Addressing Corruption through Information and Organized Networking (Action): A Survey Inclusion of Cyber Crime & Prevention

Mandeep Kaur

Research Scholar
Institute of Law, Jiwaji University, Gwalior

***Abstract*: The approach to study on Corruption through Information and Organized Networking through building our knowledge of the access-to-information environment and of essential stakeholders within India. This organized structure engage with key actors to address challenges in accessing information and in the broader fight against corruption. Information contained in National Integrity System studies and new research into access to information in India to provide the background for this approach our analysis identified gaps in implementation of the right to access information and informs our engagement and advocacy strategies. This paper propose an Organized Information Networking who develop skills, build networks and make connections between diverse groups, exploring new ways of connecting greater numbers of people in anti-corruption work. This has included a number of regional and national workshops, events and trainings with a broad array of groups and individuals. With the help of organized Information network the level of corruption must be significantly reduced.**

***Keywords*: Corruption through Information, Organized Networking of Corruption, Anti-Corruption Work**

1. Introduction

Corruption undermines sustainable economic, political and social development, for developing, emerging and developed economies alike. Corruption endangers private sector productivity by setting incentives to allocate resources to unproductive activities and by deterring innovation and the emergence of new companies. Corruption hinders public sector productivity by biasing decisions in public expenditures, by impairing the skills and professionalism of the civil service and by reducing public resources available to support productivity in the economy. And corruption is a threat to inclusive growth by undermining the opportunities to participate equally in social, economic and political life and impacting the distribution of income and well-being. Corruption also erodes trust in government and public institutions, rendering reform more difficult.

1.1 Fight against corruption

The purpose of this event was to raise awareness, among both participants and society in general, regarding the importance of fighting corruption, through coordinated public policies, at both the national and international level. The objective is to strengthen public confidence and integrity in public life by using transparency as a tool.

1.2 New Technologies to Increase Scrutiny

Evidence suggests that new, inexpensive ways of verifying identities and executing payments using digital technology can reduce the impact of corruption on public service delivery to the poorest. In India, for example, some of its large social welfare programmes suffered from ineligible beneficiaries receiving payments and officials taking a cut of, or delaying, payments meant for the poor. To combat these problems, the government distributed smartcards based on the country's biometric identification system to 19 million needy villagers in connection with the $5.5 billion National Rural Employment Guarantee Scheme. This substantially reduced the role of officials in the payment process, lessening the opportunities for misconduct. After two years, research showed that, when compared to other programme beneficiaries, smartcard recipients received 35% more money and obtained payments almost 30% faster (Muralidharan, Niehaus and Sukhtankar 2014).

2. Cyber Crime: A Technological Corruption

As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crimes involving computers. Cybercrime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cybercrimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc. In tenth United Nations congress on "prevention of crime and treatment of offenders" which is devoted to issues of crimes related to computer networks, cybercrime was broken into two categories and defined as:

A. Cyber Crime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

B. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a

Computer system or network.

2.1 Cyber Crime Includes
Following are the few examples of cybercrime:

Cyber stalking: Online harassment and online abuse all comes under stalking. It generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Cyber stalking shares important characteristics with offline stalking; many stalkers (online or off) are motivated by a desire to Control their victims. A major damaging effect of online abuse is a victim avoiding his/her friends, family and social activities.

Intellectual Property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Bot Networks: The word botnet made from the two words robot and network. A cybercrime called 'Bot Networks', when hackers remotely take control upon computers by using malware software. Computers can be co-opted into a botnet when they execute malicious software. A botnet's originator can control the group remotely.

Transmitting Virus: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.

Hacking: In general words hacking means seeking and exploiting weakness and security of a computer system or a computer network for unauthorized access. The person who do hacking is known as hacker. Hacker use computer expertise and some tool or scripts to hack any computer system.

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's 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's knowledge.

Cracking: It is a dreadful feeling to know that a stranger has broken into user computer systems without user's knowledge and consent and has tampered with precious confidential data and information. Cracker are differ with hacker because hacker are hired by companies to audit network security or test software but cracker do same work for their own profit or to harm others.

Phishing: Phishing means acquire information such as usernames, passwords, credit card details, personal detail etc. by electronic communication. Phishing commonly uses fake emails or fake messages which contain link of virus/ malware infected fake websites. These website request user to enter their personal detail.

Voice Phishing: The term is a combination of "voice" and phishing. Voice phishing is use to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.

Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account.

E-Mail/SMS Spoofing: A spoofed E-mail/ SMS may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. Here an offender steals identity of another in the form of email address, mobile phone number etc. and send message via internet.

Cross-site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefine access permissions of website. Reflected XSS is the most frequent type of XSS attack. Reflected XSS attack is also known as non-persistent XSS. Scripting languages like java script, VBScript etc. are used for Reflected XSS attack.
Cyber Squatting: Squatting is the act of occupying an abandoned or unoccupied space. Cybersquatting is the act of registering a famous domain name and then selling it to needy in high cost. It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

Child Pornography: It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. Child pornography is divided into simulated child pornography and pornography which was produced with direct involvement of the child (also known as child abuse images).

Cyber Vandalism: Vandalism means destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person.

Cyber Trespass: It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

Cyber Trafficking: It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.

Cyber Crime & Social Networking: Cyber criminals use social media not only to commit crime online, but also for carrying out real world crime owing to "over-sharing" across these social platforms**.** The risk associated with our identities. Identity theft can happen to anyone who exposes too much personal information online on various social networking sites. Get to know the security and privacy settings, and configure them to protect from identity theft. One in five online adults (21percent) has reported of becoming a victim of either social or mobile cybercrime and 39 percent of social network users have been victims of profile hacking, scam or fake link.

2.2 Present Trends of Cyber Crime in India

In the case of cybercrime, large numbers of suitable targets may emerge through increasing time spent online, and the use of online services such as banking, shopping and file sharing making users prone to phishing attacks or fraud. The major cybercrimes reported in India are denial of web services, hacking of websites, computer virus and worms, pornography, cybersquatting, cyber stalking and phishing. Nearly 69 percent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information. According to Symantec's (American Global Computer Security Software Corporation) internet security threat report (volume 18) on April 29, 2013, India has seen a 280 percent increase in bot infections that is continuing to spread to a larger number of emerging cities in India. India has the highest ratio in the world of outgoing spam or junk mail of around 280 million per day worldwide. India's home PC owners are the most targeted sector of cyber-attacks. Mumbai and Delhi emerging as the top two cities for cybercrime.

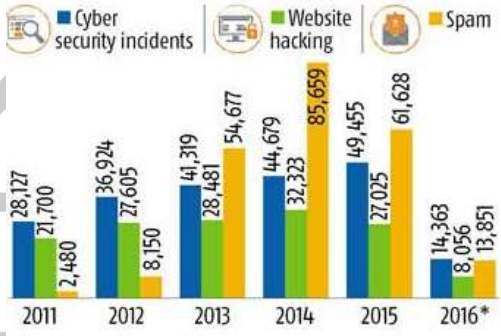

Fig 1: Comparative figure of cyber-crimes

2.3 Cybercrime Prevention Strategies

More recent versions of Cybercrime is considered one the most dangerous threats for the development of any state; it has a serious impact on every aspect of the growth of a country. Government entities, non-profit organizations, private companies and citizens are all potential targets of the cybercriminal syndicate. Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner the prevention of cyber-criminal activities is the most critical aspect in the fight against cybercrime. It's mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their "attack surface" and mitigate the risks.

3. Diagnosing Corruption

A full understanding of the causes of corruption depends on an accurate analysis of its political and economic features. It is important to know whether corruption is primarily individualistic or systemic because a different diagnostic approach should be used depending on which category dominates in some cases, the principal-agent approach may suffice, while in others it will need to be complemented by the wider political economy approach needed to combat systemic corruption.

4. Strategies to Fight General Corruption

Having looked at some of the ways in which corruption damages the social and institutional fabric of a country, we now turn to reform options open to governments to reduce corruption and mitigate its effects. Ackerman (1998) recommends a two-pronged strategy aimed at increasing the benefits of being honest and the costs of being corrupt, a sensible combination of reward and punishment as the driving force of reforms. This is a vast subject. We discuss below six complementary approaches.

- Paying civil servants well
- Creating transparency and openness in government spending
- Cutting red tape
- Replacing regressive and distorting subsidies with targeted cash transfers
- Establishing international conventions
- Deploying smart technology

References:

[1] Vinay Bhargava, "Citizens Fighting Corruption Results and Lessons of an Innovative Pilot Programmed in India", Public Affairs Centre Bangalore, India, 2013.
[2] Lindstedt, Catharina & Naurin, Daniel & D Cand, Ph. (2018). Transparency against Corruption.
[3] Alan Doig, "Dealing with corruption: the next steps", Crime, Law & Social Change 29: 99–112, 1998
[4] Robert Klitgaard, "Addressing corruption together", Addressing Corruption Together, OECD 2015.
[5] Indira Carr, "Fighting Corruption through Regional and International Conventions: A Satisfactory Solution. European Journal of Crime, Criminal Law and Criminal Justice (2007) 121–153.
[6] Donald C. Cole, Lot Jata Nyirenda, Nadia Fazal and Imelda Bates, "Implementing a national health research for development platform in a low-income country A review of Malawi's Health Research Capacity Strengthening Initiative", Cole et al. Health Research Policy and Systems (2016).
[7] Bosnia And Herzegovina, "Anticorruption Strategy FOR 2015 - 2019 and the Action Plan FOR the Implementation OF the Anticorruption Strategy FOR 2015 – 2019", Sarajevo, December 2014.
[8] "Baltic Beach Hotel, "Prevention Of Corruption: Effective Measures And Their Practical Implementation. Institutional and Sectorial Approaches", 26-27 June 2013.
[9] Haidy Ear-Dupuy, "Fighting Corruption with ICT: Strengthening Civil Society's Role", International Publications, 12 August 2016.
[10] Helena Schwer theim, "Innovations in Anti-Corruption Approaches", International Institute for Democracy and Electoral Assistance, 2017
[11] Vienna, "An Effective Tool to Reduce Corruption", Centre for International Crime Prevention December 1999.
[12] Haidy Ear-Dupuy, Olivier Serrat, "Tackling Corruption through Civil Society-led Information and Communication Technology Initiatives", Knowledge Showcases, 2014
[13] Vienna, "Value Added of Partnership in the Fight against Corruption", "Centre for International Crime Prevention, March 2001