into their recruitment and training programmes. In the near future, the nature of policing may undergo a paradigm shift from enforcers of the law to enablers of justice. Actions towards this transition will need to be imitated by the leadership of today so that personnel of tomorrow will find themselves better equipped in this role.

Note

The Authors were senior Lead, Technology Policy Research & Technology Policy Research Analyst respectively at Reserve Bank Information Technology Pvt. Ltd. (ReBIT) at the time of submission of this article.

References

- Bhushan, Shagun. 2018. Fake Messages and Death: How Social Media Giants Have Turned into Monsters Across Asia. 7 July. Accessed July 11, 2021. https://www.news18.com/news/india/fake-messages-and-death-how-social-media-giants-have-turned-into-monsters-across-asia-1804075.html.
- Kini, Ashok. 2018. Cyber Criminals Are Way Ahead Of The Law Enforcement Officers: Kerala HC Asks State Police To Train Cops To Tackle Cyber Crimes. 4 November. Accessed July 11, 2021. https://www.livelaw.in/cyber-criminals-are-way-ahead-of-the-law-enforcement-officers-kerala-hc-asks-state-police-to-train-cops-to-tackle-cyber-crimes-read-judgment/.
- Lal, Vidisha, and Anoushka Jha. 2020. Existing landscape of sexual harrassment online. Survey, New Delhi: Digital Empowerment Foundation.
- Ministry of Home Affairs. 2018. A Handbook for Adolescents / Students on cyber safety. Manual, New Delhi: Ministry of Home Affairs.
- Shukla, Manish. 2020. ISIS trying to recruit terrorists online, raises concern for Indian security agencies. 9 July. Accessed july 11, 2021. https://zeenews.india.com/india/isis-trying-to-recruit-terrorists-online-raises-concern-for-indian-security-agencies-2294700.html.

- Sriram, Jayant. 2015. "SC strikes down 'draconian' Section 66A." The Hindu, 24 March. Accessed July 11, 2021. https://www.thehindu.com/news/national/supreme-court-strikes-down-section-66-a-of-the-it-act-finds-it-unconstitutional / article 10740659.ece.
- Telecom Regulatory Authority of India . 2014-2020. The Indian Telecom Services Performance Indicators. New Delhi: TRAI.

*****

Frauds in Cyber Space – Knowledge and Mitigation Strategies

Dr. Rajveer Singh Shekhawat, Dean, Faculty of Engineering & Director, School of Computing & IT, Manipal University, Jaipur

Abstract:

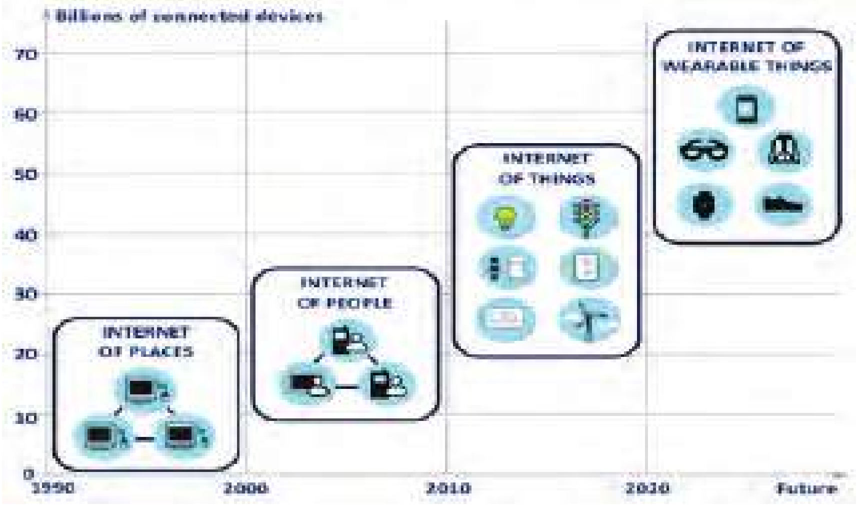
Information technology has crept into our daily lives during last two decades. The low cost of all pervasive connectivity and data sharing over internet has empowered citizens immensely to efficiently carry out their daily activities in personal lives and business domain. The pandemic period has accelerated this phenomenon and has made the cyber space inalienable part of our lives. Every technological paradigm has, however, its flip side as well and the same applies to cyber space. The freedom of free exchange of sensitive information is being misused by the hackers on the prowl. In this article, I shall delve into the technological developments that helped to evolve the connected society, what are the specific tools and platforms used for the same. The article further broadly details the categories of attacks and their nature. I shall also briefly summarize the nature of fraudsprevalent in India. The article concludes by providing some insight into the remedial actions, preventive measureslike creating awareness through training.

Keywords: frauds, cyber-attacks, malware, ransomware, hackers

1. Introduction

Human beings have a multi-faceted character and include both honest and dishonest individuals. For a smooth and pleasant living, society has many unwritten rules which urge its members to abide by these. But there are situations which make people to adopt unfair means like cheating, frauds to attain their objectives. And these behaviours are in existence since times unknown. Early days of internet and web technologies did not offer much incentives to farudsters. However, hackers enjoyed cracking passwords and went to the extent of installing root kits and taking over the servers and workstations causing frustration to the owners. Except for theft of sensitive data and information, no bigger causes were behind such nefarious activities. The open source platforms like Linux were less prone to viruses and malware than windows for the simple reasons that there was much commercial activity based on Microsoft driven machines then open source. In modern times, regulations have been brought in to punish people for their misdeeds and the quantum of punishment is supposed to be commensurate with the gravity of offence/fraud. Thus, a well agreed definition has to be in existence. A short definition of fraud is outlined in Black's Law Dictionary [Sunder2014]: An act of intentional deception or dishonesty perpetrated by one or more individuals, generally for financial gain". One may many a times report fraud which may have been a system error or inadvertent mistake on part of the agency. There are very clear rules to decide if the financial or personal information compromise has resulted from a mistake or system error or malfunction. Many a times, individuals or organizations may not be even aware that a fraud has taken place. Detecting a fraud using data analytics is like finding the proverbial needle in the haystack. Many of the frauds these days take a shape of extortion or ransom, the latter have been more prominent during the pandemic years.

This article covers enabling technologies and paradigms which has led to proliferation of online frauds. As evident, there were lesser number of them before the onset of information age in 2000. Section 3 delves into support systems, software, tools and platforms that make it easy for users to engage with online services. Many of do's and dont's and more detailed terms and condition of their use increase the propensity of common users not to fully understand the data sharing dangers to online platforms and thus once affected do not have much leverage to defend themselves legally of their actions. Next section provides an insight into frauds and their nature. What are the various mechanisms employed by fraudsters and hackers are treated in some detail. In Section 5, I have attempted to categorize the attacks, each of which address a specific set of population due to their attitudes and cir-cumstances. The last section hinges on awareness that needs to be created in all sections of the society, preventive measures that need to be taken by our law and order machinery. Simultaneously, the knowledge of IT Act of our country especially the section addressing cyber security laws needs to prevail on all the agencies looking after the welfare of citizens including police, courts and NGOs.



2. Enabling Technologies and Paradigms

The evolution of network of computers namely internet was developed in 70s but took more than a decade to become common amongst general users. The data communication costs were still high and thus except for high-end business, not much could be thought as its use. The data was mostly traveling over telephony cables and voice always had precedence on such networks. The mobile communication revolution started from Europe, Japan and US but was slow to reach Indian sub-continent. There were not, much use of data networks then messaging. The emergence of mini-computers and later on desk top computers introduced simple games which later acquired networked users attention when people across geographies could participate in them. Some of the open source projects like ET required huge computing power which was realized with participation of user of desktop machines who allowed the spare CPU time of their machines to analyze smaller chunks of data and send back. Email communication was of course the largest service using data networks and most customers were satisfied with dial-up services, the later remaining still costly. The banking and financial institutions started using emails for sensitive financial transactions opening a door to mischievous people to evolve ways to man-in-the -middle-attacks stealing passwords and login ids. A good number of people having access to emails started getting affected by cheating invites enticing them to make phone calls or agree to share their bank details etc but still such offences and frauds were rare.

A drastic change happened when 2G (GPRS) data communication led to the emergence of much personalized data communications supported by 3G data services. With increase in bandwidth, the costs could be brought down as more people got access to them. A gradually falling cost of semiconductors and auxiliary components facilitated the mobiles in everyone's hands and a significantly lower costs in the sub-continent compared to the originating countries accelerated the use not just for communication but also for simple arcade games. The arrival of smart phones aided with 4G offering much higher data rates and compute power commensurate with visual computations integrated much powerful

camera for capture of pictures and video, led by a powerful GUI opened the door to an unimagined but multiplied applications of it including financial transactions and e-commerce.

The data communication cost were no more any hinderance to almost a 24x7 connectivity of users of all segments. Sophisticated games could now be played on such phones. The computation power started to concentrate in these small devices and multiple innovations and applications to use them started pouring in. Social networks was a major paradigm that emerged with them as a potential media to leverage frauds and ransom attempts. Sophisticated sensors sharing your location and your activities were easily accessed by hackers taking advantage of lack of knowledge of one's device and app settings that were hidden in extensive jargons of terms and conditions that accompany use of them. All this offered a ripe environment for people with ill-intent, to master the use and access to the devices and information, and starting exploiting innocent civilians and un-attentive organizations world over to pay for their negligence. Inspite of cognizance of such offenses, much little losses could be salvaged or re-claimed, by the cyber forensic experts.

3. Support Systems, Tools Software, and Platforms

One of the major factors driving proliferation of mobiles has been +open source platforms like Linux. A mobile OS derived from it, called Android has contributed significantly to the many companies designing and developing mobiles and due to free OS, costs are highly affordable for the same and have fallen significantly. Simultaneously, the software for mobiles called App has flourished well with less concerns of licensing costs. Due to big numbers, there have been free and open platforms supporting app development and distribution. Android studio aided with dockers (containerization) which provided the environment and infrastructure and that too free, has led to a huge number of apps, almost for every use starting gaming to personal health and e-commerce. The use of apps has increased immensely due to low cost unlimited data access packs offered by all service providers.

The variety of social networks offered by facebook, google and many others have led to free flow of information including personal data which is sensitive info in the hands of hackers and ransomware. The free apps are also a source of virus, trojans and malware with which user remains oblivious even after strong warnings by the distributors of apps like Play Store or AppStore.

4. Nature of frauds and mechanisms employed

Online fraud is a strategy to deceitfully steal information of a victim or a business entity through websites, e-mails, or any other internet means for fraudulent transactions, identity theft, money laundering, etc. One of the latest reports suggests that 56% of Indians generally succumb to several types of internet frauds on a regular basis. Let's have a quick look at the various types of online fraud in India:

4.1 Fraud in online banking

Online banking has brought a great comfort to our lives. But unfortunately, the more people are using net banking; the more online frauds in banking are growing. Generally, fraudsters create websites that are very similar to different legitimate financial organizations. By chance if one enters those sites, one lands up sharing his credentials with them and the fraudsters can use personal details to transfer his money from his account. Sometimes, expiring of KYC of accounts is also made a pretext to lead you to fake site or share details to help you out.

4.2 Credit card and debit card frauds

In present digital world, even credit cards and debit cards are not safe! Do you remember what happened in October 2016? SBI closed its 6 lakh debit cards when a malware-related breach was informed in a non-SBI ATM network. It affected 32 lakh debit cardholders across 19 banks! Can you imagine how grave the whole matter is?Here the scammers steal the information of your card and then use it for various online and offline transactions. Through skimming entire card information gets copied without your knowledge! While you withdraw cash in an ATM, a card trapper is attached to keep your card open after a normal transaction. Nowadays the stealing or cloning of the information of credit and debit card is one of the most increasing digital banking frauds in India.

4.3 Online shopping fraud

These days online shopping is the most favorite of the majority. It saves your time and effort as you don't need to go anywhere to buy an item, you just scroll your computer or mobile screen, place the order and you will get what you need. What can be more comfortable and relaxing than this? But here also you have to be careful as online shopping frauds in India are increasing in a rapid way.For this scammers generally give fake ads of different items with lucrative discount options. When you will click on that post they will share some fake identity proof and gain your trust. After that they will ask you to give advance payment and the courier or transportation charge. When you will make the payment, they will not answer your call or emails. They will even block you so that you cannot make any further calls or messages!

4.4 Scammers can contact you even as a buyer

At first to gain your trust they will send you some small amount of money. For further transaction they will ask your QR code. After scanning it they will withdraw the money from your account.

4.5 Social media fraud

Different social media

like Facebook, Instagram, Twitter, and YouTube are burgeoning day by day. Consequently, the scammers are also using these social media making countless users as their victims. Fraudsters generally create fake profiles to present themselves as legitimate persons and to trap people in their tricks. These scammers can even hack your original profile and reach people using your profile.

4.6 Fake technical support

This is another example of online fraud. Here, you will receive a phone call from an unknown number; the person on the other end will tell you that your computer or any other technical devices need protection. They will present themselves as technical experts. Gradually, they will convince you to share your personal details. When you will give them the necessary information they will vanish like air!

4.7 False job offer

If someone is looking for a job, he can be a potential victim of a scammer. The fraudster acquires the profile from a job portal and gets into touch offering a lucrative job. Many fall into their trap and willingly make payments or divulge bank account details.

4.8 Travel frauds

If one intends to go on holiday and thus planning a trip, beware of unsolicited offers. One receives an email which will contain some amazing offers for traveling a beautiful place. To make you believe, they will offer some details and will provide fake websites. One may easily fall prey to these offers. The payments made would reach to the fake sites which one would not find next time to track the booking.

4.9 Online dating fraud

Different online dating apps like Tinder, Gleeden, and Bumble are gaining huge popularity. Online dating has become a norm in these days. But in this quest of a romantic relationship, it is highly possible that one falls unto a fraudster.The fraudster engages several times a day in the beginning and show an empathetic behavior. Gradually, he /she gets emotionally attached and get one believe all the stories. And then starts the game of financial exploitation through faking accidents, hospitalizations etc.

4.10 Mobile wallet or e-wallet fraud

Mobile wallet frauds in India have become rampant in COVID times. In this case, generally, the fraudsters target the user ID and the one-time password. When they get this information by some means, they can easily hack the account and siphon away the entire money in wallet or linked accounts.

5 Categories of attacks

Online fraud and identity theft are huge problems. Hackers are everywhere. From the lone individual in his parent's basement to state sponsored hackers from Russia and China, it's only getting worse. Like it or not, online fraud and identity theft are problems most all of us will have to experience at one time or another. Along with the discussion of fraud types, a peep into the top incentives of the same is worth considering. But we shall delve into a basic fraud which is used to propagate frauds further.

What is Identity Theft? Identity theft happens when someone steals your personal information to use for illegal activities. It happens most often through electronic means (see below). However, it also happens through methods as simple as stealing sensitive mail out of your mailbox (bank statements, etc.) or someone breaking into your home.

How Does Identity Theft and Online Fraud Happen? Online fraud and identity theft comes in many different forms. For instance, we've all gotten those emails promising millions of dollars if we help someone overseas transfer their inheritance to the US. You have also probably seen emails from PayPal or your bank saying there is a problem with your account and requesting information. They can look very official, but they are a scam.

Sometimes these attempts at fraud are very easy to spot. But if you're not careful, they can lure you into clicking a link that will download a virus to your computer. Here's a list of some of the most common methods of online fraud and identity theft:

- **Data Breaches** Data breaches happen when a hacker (or even a trusted employee) breaks into a corporate or government computer to steal data. This includes info such as credit card numbers, names, addresses, Social Security numbers, and more.

- **Skimming** Skimming happens at the point of transaction. It usually happens when an employee at a gas station, restaurant, or other business uses a hand held credit card scanner to steal your information and store it for later use.

- **Unsecure Smartphones** Smartphones are not very secure. When you make a call, use an app, send a text, or send email, someone may be monitoring those activities. With the right equipment or a malicious app, it's easy to gain access to a smartphone and steal any data on that phone.

- **Phishing** Phishing is an attempt to get you to share personal information. It usually comes in the form of an email asking for information from someone posing as your bank or other official entity. Phishing can also happen in a popup on your computer screen saying you've won a prize or a contest. The goal is to get you to click on a link that downloads a virus to your computer that gains complete access to your information.

- **Unsecure Internet Connections** Using an unsecure public wifi connection can also be a problem. Since it's public and unsecured, others can monitor your activity and gain access to your computer. Be very careful about what networks you use.

6 Awareness, Preventive Measures and IT Act 2000

The awareness quotient of people affected by cyber attacks, identity theft and social hacking (?) etc plays a major role in avoiding or nullifying the attacks. There are frequent govt advisories being issued on radio, TV, SMS, emails and also on their web sites. Banks and financial institutions also keep on updating their customers about safe ways of accessing their sites including virtual keypads and two factor authentication. News papers also carry articles written by experts to beware of unsolicited but tempting offers which make one to divulge sensitive personal and financial data. These can help one to avoid falling into traps laid by hackers and fraudsters.

In case one has got into a trap, we list and describe the 15 most useful ways to prevent frauds in the first place and some can help to mitigate and resolve the case:

- **Protect Your Passwords** Use a different password for each online account. Keep them protected using an online password manager. The most secure passwords contain at least 8 characters and a combination of letters, numbers, and symbols.

- **Use Cash** Debit and credit card information is always being stolen. I prefer to use cash in an envelope system for most of my transactions. Cash is king!

- **Never Give Information to Unsolicited Callers** Although there are some legitimate businesses that sell over the phone, 'many arent.

- **Keep Your Smart phone Protected** Use an antivirus app. Also use a password lock and a data deleting app that you can access from a computer if your phone is stolen. Only download apps from a trusted app store.

- **Secure Your WiFi at Home** Use secure encryption on your home network so that it can't be easily hacked.

- **Don't Click the Links** If an email is suspicious, don't click any links. If you do click a link, run a full scan with your anti virus software ASAP.

- **Keep Your Operating System Up to Date** Keep your OS and web browser up to date. Enabling automatic updates in your settings achieves this very well without having to constantly do it yourself.

- **Use a Firewall and Antivirus Software** You can also set these up for automatic scans to consistently keep your computer clean from viruses and other problems.

- **Check Your Bank Accounts Frequently** The more often you check your accounts, the more likely you are to spot suspicious activity quickly.

- **Only Buy From Online Retailers You Trust** There are tons of scam sites out there offering incredibly low prices on desirable items. If the price sounds too good to be true, it probably is scam.

- **Never Use a Public Network When Accessing Sensitive Information** Wait to get onto a secure network before checking your bank account or accessing other private information.

- **Use an Identity Protection Service** Services such as Life Lock and Identity Guard can provide constant monitoring and keep you protected if your identity is compromised.

- **Delete Suspicious Emails** When you get a suspicious email, completely delete it from your computer.

- **Don't Carry Your Identity Card** Keep it locked up in a safe place. You will almost never need to have the actual card with you.

- **Shred Important Documents** Some people will search through your trash for important documents. Shredding them provides extra security.

7 Conclusion

In this article, we have tried to put in context the online frauds, why they have increased so much and what are the causes for their proliferation. Assuming that these would stay I have also outlined how to escape from them and if you are trapped into it, how best to come out or get reported for further action. To provide enough background, I have described some of the frauds, how the ground is prepared before the final action so that one gets warned in timely manner of an imminent act of deception. A large amount of information is around us to make us informed cyber citizens notwithstanding the fact that such activities would keep on taking place and in fact would become more intensive whenever the opportunity arises.

*****

Rakshin, Volume VII - Year 2021

Cyber - Sextortion/Catfishing – an evolving form of Cyber - Crime in Mewat region. Understanding the need for a multi-agency concerted effort to counter the menace.

Tejaswani Gautam IPS, S.P., Alwar and
Vikas Sangwan IPS, ASP, (North), Alwar

Abstract

From a crime perspective, Mewat region (Primarily comprising of areas of States of Haryana, Rajasthan, Uttar Pradesh and Delhi populated majorly by a single community) since historic times has been a place known for registering high incidents of robberies, dacoities and other heinous crimes. In the present times, the region infamously known for“tatloobaazi”(a type of economic fraud or cheating done by criminals in Mewat region using the modus operandi of selling fake gold bars at low prices)has evolved and has now been infamously known for complex cyber frauds like Olx-based advertisement frauds and Cyber Sextortion (also known as Catfishing in common parlance). Sextortion generally involves an act of extortion where one dupes the victim by threatening to share one's private pictures, videos or sex chats and activities to one's friends, near relatives and family members. In many such acts, the victim, out of shame, insult and fear of rebuke does not report the same to the family members and Law enforcement agencies and continues to be harassed and extorted. In the times of social media platforms, dating applications (Tinder, Lamour), Chat messengers, this crime has given way to Cyber Sextortion. Here the anonymity, jurisdictional ambiguity of cyber-crimes, easy access to personal information and viral spread via social media provides advantage to criminals and acts as a disadvantage to victims. This paper is an attempt to enlist the methodologies used by cyber fraudsters specifically in Alwar

district of Rajasthan. Most of the findings belong to personal experiences of working in this area and through interrogation of the gangs so caught by Alwar Police in the past one year. Amongst other types of cyber frauds, this paper focuses on the modus operandi of Catfishing or Sextortion which has recently become one of the most used MO by these criminals in Mewat Region.

Cyber Extortion Flow Diagram

Before we delve into the details like stakeholders involved and how this industry functions, it is pertinent to understand the Modus Operandi through a flow diagram.

Creating Fake Facebook/ Instagram Profiles

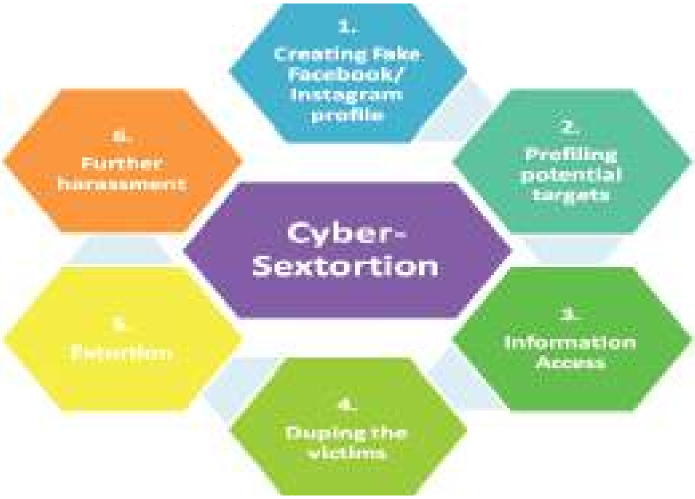
These fraudsters create fake social media profiles with pictures of young girls and add many friends to make these profiles appear as genuine.

Profiling potential targets

They screen social media profiles of young males whose details are available in open domain and filter on potential targets by assessing their financial status, located far off from fraudsters location.

Information Access

Once the friend request is accepted by the targeted profile, they get access to restricted information like pictures, friend list, comments etc. The comments are read and analyzed and based on that further requests are sent to close friends



and relatives of the victim.

Duping the victims

Normal conversation is started over messenger and slowly as the conversation grows phone numbers are exchanged to take the conversation forward. After some initial conversation on WhatsApp messages, the fraudster asks for a nude video call and most of the times youngsters get lured by it. While getting on a Video call the fraudsters generally play a pre-recorded video of a girl who exchanges some greetings like hey and then starts taking off her clothes. At the same time the girl in the recorded video makes some gestures asking the victim to take off his clothes and engage him in some intimate sexual activities. The victim, ignorant of the fact that a fraudster using the screen recorder application is recording all his acts of the video call, finally becomes a prey to them.

Extortion

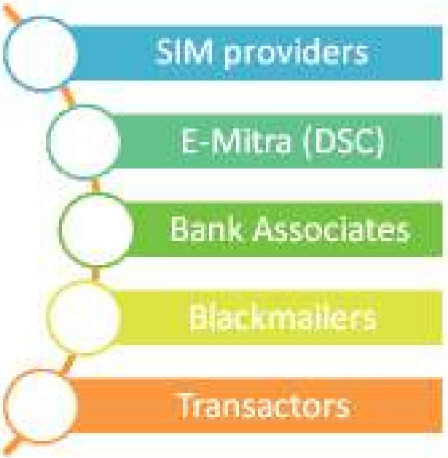
By this time the fraudster is well prepared to extort the victim, since he has access to the social media profile of victim, his friends and his nude video call recording. He takes some screenshots of the video call and shares them with the victim over WhatsApp chat warning him to send money else he would post this video to his relatives, friends. To further escalate the distress, he would take screenshots of video being uploaded on YouTube. This comes as a traumatic moment to the victim since he is shocked to know that he has been recorded and this fraudster would publish this video everywhere. He finds himself broken and ashamed and finds no one to share to explain what has happened to him and seek any redressal. The fraudster shares some Google Pay, Phone Pay, UPI ID to ask for some payment in lieu of not posting the video. Ultimately, he is compelled to pay some money as his self-respect, public image is at stake.

Further Harassment

The act of extortion is not a single instance. The duped person is extorted multiple times citing various reasons. Fraudsters ask for money in case the victim wants a proof that he has deleted his video. To further extort the person, they give calls to victim from different numbers posing themselves as Police officers from Cyber Crime Cell and asking for money if they don't want any legal action on their pornographic content. Sometimes the victim is extorted by giving calls to victim by presenting themselves as YouTube Manager and asking for money to delete the nude video uploaded on YouTube.

Cyber sextortion – An Organised Crime

The cybercrime industry has evolved itself over years and now it functions on the lines of an organized business setup where different stakeholders are involved with pre-decided work profile. The industry works on competition where competitive commission percentages are decided and paid to different stakeholders of the extortion gang. These criminal cohorts thrive on an infrastructure which is built up of fake SIM cards, fraudulently opened bank accounts, stolen mobile phones to ensure a difficult catch for Law Enforcement Agencies. It also provides an easy escape to these fraudsters from any legal hassles due to lack of KYC documents, ID Proofs, other evidences establishing their involvement in cyber frauds. We will list out some of the major stakeholders whose role must be understood to work out a Standard Operating Procedure (SOP) for investigating these crimes and ensure an 'iron fist' crackdown on each block of these cyber sextortion rackets. At the same time this understanding would form basis for a cohesive, collaborative, consistent strategy plan involving all stakeholders as a counter response to the challenge posed by these cybergangs.



SIM Providers

Based on the broad analysis done on CAF (Customer Application Forms) of the fake SIM cards made available from the members of these cyber-criminal gangs caught by us, it was found that majority (around 80%) of them have their origin from POS located in states of Assam, West Bengal and Orrisa. Even within these states it is found that some specific POS (SIM retailers) are involved in making available these fake SIM cards issued over fraudulently used Aadhar Card, Photo and other ID proofs of previous customers available in their database/ Computers at their kiosks. Most of these SIMs are brought over in the region by the truck drivers who travel to eastern India for their consignments. These are brought in bulk and then distributed to the retailer network in Mewat region. To the end user, these fraud SIMs cost anywhere between Rs.1000-Rs.3000.

E-mitra (Digital Services Centre)

A network of these government approved DSCs has propped up in the Mewat region. Almost each of these villages has four to six E-Mitra shops/kiosks setup, most of which have come up in the past few years. This number itself is an outlier to the E-mitra density in Mewat (encompassing Alwar, Bharatpur districts in Rajasthan and District Nuh-Mewat in Haryana) vis-à-vis rest of Rajasthan. These E-mitra shops are involved in activities like creating altered ID proofs, adding fake SIM numbers to Aadhar Card IDs and then using these to open fraud bank accounts and obtain SIM cards. AEPS and Card swipe machines available with these kiosks are also used by these fraudsters to withdraw money from the bank accounts. Commission at every level is fixed just like an organized business model.

Bank Associates

In several cases, it was seen that some of the bank associates especially from Private sector banks are hand-in-glove with the fraudsters and help them open bank accounts using fraud documents without much detailed scrutiny and verification. Sometimes these fraudsters also cheat the innocent laborers, poor people in name of some Government Scheme giving them money on pretext of opening a bank account. They then use their documents to open an account and hand over their account details and ATM card to these fraudsters and pay them a certain amount for opening each bank account. At many times it is found that the SIM (phone number) that is seeded to these bank accounts to perform OTP transactions doesn't belong to the genuine owner of the bank account and is mostly obtained fraudulently which is then used to commit fraud transactions and escape identity of the fraudsters. The bank associate also gets a high commission for this work.

Blackmailers

They are the master minds of the game. They identify potential targets. Send friend requests to them and try to get them into a conversation. Once believed in, they invite them over a WhatsApp Video call for nude sex chat and it is then that they record then sexual activity and the game of extortion begins. They blackmail the victim over phone calls and extort money by threatening to share their nude clips to the victim's near relatives and friends. Even after robbing them multiple times, they don't delete videos and the same video is shared with some other fraudster who further extorts presenting himself as some Law Enforcement Agency official or as a social media site (Example YouTube) Manager. It is a harrowing time for the victim where he is sometimes forced to commit suicide, as reported in several newspaper reports. The blackmailers make most money in this whole chain.

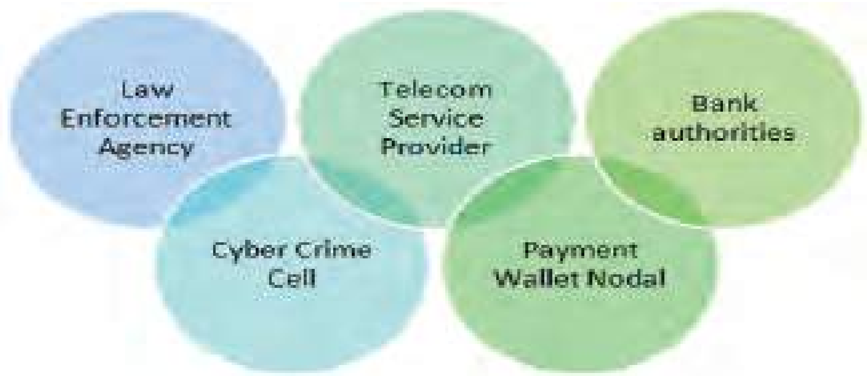
Transactors

The extorted amount using various UPI IDs (example Google Pay, Phone Pe) and transactions, is then transferred to some other wallet account and then to another account. This chain of transactions makes it difficult for the Law enforcement agencies to scrutinize fraudsters and delays their arrest while at the same time fraudsters get enough time to take out the extorted sum physically, leaving no trail and option for freezing the account by the banking or other financial authorities. The withdrawal is done by an ATM card belonging to a fraudulently opened bank account. Usually, it is seen that the withdrawals are done from a different city or far off located ATM from the blackmailer's place to escape any detention or arrest by the Police. The Transactor usually gets nearly 15-20% of the amount in the whole chain, as a commission.

Cyber Sextortion Investigation

A Police Perspective Investigation of cyber-crimes goes beyond the physical boundaries of territorial jurisdiction since the crime is committed in a cyber space where different entities of the crime are placed at different locations. It is for this very reason that the task of police investigation gets complicated and needs support of technical teams, well equipped cyber cell, trained policemen to solve the challenge faced. As seen from the above shared workflow and the stakeholders overview, there are multiple partakers in one incident of a cyber-crime. To ensure successful investigation it is a must that all the levels of this organized crime are sewed in properly along with technical evidences establishing them as part of the chain of crime. Police teams in close coordination with the nodal authorities of Telecom Services Providers (TSP) gain location coordinates and Call Data Records (CDR) of these fraudsters. Working on them the team identifies the other primary numbers being used by these fraudsters in their phones (unique IMEI slot), which help identify their particulars as per the Customer Application Form (CAF) details. The other thread is to learn about the timestamped ATM withdrawals done by them. By due coordination with the bank officials, the ATM locations (based on code mentioned in transactions) are identified and CCTV footages are looked in for accused identification. This further requires a study of the BTS Tower Dump data to identify potential fraudster's number who might have done some call before/after the transaction or otherwise might have been active during the transaction timestamp. The bank account details of the ATM card used in the transaction is also requested to the concerned bank to know the person in whose name the account has been opened. Once this piece of information is obtained, the field teams verify the particulars of that person and try to get information from that person who fooled them to open a bank account in their name and handover the ATM card to them.

This is a critical piece of information since it is this person who is in touch with the blackmailer and the transactor. On further collecting and connecting the available pieces of information, the field teams in close coordination with the cyber cell team identify these fraudsters and take them into custody.All of this is obtained only after a close and quick coordination between the police team, cyber cell team, nodal authorities of the Telecom service providers, payment wallets and the bank authorities.



Brainstorming the counter-response and some Suggestions

Security Analysts hold the view that the war at the nation frontiers in the decades to come is not going to see conventional wars diffusing bloodshed but it would be rather in the form of Cyber warfare. Similarly, the internal threat to the society from these criminals would emanate from Cyber-crime which like cyber warfare, would be a silent but impacting lives. To ensure an 'iron-fist' response to this challenge it is must that a coordinated effort is taken to establish a mechanism at individual, societal and institutional level.

Individual

✓ Do Not accept friend requests from unknown people.

✓ Do Not accept video calls from unknown numbers.

✓ Do Not exchange any private or personal information over social media platforms.

✓ In case one becomes a victim of sextortion the first thing should be to report the same to nearest police station or cyber-crime helpline (155 260).

✓ Do Not involve yourself into any conversation with the fraudster. Just block the number and avoid picking any unknown numbers. The intent is to intimidate the victim and extort money. Numerous interrogations/investigations of these accused reveal that they don't share/post anything if the victim doesn't respond them well since their main intent is just to extort money.

✓ Share information with your close friends/relatives and seek help from them in case you panic and register the complaint as soon as possible.

✓ An early reporting on cybercrime helpline is always helpful in blocking the bank accounts/transactions of these fraudsters and ensure recovery of the money.

✓ Don't fall prey to the perils of social media and click or surf the internet and unknown links and sites very very carefully.

✓ We need to follow cyber hygiene and generate awareness about cyber safety.

Societal

✓ Need to reject the acceptance of cyber criminals and their illegal earnings by the society. Since it doesn't have the colors of a conventional heinous offence its proceeds are not seen as illegitimate by the family and the society.

✓ Communities where such crime is prevalent must report such crimes to the LEAs and support them in their investigations.

✓ Motivate people to come forward and report if such a fraud has happened to them.

Institutional

✓ Capacity Building of Police personnel to be able to investigate these crimes in a more effective and professional manner.

✓ The resistance to register cybercrimes must be done away with and it can only happen if Police is given the requisite resources to effectively deal with investigation of cybercrimes.

✓ Banks must double check documents that are used to open fraudulent bank accounts and need to device a stricter policy for online safety.

✓ SIM vendors and the telecom

authorities should have a mechanism in place to identify fraud SIMs working in their circles.

✓ Police must work out a strategy to classify these crime hotspot villages (into red, orange, yellow list) and take help from TSPs to identify fraud numbers and work with bodies like Indian Cyber Crime Coordination Centre (I4C under MHA), National Payment Corporation of India (NPCI) to identify fraud numbers, wallets, bank accounts and block them on a massive scaleto break the spine of the cybercrime setup (as being done by Alwar Police).

✓ Since cybercrime doesn't respect territorial boundaries, it requires furthermore coordination and support to the police teams visiting from other states in catching their criminals.

Government

✓ Government through its regulatory bodies should do an effective check on E-mitra kiosks involved in such frauds.

✓ Data security is the next focal area for any state government to ensure personal identification data (like Aadhar, phone number, bank account number) belonging to an individual is not available for public access. Proper data masking must be done to deter data thefts.

✓ Special Cyber experts should be hired by the government for capacity enhancement of the cybercrime cell teams. This must go alongside the regular training of the existing police force to handle these crimes.

✓ Setup closely connected teams, which can be further empowered to work out a mechanism to crackdown on the criminal network.

✓ A timely response is must to check a crime which is a matter of seconds. Round-the clock support teams must be setup by the banks, telecom nodal, wallet companies, cyber-cell etc. This can be put in place through some legislation/executive order by the government.

Conclusion

Digital India envisions using digital platforms for quicker and more efficient form of transactions in all fields. While the concept is the need of the hour what we have not assessed is its side effect in the form of increasing cyber crimes. This paper focussed on one type of cyber crime namely catfishing or sextortion in Mewat Region. Every day the methodologies used by cyber fraudsters is changing and they are developing newer modus operandis to dupe or cheat victims. The trauma that a victim goes through is unexplainable as most victims are innocent and poor persons with little or no knowledge of using the technology. Its high time we developed stricter norms of cyber safety and rigorously followed the cyber awareness generation programs. Visiting some of the identified hotspots in Alwar district and speaking to the people of the village, there is one conclusion we can safely draw, the infamous tag of Mewat Region becoming the second "Jamtara" is something which everyone wants to fight against. Till now the youngsters in these villages and mostly illiterate and school drop outs considered this kind of cyber fraud as a fun activity. But generating awareness about the legal consequences of this crime, engaging Financial Agencies like Enforcement Directorate and Income Tax Department and registering FIRs and complaints against these fraudsters and ensuring convictions for them, has definitely acted as a deterrence in these areas. Alwar Police is initiating and putting continued efforts in this direction and we are sure that we will be able to end this menace soon with the support of all agencies.

References:

- http://www.cybercelldelhi.in/Sextortion.html
- https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail
- https://www.fbi.gov/video-repository/newss-what-is-sextortion/view
- Own experience and interrogation reports in various cyber crime investigations done by us.

*****

Rakshin, Volume VII - Year 2021

Online Gender Based Violence During Covid-19 Lockdown – A Longitudinal Study

Dr. Amrita Duhan IPS
S.P., Pratapgarh (Rajasthan)

ABSTRACT

Since its outbreak, the COVID-19 pandemic has only intensified Violence against Women and Girls, particularly in, but not limited to, the domestic sphere. The lockdown impact has been felt at online spaces too.

This study focuses on exploration of a relation between the COVID lockdown in the year 2020 and the crime against women especially at the online sphere.

Keywords gender-based violence, pandemic, cyber based sexual crimes, domestic violence, COVID 19

INTRODUCTION

"Never forget that it will be enough for a political, economic or religious crisis for the rights of women to be called into question" – Simone de Beauvoir.

Quarantine is necessary to reduce the community spread of the Coronavirus disease, but it also has serious psychological and socially disruptive consequences. This is known as the quarantine paradox. The Covid-19 pandemic has upended life for billions — but the strain and hardship is particularly acute for those who already face the greatest challenges. It's almost always the most vulnerable who suffer most in any crisis, and Covid-19 is no exception. As evidence of the human costs of the pandemic gathers, it's increasingly clear that women and girls are suffering from a surge of violence and domestic abuse. So many women are locked down at home in dangerous situations, just as there are fewer shelters and services available, and friends and support networks are harder to reach. And we're seeing that this gender-based violence is increasing online too.

However, there exists a clear gap of rigorous literature exploring the issue. Hence, the current paper attempts to understand online gender-based violence as an aspect of the COVID-19 lockdown. It reviews the pattern of rise in gender violence cases along with other reasons of violence against women.

METHODS

The present study is based on the calls received on Mahila Garima Helpline number 1090 from whole of state of Rajasthan before, during and after the lockdown period. Mahila Garima Helpline 1090 provides institutional support framework to the women living in difficult circumstances without any family, economic or social support to meet their basic needs of food, shelter and clothing as economic and social security. This helpline operates under Abhay Command and control centre, Jaipur Commissionerate and receives calls from all over Rajasthan. The calls are then filtered here area wise and concerned district's control room is contacted for further action. A follow up regarding action taken report is also recorded thereafter.

Hence, 1090 helpline shows a reflection of the violence against women especially during lockdown when women could not go to the Police Stations physically to report such cases from the whole state of Rajasthan.

ANALYSIS

The calls on 1090 helpline for the years 2019 and 2020 were analysed. A comparison of the number of calls and type of calls was done for both the years as a whole and then month wise comparison was done between the COVID lockdown months and COVID FREE months within the year as well as between the two years to analyse the effect of COVID lockdown on the number of calls received on 1090 related to violence against women especially online crimes.

Covid knocked the doors of India in February 2020. India was placed under a "total lockdown" from 24th march 2020 and the country began a phased lifting of restrictions on 8 June. This phased lifting of restrictions continued in a series of "unlocks" which extended into November 2020. Hence, two third of year 2020 was under various phases of lockdown and almost the whole year under the impact of COVID.

TABLE 1- COMPARISON OF TOTAL CALLS RECEIVED ON 1090 YEAR WISE

		YEAR			
	2016	2017	2018	2019	2020
Number of calls received on 1090	1940	1667	2299	2855	3521
Percentage increase (from last year)	base year	-16%	27%	19%	19%

The Table 1 shows the trend of total calls received on 1090 year wise from 2016 onwards to study whether the total calls increased in the lockdown year 2020. It is clear from the table that there is no significant increase in the calls in the year 2020, rather in comparison to year 2018 the percentage increase in calls year wise was less in 2020, whereas almost equal to 2019. This shows that probably COVID lockdown did not have impact on total calls received on Women's helpline in Rajasthan.

TABLE 2 - COMPARISON OF CALLS (BASED ON REASON) ON NUMBER 1090 (YEAR WISE)

S. No.	Reason based differentiation of calls	YEAR 2017	YEAR 2018	YEAR 2019	YEAR 2020
1	Indecent phone calls/ messages and verbal abuse	1381	1810	2364	2413
2	Threat (of life/acid attack/suicide/firing/rape/blackmail)	77	108	121	135
3	Molestation (stalking/through phone calls/comments)	22	70	37	54
4	Domestic violence by husband/ in laws	35	104	106	461

5	Cyber violence (indecent video calls/photo upload on Instagram, facebook/creation of fake IDs/indecent comments on social media/threat of making indecent video viral on social media)	114	163	162	334
6	Cases related to love marriage	0	2	2	3
7	Pressure for marriage	1	1	10	8
8	Seduction in lieu of marriage	5	5	15	18
9	Rape	2	0	0	3
10	Attempt to rape	0	3	1	8
11	Harassment at work place	3	1	3	6
12	Harassment by cab drivers	3	1	2	2
13	Sexual abuse by known	0	2	2	3
14	Pressure for child marriage	0	0	0	1
15	Pressure for making relationship	1	2	2	1

In Table 1, it can be seen that the numbers of calls are increasing year wise, but the percentage increase was almost the same in the year 2019 and COVID lockdown year 2020. Hence, Table 2 was formed in which categorisation of calls were done based on the major reasons to appreciate if the calls in a significant category increased or not during COVID or whether COVID lockdown had any effect on the crimes against women especially cyber related sexual crimes. On analysis of Table 2, the numbers seem to be raised in different categories especially in cases of Domestic violence and cyber related sexual crimes. To see if the increase in number in these two categories is relative increase because of overall increase of calls in 2020 or is an absolute increase when compared to the previous years, a comparative was done based on the percentage of total numbers which is shown in Table 3.

TABLE 3- COMPARISON OF CALLS (BASED ON REASON) ON NUMBER 1090 (PERCENTAGE OF TOTAL, YEAR WISE)

S. No	Reason based differentiation of calls	Percentage of Total (2017)	Percentage of Total (2018)	Percentage of Total (2019)	Percentage of Total (2020)
1	Indecent phone calls/ messages and verbal abuse	83%	79%	83%	69%
2	Threat (of life/acid attack/suicide/firing/rape/blackmail)	5%	5%	4%	4%
3	Molestation (stalking/through phone calls/comments)	1%	3%	1%	2%
4	Domestic violence by husband/ in laws	2%	5%	4%	13%
5	Cyber violence (indecent video calls/photo upload on Instagram, facebook/creation of fake IDs/indecent comments on social media/threat of making indecent video viral on social media)	7%	7%	6%	9%
6	Cases related to love marriage	0%	0%	0%	0%
7	Pressure for marriage	0%	0%	0%	0%
8	Seduction in lieu of marriage	0%	0%	1%	1%
9	Rape	0%	0%	0%	0%
10	Attempt to rape	0%	0%	0%	0%
11	Harassment at work place	0%	0%	0%	0%
12	Harassment by cab drivers	0%	0%	0%	0%
13	Sexual abuse by known	0%	0%	0%	0%
14	Pressure for child marriage	0%	0%	0%	0%
1	Pressure for making relationship	0%	0%	0%	0%

Table 3 shows percentage of different categories of the calls to total number of calls on women helpline. The previous 3 years showed almost the same percentage of stress calls in major categories or categories with larger numbers of calls such as of S.No. 1,2,3,4,5 &16 in Table 3. This percentage of calls is slightly skewed in the lockdown year 2020. There is significant decrease of calls in the category of Indecent calls/messages (from around 80% in the previous years to 69% in 2020). The decrease in the number of calls in the largest category is compensated by increase in the calls in other categories. The most significant increase in the calls is due to Domestic violence (13% instead of around 4% in the previous years). Then the next significant increase in the percentage of calls is due to cyber related sexual crimes such as indecent video calls/photo upload on Instagram, facebook/creation of fake IDs/indecent comments on social media/threat of making indecent video viral on social media (an increase of >2% when compared to the previous years).

TABLE 4
STUDY OF PERCENTAGE INCREASE IN CALLS IN DIFFERENT CATEGORIES IN THE YEAR 2019 AND 2020

S. No.	Reason based differentiation of calls	YEAR 2019	YEAR 2020	Percentage increase
1	Indecent phone calls/ messages and verbal abuse	2364	2413	2%
2	Threat (of life/acid attack/suicide/firing/rape/blackmail)	121	135	10%
3	Molestation (stalking/through phone calls/comments)	37	54	31%
4	Domestic violence by husband/ in laws	106	461	77%
5	Cyber violence (indecent video calls/photo upload on Instagram, facebook/creation of fake IDs/indecent comments on social media/threat of making indecent video viral on social media)	162	334	51%
6	Cases related to love marriage	2	3	33%
7	Pressure for marriage	10	8	-25%
8	Seduction in lieu of marriage	15	18	17%
9	Rape	0	3	100%
10	Attempt to rape	1	8	88%

11	Harassment at work place	3	6	50%
12	Harassment by cab drivers	2	2	0%
13	Sexual abuse by known	2	3	33%
14	Pressure for child marriage	0	1	100%
15	Pressure for making relationship	2	1	-100%
16	Others (cyber fraud/physical abuse by own family members/property disputes/second marriage etc)	28	71	61%
	Total	2855	3521	19%

On analysis of Table 4, the findings in Table 3 were reiterated that there is a definite large increase in the calls in the category of Attempt to rape (88%), Domestic violence (77%), Cyber related sexual crimes (51%) and Harrassment at workplace (50%). The actual number of calls is very less in Attempt to rape and Harrassment at work place. It seems strange to observe the increase in number of calls due to harassment at workplace especially when most of the year 2020 was devoted to Work from Home. The large increase in other categories is because of very small number of total calls of that category in a year, hence even a small increase brings about large difference in percentage increase eg. Rape (100%) and Pressure for child marriage (100%).

DISCUSSION

In this study, the focus was on the digital dimension of the crisis and warn that the growing trend of online violence and abuse against women has accelerated during Covid-19 and offer our few suggestions for tackling this violence.

Many forms of online abuse have skyrocketed during the Covid-19 crisis as life has shifted online and people spend more time on digital devices. For instance, there has been a surge in non-consensual sharing of images designed to threaten, shame and control women. Distribution or threats of sharing non-consensual intimate images also takes place largely within contexts of intimate partner violence. One UK helpline has seen a doubling of their website traffic since lockdown began, with 50% of cases linked to domestic violence.

According to a paper by Tim Berners-Lee, the web is too often not safe for women. 52% of young women and girls he surveyed said they'd experienced online abuse, including threatening messages, sexual harassment and the sharing of private images without consent. 87% said they think the problem is getting worse.

This abuse has devastating consequences for the mental wellbeing of victims as they are often left alone with their experience, an experience that is normalized and invisibilised on social media and in society in general, driving victims to silence and shame, exposing them to their perpetrators, and sometimes leading them to self-harm, depression and suicide.

Based on the above discussion, it can be maintained that there is a need for a holistic response model to deal with the issue of gender-based violence during current and possible future pandemics. Police, Health professionals, media, and community efforts must be combined to effectively deal with the issue of gender-based violence. Moreover, continuous and rigorous efforts are required to put an end to the stigma associated with gender-based violence. Rajasthan Police has been reaching out to society to create awareness and combat about Gender based violence by taking multiple initiatives eg Formations of all women Police patrolling squads such as Nirbhaya squad of Jaipur Commissionerate, Women Helpline 1090, Mahila desks at every Police station, Suraksha Sakhi Yojana etc. But still many voices go unheard, many calls still incomplete, many cases to be followed up. It is the prime duty of police to safeguard Women and children of the society moreover so in times of epidemic when they are most vulnerable.

CONCLUSION

The year 2020 as a result of lockdown due to COVID 19, saw increase in Gender based violence. The women were more vulnerable at home for Domestic violence and on online platform for cyber based sexual abuse.

The women should come out and seek help on the multiple platforms provided by the Government rather than succumb to the atrocities. They can get FIRs registered and seek justice.

On the other hand, awareness campaigns should be regular feature by the administration and government machinery regarding the types of abuse and remedial measures. Cyber awareness is a must to avoid occurrence of online sexual crimes. Health professionals, media, and community efforts must be combined to effectively with the prompt response to such complaints and a proper follow up of each and every case.

References

- Mittal S and Singh T (2020) Gender-Based Violence During COVID-19 Pandemic: A Mini-Review. Front. Glob. Womens Health 1:4. doi: 10.3389/fgwh.2020.00004.
- There's a pandemic of online violence against women and girls. Web Foundation · July 14, 2020 'Womens Rights Online. Submission to the UN Special Rapporteur on violence against women
- Fraser. Impact of COVID-19 Pandemic on Violence against Women and Girls. (2020). Available online at: https : //gbvguielines.org / wp/w-content / uploads / 2020/03/vawg-helpdesk-284-COVID-19-and-vawg.pdf.

*****

Vulnerability of Cyberspace

Ranjeeta Sharma, IPS
Astt. Superintendent of Police, Jodhpur

Year 2018 reported a large number of kids inflicting fatal injuries upon them, owing to their fascination with 'Blue Whale', an internet based game that would psychologically influence the players to undertake dangerous tasks. While it continues to be a mythological construct without any solid evidence, it is just one of the manifestations of the perils lurking in cyberspace, that our children are vulnerable to. Welcome to the digital age, the 5G world! Here we find ourselves thriving on the opportunities the Internet has to offer.

And with the entire world being practically shut down because of the Coronavirus pandemic since early 2020, most people ended up spending more of their lives online. We have gotten comfortable with working from home, shopping online and streaming on-demand content on OTTs platforms and learning through online courses.

Lurking danger

The Internet has truly transformed how young people learn, socialise and communicate today, but the urge to share intimate images, rising cases of cyber bullying and cyber scams, exposure to content that may promote self-harm, anorexia etc., make the youth more vulnerable and puts them at a greater risk.

The Youngistan of today uses smart phones for everything. Every day millions of Apps are downloaded, and sensitive personal information is shared with the authors. With online shopping platforms growing exponentially, there's a tendency to share financial information knowingly or unknowingly for making payments which increases vulnerability to online frauds.

In colleges, the internet is a sine-qua-non. Students rely heavily on it, for almost every activity. Every time they open a link, pop-ups and links to unsafe websites appear. Many times, these links have malwares hidden in them that either intend to damage their devices or pry on their personal information.

The Internet is abuzz with contests, discounts, goodies that trick young participants to share their personal details thus exposing them to risk of identity theft. These stolen identities fuel online scams.

This is just the tip of the iceberg. Apart from this, online grooming, cyberbullying, and online social abuse are rampant across the web.

Nearly everyone can afford a data service. But as technology becomes more accessible, the barriers are lowered for bad actors as well. Online safety has become a matter of great concern, across the globe, especially given the number of younger people who are now using the Internet.

This calls for a review of the legal remedies available to protect the child rights in the country. Constitution and it's interpretation in the Apex court judgements , statues and guidelines of the Union government have provided a framework for online safety of netizens, especially for children.

Legal Position

Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors is the landmark case where the apex court recognized the right to privacy under the ambit of articles14,19 and 21 of Indian constitution. Which means now the Constitutional courts could be moved under article 32 and 226 for protection of rights of the children.

In terms of statutes, the provisions are provided in general in IPC as section 354A and 354D provide punishment for cyber bullying and cyber stalking against women.

There are cyber police stations across the states, though complaint can be registered in any police station.

POCSO Act, 2012 is a dedicated law enacted to protect children from sexual harassment of any kind. Certain provisions have been included to cover cyber world. Section 13 to Section 15 deals with the issue of child pornography. Section 14 and Section 15 lay down the punishment for using child for pornographic purposes and storage of pornographic material involving child.

Further, the IT Act, 2000 has provisions to deal with cybercrime against children. Section 67B of the act provides stringent punishment for publishing, browsing or transmitting of material depicting children in sexually explicit act, etc.in electronic form. While these enactments prescribe certain offences, but these alone cannot suffice. Government has recognised multiple stakeholders when it comes to shielding children from perils of cyber world. Hence parallely, policies, guidelines and mechanisms have been developed to reinforce the legal framework. Other steps taken to combat cybercrimes against children include:

1. The information technology (intermediary guidelines and digital media ethics code) rules, 2021 notified under the IT act, specifies that the intermediaries shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that is inter-alia, obscene, pornographic, paedophilic, has minor in any way; violates any law for time being in force.

2. Instructions to concerned ISPs to work out a suitable arrangement for receiving internet watch foundation, UK list of CSAM that is child sexual abuse material websites/ webpages on a dynamic basis and block access to child pornography webpages /websites

3. Department of telecommuncation had requested all ISPs to make suitable arrangement to spread awareness among their subscribers about the use of parental control filters in the end use machines through messages, emails, invoices, SMS, website etc.

4. CBSE has issued guidelines to schools on the safe and secure use of internet, and it directs the schools to install effective firewalls, filtering and monitoring software mechanisms in all the computers and deploy effective security policies.

5. National cybercrime reporting portal, www.cybercrime.gov.in has been launched by the government of India to enable citizens to online reports complaints pertaining to all types of cybercrimes with special focus on cybercrimes against women and children. Complaints reported on this portal are attended by respective law in force meant authority is of the states a nationwide helpline number i.e 155260 is also functional.

The protective frame work is still evolving in India. There's been an overwhelming rise in crimes against children through internet. While the laws offer a punitive approach, envisioned to create deterrence, one can not underestimate the importance of preventive measures that can be taken at the local level – family, school and community.

How to prevent?

In the wake of this cobweb of challenges, it's imperative that leaders, mentors, educationists, parents and guardians join forces and work towards empowering youth to have safe browsing experiences.

First and foremost, we need to talk! The safety of our children is our responsibility and we need to talk to them about safe Internet use, online dangers and threats. Awareness is the key. Families and schools should together work on this front.

Then comes equipping the children the necessary skills and competencies. Simply, encouraging two factor authentication, logging off when done with the system use, not sharing passwords, OTPs etc are basic practices which we can inculcate amongst our young netizens.

We need to encourage children to check the reliability and credibility of online web-sites, a habit missing even in their older counterparts. Educate them to keep their social media accounts private. Urge them to avoid adding doubtful people to their friend list. These small steps can make a big difference.

It is necessary that children know the importance of privacy and that it is 'not okay' to share their pictures with strangers or be harassed, bullied or humiliated online.

The need of the hour is to imbibe safe and sound online habits in the youth and focus on their digital intelligence and socio-emotional skills.

We need to ensure that our children should continue to learn and explore the world safely with the Internet. IOT is no more just on whitepaper!Presence of Internet would be exponentially growing in our lives. All our devices and equipment will be network enabled, thus exposing our lives on scale like never before. This calls for all the stakeholders – government, community and corporates to join forces and deliver a safe and sound browsing experience to the Youngistan.

*****

Deepfakes And Detection Mechanisms During COVID 19

Dr. Ananth Prabhu G, Dr. Anush Bekal, Harisha K, Sahyadri College of Engineering & Management, Mangaluru, Karnataka

Since the invention of photography in the nineteenth century, visual media have been adored by the public, and unlike audio recordings, photos and videos have seen widespread use as evidence in court cases (Meskin and Cohen, 2008), and it is widely acknowledged that visual media are a particularly potent propaganda tool (Winkler and Dauber, 2014).As a result, the incentives to create forged visual documents have always been strong. The Soviet Union documented extensive use of manipulated images for political purposes as early as the 1920s (Dickerman, 2000; King, 2014).

Individual images can be easily manipulated using the retouching technique.The technique was already in widespread use in the 1920s, most notably in the Soviet Union (King, 2014).One prominent example is the removal of Alexander Malchenko from official photographs after his execution in 1930 (Dickerman, 2000; King, 2014). (Figure 1). While this example, as well as many others, and the possibility of manipulating photos in general, have been widely known for a long time, the effort involved in creating manipulated images has been relatively high until recently. Experts, on the other hand, were usually capable of detecting such manipulations. As a result, unlike audio recordings, photos have generally main-tained public trust. Even today, the term "photographic evidence" is somewhat commonly used, despite the fact that confidence appears to be declining (Meskin and Cohen, 2008).

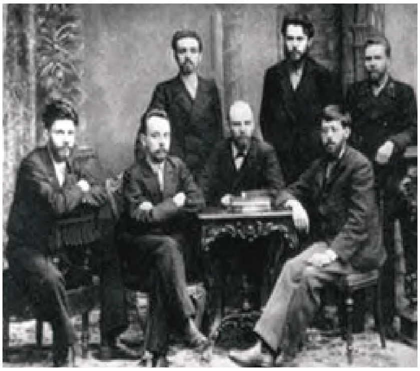


Figure 1

Image manipulation has been available to the general public since the 1990s. In fact, the term "to Photoshop," named after the Adobe Photoshop programme (Adobe, 2020), is now used as a verb to describe the act of manipulating images.Typically, this refers to minor manipulations, such as forcing a person to conform to a beauty ideal, but larger manipulations for commercial or entertainment purposes abound (Reddit, 2020).Naturally, these techniques can and have been used for propaganda purposes.The manipulation shown in Figure 1, i.e., the removal of a person from an individual image, now requires only a few minutes of work by a skilled user using image processing software.

The total number of images taken worldwide in the 1940s was comparatively low.As a result, the number of photographs that documented a single event was typically so small that a contrafactual narrative could be established by manipulating individual photographs.On the other hand, for political purposes, the manipulation of an individual's image carries little weight today.With the proliferation of digital photography and smartphones that are always with you, the number of pictures taken per year has exploded to an estimated 1.2 trillion in 2017. (Business Insider, 2017).Thus, when thousands of original images exist for major events, it is usually no longer possible to establish a narrative by censoring or manipulating individual images.This would necessitate the automatic manipulation of a large number of images. On the other hand, if a large number of images or videos of an event are available, it becomes possible to automatically create believable manipulations using artificial intelligence, assuming that the majority of the material can be accessed and changed.Simple versions of such systems have been used for some time to censor pornographic content on online platforms, for example (Gorwa et al., 2020).For privacy reasons, Google Street View detects and blurs faces and licence plates automatically. However, the same technology could be used for far more evil purposes, such as automatically removing or replacing people or events from all accessible video documents.

Video manipulation, on the other hand, necessitates the use of skilled professionals as well as a significant amount of time due to the need to change each frame individually.In the 1990s, Hollywood perfected video manipulation technology, but it was so expensive that only a few films took full advantage of it (Pierson, 1999).As a result, manipulating videos for political purposes was uncommon. However, a technique known as deepfake has recently become available, which allows for the manipulation of entire videos with little effort and consumer-grade computing hardware.It makes use of modern artificial intelligence to automate repetitive cognitive tasks like identifying a person's face in every frame of a video and swapping it for a different face, making the creation of such a manipulated video relatively cheap.

This article, which was compiled from various sources, is divided into four parts for easier comprehension a Understanding Deepfakes.

b) How are Deepfakes created

c) Detection Software

d) Proposed System

e) The roadmap ahead..

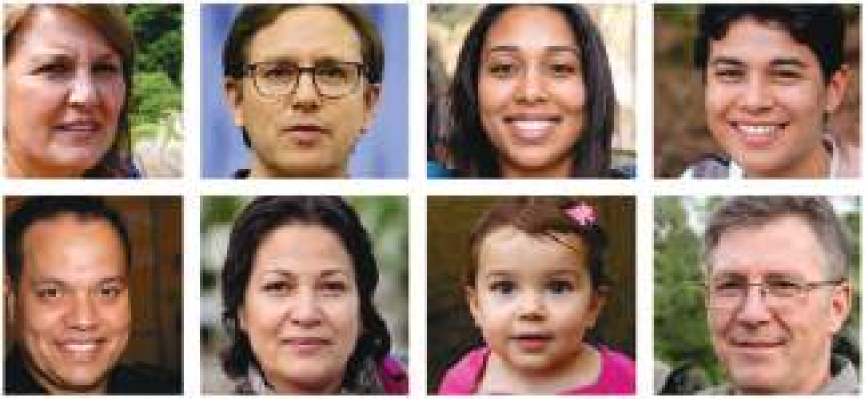


Figure 2: Courtesy: www.thispersondoesnotexist.com

The people in the photos above appear to be people you know.They aren't, however.All of these images are "deepfakes," which is the term for computer-generated, photorealistic media created using cutting-edge artificial intelligence technology.They're just one example of what this ever-changing method can accomplish.(You can create your own synthetic images at ThisPersonDoesNotExist.com.) Hobbyists, for example, have flooded YouTube with startlingly lifelike video spoofs using the same AI techniques.

Understanding Deepfakes

Deepfakes, a combination of the terms "deep learning" and "fake," first appeared on the Internet in late 2017, powered by generative adversarial networks (GANs), an innovative new deep learning method. Deepfakes, an anonymous Reddit user who started the movement in November 2017 by posting AI-generated videos with the faces of celebrities like Scarlett Johansson and Gal Gadot mapped onto the bodies of porn stars in action, gave the technology its name.The amount of deepfake content on the internet is rapidly increasing. According to a report from start-up Deeptrace, there were 7,964 deepfake videos online at the beginning of 2019; nine months later, that number had risen to 14,678. It has, without a doubt, continued to expand since then. Bill Hader morphing into Al Pacino on a late-night talk show, President Obama using an expletive to describe President Trump, and Mark Zuckerberg admitted that Facebook's true goal is to manipulate and exploit its users.

The term "deepfake" has a lot of connotations. Computer vision and graphics researchers, on the other hand, are united in their dislike of the term.It's become a catchall term for everything from cutting-edge AI-generated videos to any image that appears to be skewed.A lot of what's referred to as "deepfake" isn't. For instance, there's a contentious "crickets" rule. The former presidential candidate Michael Bloomberg's campaign released a video of the Democratic primary debate in the United States, which was edited using standard video editing techniques. Deepfakes were not used.

Scan the
QR Code to
watch the
Deepfake Video

A deepfake survey, published in May 2020, provides a timeline of how deepfake creation and detection have progressed in recent years.Researchers have been focusing on solving the following deepfake creation challenges, according to the survey:

Generalization High-quality deepfakes are often achieved by training on hours of footage of the target. The goal is to reduce the amount of training data needed to generate high-quality images while also allowing trained models to be applied to new identities (unseen during training).

Paired Training High-quality results can be obtained by training a supervised model, but this requires data pairing.This is the procedure for gathering examples of inputs and desired outputs for the model to learn from.When training on multiple identities and facial behaviours, data pairing is time-consuming and impractical.Self-supervised training (using frames from the same video), unpaired networks like Cycle-GAN, and network embedding manipulation are some of the solutions.

Identity leakage The identity of the driver (in a re-enactment, the actor controlling the face) is partially transferred to the generated face.Attention mechanisms, few-shot learning, disentanglement, boundary conversions, and skip connections are some of the solutions proposed.

Occlusions Artifacts can occur when a part of the face is obstructed by a hand, hair, glasses, or any other object.A closed mouth, which hides the inside of the mouth and the teeth, is a common occlusion.Image segmentation during training and in-painting are two examples of solutions.

Temporal coherence Because the network has no context for the preceding frames, artefacts such as flickering and jitter can occur in videos containing deepfakes.To help improve realism, some researchers provide this context or use novel temporal coherence losses.The amount of interference is decreasing as technology improves.

Deepfakes are expected to have a wide range of consequences in the media and society, including media production, media representations, media audiences, gender, law and regulation, and politics.

Figure 3. Courtesy: MIT Open Learning

How are Deepfakes created

Deep fakes are made possible by a branch of deep learning called generative adversarial networks, which is a type of deep learning (GANs).I an Good fellow invented GANs in 2014 while pursuing his PhD at the University of Montreal, one of the world's leading AI research institutes.

GANs were dubbed "the most interesting idea in machine learning in the last ten years" by AI guru Yann Le Cun in 2016.

Neural networks were good at classifying existing content (for example, understanding speech or recognising faces) but not at creating new content before the development of GANs.

GANs give neural networks the ability to create as well as perceive.

Good fellow's conceptual break through was to build GANs by pitting two separate neural networks against each other, as shown in Figure 4.

The generator starts with a given dataset (say, a collection of photos of human faces) and generates new images that are mathematically similar to the existing images in terms of pixels. Meanwhile, the discriminator is fed photos without knowing whether they came from the original dataset or from the generator's output; its job is to figure out which ones were created artificially.

The two networks hone each other's capabilities as they work against each other iteratively— the generator trying to fool the discriminator, the discriminator trying to figure out the generator's creations.The discriminator's classification success rate eventually drops to 50%, which is no better than guessing, implying that the synthetically generated photos are no longer distinguishable from the originals.

The machine learning community's open-source ethos is one reason deepfakes have spread: since Goodfellow's original paper, whenever a research advance in generative modelling is made, the technology is generally made available for free for anyone in the world to download and use.

Figure 4: Source: K SEELIGER ET AL/NEUROIMAGE 2018

To date, a whole subgenre of deepfake parody videos has emerged on video platforms like YouTube, with the most common manipulation being switching the main actors in a movie.For example, in a short film titled Home Stallone (Face, 2020)—a reference to the 1990 comedy film Home Alone—an AI-generated Sylvester Stallone, rather than the real actor Macaulay Culkin, plays the lead role.On the internet, there are a plethora of similar videos.

On April 14, 2020, the hashtag # TellTheTruthBelgium gained media attention.A video depicted Belgian Prime Minister Sophie Wilmès' nearly 5-minute speech, which depicted the COVID-19 pandemic as a result of environmental destruction. Extinction Rebellion, an environmental group, used deepfake technology to alter

Sophie Wilmès' previous address to the nation (Extinction Rebellion, 2020; Galindo, 2020).

Another example is an appeal to Mexican President Andrés Manuel López Obrador.In a video released on October 29, 2020, Mexican author and journalist Javier Valdez urges President López Obrador and his administration to fight corruption and organised crime more aggressively.As his digital alter ego explains at the start of the video, Javier Valdez was murdered on May 15, 2017.He was most likely assassinated as a result of his investigations into organised crime. The "Defending Voices Program for the Safety of Journalists" used deepfake technology to bring Mr. Valdez back to life for 1 minute and 39 seconds in order to demand justice for killed and missing journalists.The Defending Voices Program for Journalist Safety is a collaboration between Propuesta Cvica, a Mexican human rights NGO, and Reporter ohne Grenzen, a German journalist association (Reporter ohne Grenzen, 2020).

While many applications of deepfake technology are amusing or harmless, they do have the potential to be abused.Although the above examples are not malicious in nature, the case of Manoj Tiwari demonstrates that synthetic media can be used to deceive voters. The other two examples were released with a disclaimer that deepfake technology had been used.Deepfakes have long been suspected of being used to sway the 2020 presidential election in the United States.However, as of this writing, video manipulation has largely relied on traditional methods (Politifact, 2020; The Verge, 2020).Deepfake videos warning about threats to democracy have been released instead (Technology Review, 2020).So far, it appears that outright fabrications rarely make it to the public sphere, where they can be debunked, but such videos could be circulated in closed groups with the goal of mobilising supporters.Foreign politician videos appear to be particularly viable because it is more difficult for people to judge whether the depicted behaviour is believable for that person

(Schwartz, 2018).

Deepfakes aren't primarily targeting the political sphere at the moment.More than 85 percent of all deepfake videos target female celebrities in the sports, entertainment, and fashion industries, according to the Dutch startup Sensity. ai (Sensity, 2020), which tracks and counts deepfake videos available on the internet.Some of these are examples of so-called involuntary pornography, in which the target person's face is inserted into a pornographic source video.At first, this necessitated a large number of images of the target person, so only celebrities were chosen as targets.Recent deepfake technology based on generative adversarial networks, on the other hand, allows for the targeting of people for whom only a few images exist.

As a result of the widespread availability of this technology, the use of deepfakes for cyberbullying has emerged as a serious threat.In South Korea in 2019, an incident known as the Nth Room Scandal (International Business Times, 2020) occurred.Production and distribution of pornographic deepfake videos featuring the faces of female celebrities, as well as other exploitative practises, were part of the event.Similarly, DeepNude (Burgess, 2020), a Telegram extension, first appeared in 2019 and then reappeared in 2020.It essentially replaces the clothed body in a photo of the target person with a naked body, resulting in a likeness of a naked picture of the target person. The programme is basic, and it appears that it was designed specifically for white women.Its design, on the other hand, effectively eliminates all remaining barriers to the creation of potentially harmful content.Because it relies on external servers, it's possible that more advanced programmes could be developed in the future that delivers high quality images or videos.

The impersonation of other people in online communication is a different application of deepfake technology.Criminals impersonated a CEO on the phone in 2019 and ordered an employee to transfer a large sum of money to a private account using audio manipulation (Stupp, 2019).A software that uses deepfake technology to allow impersonation in video calls was recently released (Siarohin et al., 2019).Clearly, such technology has a wide range of criminal applications, the most concerning of which is the use of such technology by sexual predators to impersonate minors (Foster, 2019; Hook, 2019).

Detection Software

The Defense Advanced Research Projects Agency (DARPA) of the United States established the media forensics project in response to the threat posed by manipulated visual media (Darpa, 2020), with the goal of developing tools for recognising manipulation in videos and images using a variety of tools such as semantic analysis. In this context, Adobe, the maker of the popular Photoshop software, has released a programme that can detect the majority of image manipulations that Photoshop can perform (Adobe Communications Team, 2018).The technology is based on extensive research conducted at the University of Maryland (Zhou et al., 2018).Large data sets for training and testing detection algorithms have also recently become available (Dolhansky et al., 2019; Guan et al., 2019; Rossler et al., 2019).

In a competition organised by Facebook in 2020, many ideas for AI-based deepfake detectors were tested (Dolhansky et al., 2020; Ferrer et al., 2020).Several new detector approaches resulted from the challenge (Mishra, 2020).Verdoliva recently gave a presentation on the field of media forensics and fake news (Verdoliva, 2020).

While these approaches have potential, their success ultimately depends on how they are implemented.Furthermore, recent research (Gandhi and Jain, 2020; Neekhara et al., 2020) based on adversarial strategies (Goodfellow et al., 2014) suggests that even the best detectors can be deceived.The addition of noise to a video or image is an adversarial strategy.Although this noise is undetectable to the naked eye, it is enough to fool a fake news detector.

As a result, many of these systems are likely to be flawed in practise because they do not provide 100% detection accuracy, and if made public, misinformation creators will have access to them as well. Even if the detection accuracy is 99%, the system can be hampered in some way.It is well known that a large number of adversarial examples, or pairs of input images that will be recognised as the same object by humans but as very different objects by neural networks, exist for state-of-the-art image recognition (Szegedy et al., 2013; Gu and Rigazio, 2014). As a result, a manipulation detector based on the same technology would suffer from the same flaws, and could theoretically be defeated by making minor changes to the manipulated content.

The issue is similar to that of anti-virus software (Fedler et al., 2013; Rastogi et al., 2013).The use of detection software running on user systems has not solved the malware problem in the last three decades.Similarly, it is unlikely that the situation will change in the case of manipulated media."Currently it is trivial for malware authors to slightly alter existing malware, with the effect that it will not be detected by antivirus software until new signatures have been released." says the statement succinctly.(Fedler and colleagues, 2013).Malware and spam detection has seen some success thanks to centralized instances that can't be accessed and tested indefinitely by malware creators. For example, software on smartphones is typically only available through controlled channels (Apple App Store, Google Play), and the methods for getting around this restriction are typically limited to technically savvy users. Malware that has been confirmed is regularly removed from these channels.This strategy has proven to be effective in the past.One possible explanation is that smartphone operating system providers have a strong incentive to keep malware out of their systems and thus provide value to their customers.

However, a centralised system controlled by a single company is clearly not a desirable solution for news distribution.A diverse selection of independent news sources is the hallmark of a healthy media landscape in a democratic society.Thus, even in the benign form of manipulation detection, central control over what is "truth" carries a significant risk of abuse. Further more, such an instance would almost certainly be subject to political pressure, similar to how social media platforms like Facebook and Twitter are frequently pressured by private or state actors to remove certain types of content from their platforms.As a result, an open, decentralised, and open-to-all solution would be preferable.The technical challenge is to create a solution that is both efficient and effective.

Other technological approaches, such as the New York Times' News Provenance Project (Koren, 2019), which uses blockchains to ensure that a video has not been tampered with, are available in addition to detection software (Hasan and Salah, 2019b).They are not affected by the accuracy issues discussed above because they are based on cryptography rather than artificial intelligence.They would, however, require widespread adoption to be effective.

The Proposed System

Title: Design and development of model for Deepfake video detection by eye blinking rate detection using CNN & RNN

Summary

The development of camera technology, the widespread availability of cell phones, and the popularity of social networks (Facebook, Twitter, WhatsApp, InstaGram, and SnapChat) and video sharing portals (YouTube and Vemeo) have made the production, editing, and dissemination of digital videos easier than ever before. Detailed 3D computer graphics models were used to create realistic images and videos. Recently, new deep learning algorithms, especially those based on generative adversary networks, have been developed (GANs). In this work, we describe a new method to expose fake face videos generated with neural networks. Our method is based on detection of eye blinking in the videos, which is a physiological signal that is not well presented in the synthesized fake videos. Faces are first detected in each frame of the video by our system. Based on the identification of facial landmark points, the identified faces are then aligned into the same coordinate system to discount head shifts and changes in orientation. To form a stable series, regions corresponding to each eye are extracted.

Origin of the proposal:

The pattern of human eye blinking has been shown to vary greatly depending on a person's general physical state, cognitive activities, biological influences, and level of information processing. The pattern may be influenced by a person's gender or age, the time of day, or the person's emotional state or level of alertness, for example. Therefore, integrity can be used to identify Deepfakes. Deepfakes can be identified by using a heuristic approach based on the findings of medicine, biology, and brain engineering science, as well as machine learning and various algorithms based on engineering and statistical knowledge, to monitor significant changes in the eye blinking patterns in deepfakes. As a result, we can use track to conduct integrity checks. This ensures that we can verify the integrity of a video by monitoring major shifts in a subject's eye blinking pattern.

The problem definition: Enhancing the detection rate of deep learning model using Convolutional Neural Network and Recurrent Neural Network by the eye blinking rate prediction for deepfake videos.

International status

Facebook, Microsoft and industry body Partnership for AI have joined forces with universities and research institutions to come up with the Deepfake Detection Challenge. This competition, which will run through to March 2020.

Methodology

1. Pre-Processing
2. Feature extraction
3. Designing CNN model
4. Classifier
5. Testing
6. Deployment of model2

Figure 5: The Deployment Model

Organization of work elements: The following points indicate the workflow of the project

a. Collection of suitable datasets

b. Pre-processing on the dataset

c. Feature extraction- eyeblink will be extracted from the frames of a video

d. Model design- development of classifier

e. Training the model

f. Testing the model against the sample deepfake videos

g. Evaluation of model performance

h. Deployment of the model

Figure 6: Architecture of the Proposed System

Input: The system was verified for detecting fake videos during Covid 19 Pandemic. During the Covid-19 pandemic government and other agencies have put all the efforts to spread awareness about it. Various infrastructure and technological development were required for sample collection, testing, treatment, and vaccination. To spread the awareness about Covid-19, videos were made by celebrities, politicians, doctors, and scientists on different social media platforms which played a major role in reducing the stress level of individuals. In such situation, cyber security becomes extremely important so that the actual videos cannot be altered or if altered it must be identified. If these videos are created with the morphing of celebrity faces and negative information with fake news is put in such videos, then this may lead to major disaster and panic among the people. These types of videos are called deepfake videos. To find the deepfake videos, we propose a system, a new architecture. If deepfake video is generated through a Generative Adversarial Network (GAN) model, it can be detected based on an eye blinking pattern.

Many technological upgradations took place in the field of Artificial Intelligence and Deep learning in recent years. Today using Artificial Intelligence technique any images or videos can be manipulated in such a way that altered video is indistinguishable from original videos. Word deepfake has been originated from deep learning and fake Today many people use the social media to reach out large crowd and if any fake content released on social media reaches large number of people it creates problem with mental health hence deep fake on social media has become serious issue. Nowadays deepfakes are generated through Generative adversarial network [GAN] Model. When there is situation of covid-19 pandemic and lockdown is imposed, public who are residing inside their home are more reliable on social media. Fake news with the help of deepfake videos gives more mileage to reach large number of people and it creates panic among the crowd. There are some models that have been developed but video created using GAN which bypass the detector and it becomes unidentified.

Outcome:

Figure 6: Graphical Representation of the Outcome

Output Screen

The roadmap ahead

Looking beyond purely technological remedies, what legislative, political, and social steps can we fancy defend against deepfakes' dangers?

The contest between the making and detection of deepfakes won't finish within the foreseeable future. We will see deepfakes that are easier to form , more realistic and harder to differentiate . The current bottleneck on the shortage of details within the synthesis is going to be overcome by combining with the GAN models. With advances in hardware and lighter-weight neural network structures, training and generating time will be reduced. We've seen new algorithms emerge in the last few months that are ready to deliver a much higher level of realism or run in near real-time. Deepfake videos are evolving to include whole-head synthesis (head puppetry), joint audio-visual synthesis (talking heads), and even whole-body synthesis, in addition to simple face-swapping.

Furthermore, the first deepfakes are only meant to fool human eyes, but lately, there are measures to form them also unnoticeable to detection algorithms as well. Counter-forensics exploits the vulnerability of deep neural networks by introducing targeted invisible "noise" to the generated deepfake video in order to deceive the neural network-based detector.

To restrain the threat posed by increasingly sophisticated deepfakes, detection technology will also have to be coerced to maintain the pace. As we work to improve overall detection performance, we should also focus on making detection methods more robust against video compression, social media laundering, and other common post-processing operations, as well as intentional counter-forensics operations. However, given the speed and reach of online media, even the most effective detection method will largely be post-mortem, applicable only after deepfake videos have been discovered. Therefore, we'll also see developments of more proactive approaches to guard individuals against becoming the victims of such attacks. This can be accomplished by "poisoning" potential training data in order to sabotage deepfake synthesis model training. Technologies that use invisible digital water marking or control capture to authenticate original videos will be actively developed to improve detection and protection methods.

Deepfakes aren't just a technical issue, and because Pandora's box has been opened, they're not going away anytime soon. However, as our ability to detect them improves, and as a result, public awareness of the issue grows, we will learn to coexist with them and limit their negative effects in the future.

We are at a crossroads right now. Deepfakes have the potential to grow from an online oddity to a widespread political and social force in the months and years ahead. To prepare for the future, society must act now.

Acknowledgement Special thanks to VGST, Department of IT, BT & ST, Govt of Karnataka for the financial support to procure laboratory equipment to carry out this research.

References

- Adobe (2020). Photoshop. Available at: https://www.adobe.com/products/photoshop.html (Accessed April 1, 2020).

- Adobe Communications Team (2018). Spotting image manipulation with AI. Available at: https://theblog.adobe.com/spotting-image-manipulation-ai/ (Accessed April 1, 2020).

- Al-Sharieh, S., and Bonnici, J. M. (2019). "STOP, you're on camera: the evidentiary admissibility and probative value of digital records in europe," in Synergy of community policing and technology. Editors G. Leventakis, and M. R. Haberfeld (Cham, Switzerland: Springer), 41–52.

- Ayyub, R. (2018). I was the victim of A deepfake porn plot intended to silence me. Available at: https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316 (Accessed April 1, 2020).

- Beridze, I., and Butcher, J. (2019). When seeing is no longer believing. Nat. Mach Intell. 1 (8), 332–334. doi:10.1038/s42256-019-0085-5

- Bradford, H. (2017). Abercrombie and fitch's reputation takes A hit after CEO's 'fat' comments resurface. Available at: https://www.huffpost.com/entry/abercrombie-reputation-ceo-comments_n_3288836 (Accessed April 1, 2020).

- Brown, N. I. (2020). Deepfakes and the weaponization of disinformation. Va. JL Tech. 23, 1.

- Burgess, M. (2020). A deepfake porn bot is being used to abuse thousands of women. Available at: https://www.wired.co.uk/article/telegram-deepfakes-deepnude-ai (Accessed April 1, 2020).

- Business Insider (2017). People will take 1.2 trillion digital photos this year—thanks to smartphones. Available at: https://www.businessinsider.com/12-trillion-photos-to-be-taken-in-2017-thanks-to-smartphones-chart-2017-8?r=US&IR=T (Accessed April 1, 2020).

- Cameroon, B. H. (2020). The bellingcat podcast season 2-the executions. Available at: https://www.bellingcat.com/resources/podcasts/2020/07/21/the-bellingcat-podcast-season-2-the-executions/ (Accessed April 1, 2020).

- Chesney, B., and Citron, D. (2019a). Deep fakes: a looming challenge for privacy, democracy, and national security. Calif. L. Rev. 107, 1753. doi:10.2139/ssrn.3213954

- Chesney, R., and Citron, D. (2019b). Deepfakes and the new disinformation war. Available at: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war (Accessed April 1, 2020).

- Darpa (2020). Media forensics (MediFor). Available at: https://www.darpa.mil/program/media-forensics (Accessed April 1, 2020).

- Dickerman, L. (2000). Camera obscura: socialist realism in the shadow of photography. October 93, 139–153. doi:10.2307/779160

- Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., et al. (2020). The deepfake detection challenge dataset. Preprint repository name [Preprint]. Available at: arXiv:2006.07397.
- Dolhansky, B., Howes, R., Pflaum, B., Baram, N., and Ferrer, C. C. (2019). The deepfake detection challenge (dfdc) preview dataset. Preprint repository name [Preprint]. Available at: arXiv:1910.08854.
- Donovan, J., and Paris, B. (2019). Beware the cheapfakes. Available at: https://slate.com/technology/2019/06/drunk-pelosi-deepfakes-cheapfakes-artificial-intelligence-disinformation.html (Accessed April 1, 2020).
- EU vs DisInfo (2020). Disinformation can kill. Available at: https://euvsdisinfo.eu/disinformation-can-kill/ (Accessed April 1, 2020).
- European Science Media Hub (2019). Deepfakes, shallowfakes and speech synthesis: tackling audiovisual manipulation. Available at: https://sciencemediahub.eu/2019/12/04/deepfakes-shallowfakes-and-speech-synthesis-tackling-audiovisual-manipulation/ (Accessed April 1, 2020)
- Extinction Rebellion (2020). The prime minister's speech by our rebels. Available at: https://www.extinctionrebellion.be/en/tell-the-truth/the-prime-ministers-speech-by-the-rebels (Accessed April 1, 2020).
- Face, C. S. (2020). Home Stallone [DeepFake]. Available at: https://www.youtube.com/watch?v=2svOtXaD3gg (Accessed April 1, 2020).
- Fedler, R., Schütte, J., and Kulicke, M. (2013). On the effectiveness of malware protection on android. Fraunhofer AISEC 45.
- Ferrer, C. C., Dolhansky, B., Pflaum, B., Bitton, J., Pan, J., and Lu, J. (2020). Deepfake detection challenge results: an open initiative to advance AI. Available at: https://ai.facebook.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/ (Accessed April 1, 2020).
- Foster, A. (2019). How disturbing AI technology could be used to scam online daters. Available at: https://www.news.com.au/technology/online/security/how-disturbing-ai-technology-could-be-used-to-scam-online-daters/news-story/1be46dc7081613849d67b82566f8b421 (Accessed April 1, 2020).
- Galindo, G. (2020). XR Belgium posts deepfake of Belgian premier linking Covid-19 with climate crisis. Available at: https://www.brusselstimes.com/news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/(Accessed April 1, 2020).
- Gandhi, A., and Jain, S. (2020). Adversarial perturbations fool deepfake detectors. Preprint repository name [Preprint]. Available at: arXiv:2003.10596. doi:10.1109/ijcnn48605.2020.9207034
- Goodfellow, I. J., Shlens, J., and Szegedy, C. (2014). Explaining and harnessing adversarial examples. Preprint repository name [Preprint]. Available at: arXiv:1412.6572.

*****

Rakshin, Volume VII - Year 2021

Tools for Law Enforcement for Monitoring Tor Traffic

Dr. Emmanuel S. Pilli and Pulkit Chandel
Department of Computer Science & Engineering
Malviya National Institute of Technology, Jaipur

Abstract:

Search engines such as Google, Yahoo, and Bing cannot index deep web content. Anyone with The Onion Router (TOR) browser can access the darkweb. TOR is important for anonymity and privacy of the user but it's been misused by explicit users to perform illegal activities on web. Tor forensics is an important aspect now-a-days due to huge popularity of Tor and its misusage. Law Enforcement Agencies(LEA) should be able to investigate Tor to find out such illegal users. The Tor monitoring tools would help LEA in Tor forensics effectively.

I. Introduction

Anonymity and privacy are two key components in ensuring freedom of expression on the internet. The goal of anonymity is to protect all information that can disclose a user's true identity, such as location and IP address. The purpose of privacy is to ensure that no organization or institution collects or stores any personal or private information about users without their permission, such as browser history, location information and so on. The Tor project was started by the US Naval Research Laboratories in 1995. The major purpose of their research was to decouple identification information from routing and create an anonymous military communication network.

This paper presents us with the tools that can be used by LEA for analyzing the traffic over Tor to find out if any illegal activities are taking place secretively over the web which can't be seen by normal browser and tools.

In section II, we introduce the TOR. In section III, we have examined the Tor monitoring tools which can be used to gather important information about the TOR relay. In section IV, the overview of Tor forensics, on how the information is used is given. In section V we have described how LEA could use Tor forensics to uncover the evidence and in Section VI we conclude the paper and suggest future directions.

II. TOR (The Onion Routing)

Tor is a global overlay network of relays that aids in the accomplishment of user Internet traffic privacy and anonymity. The Tor network creates a virtual circuit for each transmission that consists of at least three subsequent, randomly selected relays.

The Tor client at the source system downloads information about the relays from a directory server. Diffie-Hellman key exchange protocol is used to exchange keys with the designated relays. The data packets are encrypted several times at the source node, one for the message with its unique decryption key. The exit node decrypts the innermost layer of encryption and unencrypted data packet is sent to its final destination. As a result, the privacy of consumers data is maintained until the very last hop. Data between the last hop and the destination is likewise encrypted when using https through Tor.

The Tor browser secures users communications by routing them through a dispersed network of relays run by volunteers all over the world. It protects others from learning about websites visited as well as actual locations, and it allows access to websites that would otherwise be restricted on other networks.

III. Tor Investigation Tools

The Tor browser leaves numerous artefacts on the user's computer, particularly in system memory and also while running. All conceivable artefacts from the host system can be recovered. To discover crimes committed as a result of Tor anonymity, investigators determine whether individuals used Tor and then decide what to do next.

A) Earlier Tools

Memory artefacts: In these techniques the memory dump of the computer on which either Tor browser was installed or used are analyzed using the Volatility framework.

Hard disk artefacts: Hard disk analysis is carried out to support the results and artefacts produced by RAM memory artefacts. In this we search for Onion sites in FTK imager in the hard disk content.

B) NYX:- Nyx is a Tor command-line monitor. This gives you detailed real-time information about your relay, including bandwidth utilization, connections, logs, and more. Nyx is particularly well suited for ssh connections, terminals, and command-line experts. It uses STEM API as its core process. Stem is a Python controller library for Tor. With it you can use Tor's control protocol to script against the Tor process. Its makes it easy to write Tor analysis tools.

C) Track Tor :- Track Tor is a platform-independent tool that collects statistical and analytical data from tor services used by the end user. Detailed Bandwidth, Connections, and Resource's utilization information, as well as Event Logs details, are just a few of TrackTor's standout features. It is a more advanced and versatile Graphical User Interface (GUI)-based solution, giving it an advantage over current monitoring systems. Some of its utilities are Realy info., Node info., Bandwidth graph, Resource graph, New identity creation, Edit and Configure Torrc, etc.

IV. TOR Forensics

Tor is a well-known anonymous communication system with a minimal latency. However, it is currently being misused in a variety of ways. Some researchers used forensic analysis to find evidence. They wanted to see if there had been any modifications as a result of the Tor Browser's presence. Using searches, temporary data, logs, and the Windows registry, they were able to determine the existence of Tor Browser on the laptop after it was deleted. Some of the forensics ways are:-

RAM Forensics:-It is considered as volatile memory forensics. Many tools like Belkasoft RAM capturer will be used to capture dump of RAM and Hex dump will be used to view hexadecimal view of RAM dump.

Registry Changes: - Registry forensics can be carried out by tools like Regshot and can extract information like evidence of Tor installation and date of last accessed. Network forensics: -Network Forensics is carried out using tools like Wire shark and network miner and the information extracted from them are related to web traffic.

Bitcoin Forensics:- Extracting forensic artefacts from the installed Bitcoin wallet programme on the user's machine can be used to do Bitcoin transaction forensics.

V. Forensics For LEA

On Internet there is an abundance of information on nearly every imaginable topic. The partially decentralised anonymous network Tor is widely used for illegal purposes, including but not limited to dark net markets where anonymous users can buy and sell illicit products such as narcotics, stolen credit card information, firearms, and other items. The Tor hidden services make it possible to operate marketplaces without revealing the web server's IP address, making them difficult for law authorities to shut down.

This creates a lot of work to be done by the LEA in order to identify the illegal activities conducted on the darknet due to its secret nature and security aspects. Tor monitoring tools such as NYX could help in monitoring statistical data through command line of Tor usage on the computer.Through TrackTor a detail GUI enabled overview of the Tor traffic can be viewed and certain functionality of it provide LEA with more control over monitoring traffic and analysing it. They could also be able to find certain Tor artefacts on the physical device using tools for RAM artefacts, Network artefacts, etc.The artefacts data then can be used against the criminal in the court of law to tie the crime to them.

VI. Conclusion

There is little research in this field based on the Tor forensics background.The main threats to freedom of expression are censorship and surveillance. To overcome these obstacles, more and more websites are migrating to the onion domain, and it is projected that Tor browser will be among the top 5 browsers in cyber market in near future. So, advancements and more research are required in this field to overcome the crime and misuse of Tor in near future.

An all-in-one tool need to be created for the future work so that monitoring of Tor traffic for illegal activities could be done effectively on the go.

Acknowledgement

Harsh Gandhi, Parul Agarwal, Ritu Karela Divya Gupta and Narendra Singh Yadav

References

- A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal, Y. A. Bangash, “Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web” in Forensic Science International, 2019, Vol. 299, pp. 59-73.
- M. Alfosail and P. Norris,“Tor forensics: Proposed workflow for client memory artefacts” in Computers & Security, 2021, Vol. 106.
- Huang, Ming-Jung Chiu, Yu-Lun Wan, Chang-Po Chiang and Shiuh-JengWang,“Tor Browser Forensics in Exploring Invisible Evidence” in 2018 IEEE International Conference on Systems, Man and Cybernetic, 2018, pp. 3909-3914

*****

Book Review: Essentials of Online payment Security and Fraud Prevention : By David Montague, Published by John Wiley & Sons

Digant Anand, IPS
DCP (West), Jodhpur Commissionarate

Amid slowing economic activity, COVID-19 has led to a surge in e-commerce and accelerated digital transformation. As Lockdowns became the new normal, businesses and consumers increasingly went digital, providing and purchasing more goods and services online, raising e-commerce's share of global retail trade from 14% in 2019 to about 17% in 2020. This trend towards e-commerce uptake seen in 2020 is likely to be sustained. With the surge in e-commerce transactions came along the threats and vulnerabilities of the e-commerce space. The book ”Essentials of Online payment Security and Fraud Prevention”, 2011 by David Montague, published by John Wiley & Sons is a one of its kind book to focus exclusively on electronic commerce (e-commerce) fraud prevention. This book focuses on the prevention of fraud for the card-not-present transactions which is most commonly used in India for e-commerce transactions. This book is written to provide the essential information companies need to find, assess, and select the right fraud management options they will need for their e-commerce channels, however it's also a useful read for the law enforcement practitioners engaged in detection and prevention of online frauds as well as regulators responsible for designing systems and work flows for such fraud preventions. This book provides the basic concepts around payment flow and management as well as the ways fraud is perpetrated however it does not go into any detailed strategy design. The book focuses on the prevention of fraud for the CNP (Card not present) transaction. The payment process, fraud schemes, and fraud techniques all focus on these types of transactions. CNP includes all transactions in which the goods and services are sold to a consumer and the physical card is not given to the merchant.

The book is written with the perspective of a fraud practitioner in mind. A fraud practitioner is a person who is actively engaged in defining, managing, and monitoring fraud-prevention practices for a business. In short, the book is meant for individuals who have a responsibility to stop fraud. The book is unique in its sense that it caters to the readers who are new to e-commerce payments and frauds. Such readers can start reading the book from the beginning and work their way through it since each chapter builds on what we have learned before. For the more advanced fraud practitioner, this book may be used as a reference tool to look up certain techniques or schemes.

The first Chapter "Understanding Online Payment Options"and the following three chapters are a primer which helps reader to understand various types of consumer-not-present (CNP) payments and fraud, and the mechanics behind it. It is very well written and clarifies all the terms and jargons used further in the book. Next eight chapters are aimed at developing an understanding of the use and best practices for the 8 categories of fraud prevention tools along with the top 45 ecommerce fraud prevention techniques. The techniques which are discussed in the book include:

- Identity Proofing
- Guaranteed Payments
- Fraud Scoring
- Operational Management (Enterprise)
- Analytics
- Data Quality
- Technology
- Data Sharing

Every chapter deals with a particular technique in detail and lists all tools required for the technique implementation. The chapters are very well organised in the sense that they deal with all aspects of the given fraud prevention technique viz:

- Efficacy
- Estimated costs of implementation
- Detailed working mechanism
- Interpretation of results
- How to build the technique

in-house

On the critical side, the book deals with limited techniques of fraud prevention that too on a very high level without actually discussing the actual implementation and use cases describing situations where even these controls have been surpassed by the fraudster. Moreover, since e-commerce and payments systems are a part of a fast-paced industry the book seems a few years out of date as it fails to cover the new and prevalent payment systems and frauds in the CNP transactions domain. Some chapters have limited relevance in the Indian context due to varied credit card and banking norms extant in the country. However overall, as the name suggests the book is an essential guide for learning and reference for any practitioner engaged in the prevention of fraud for the card-not-present transactions.

*****

Guidelines for Authors/Contributors

1. Papers/articles are welcome for publication on the understanding that these contain original unpublished work not submitted for publication anywhere else. A certificate to this effect should invariably accompany the article.

2. Papers presented/submitted in a conference/seminar must be clearly indicated at the bottom of the first page and the author should specify with whom the copyright rests.

3. Articles must be not more than 4,000 words including notes references and tables.

4. All papers must be submitted in hard and soft copy format. The soft copy can be sent by e-mail; alternatively it can be sent by post on a CD. Both the hard and soft copies are essential for processing.

5. Papers should be accompanied by an abstract not more than 300 words.

6. Contributors are requested to provide 10-15 keywords for their contribution.

7. Authors are requested to provide full details for correspondence postal and e-mail addresses and daytime phone numbers.

8. The article should be proof-read and free of corrections. A submission to Academy journal 'Rakshin' regarded as a commitment to publish. Submission to other journals under review is not acceptable.

9. References should be cited in the text by using the last name(s) of author(s) and year of publication, using page numbers only in the case of a quote. Multiple citations should be alphabetized.

10. Examples of bibliographical references

    (a) Raj. S, 1989 "The Effects of Crime Rates. The SVP, NPA Journal, Volume XV, Jan-June, P.

    (b) Pinker, S.2007. Introduction in J. Brocknan (Ed.), what is your dangerous idea? New York: Harper Collins.

    (c) Pinker, S., & Rose, S.1998. The two Steves: A debate. Edge.

    http://www.edge.org/3rd_culture/pinker_rose/pinker_rose_pl.html.

11. The copyright for articles published is transferred to Rajasthan Police Academy.

12. Kindly send your comments and contribution to our Email Id - **rakshin.rpa@gmail.com**

**If You want peace,
work for justice**

- Pope John Paul VIth

न्याय शांति का
प्रथम न्यास है।

–राष्ट्रकवि 'दिनकर'

Rajasthan Police Academy
Nehru Nagar, Jaipur (Rajasthan) INDIA
Phone : 0141-2302131, 2303222, Fax : 0141-2301878
E-mail : rakshin.rpa@gmail.com • Web. : www.rpa.rajasthan.gov.in