STRATEGIES AND INITIATIVES OF CONTROL CYBER CRIME

ABHAY GOYAL

Department of Faculty of Law , Graphic Era Hill University, Dehradun,
Uttarakhand, India 248002

ABSTRACT

Hackers in the cybercrime industry utilize the internet and computer technologies to steal sensitive information from businesses, governments, and individuals. Hackers are the cyber criminals who engage in these acts. Approaches to avoid conflict and tools for engaging in combat, supported by unified troops. Initiatives for the prevention and detection of cybercrime and development of a cybercrime strategy among the enormous number of crimes that plague humanity, cybercrime is the most recent addition. Newline as crimes committed online know no national borders and may have far-reaching consequences, the emergence of cyber law was inevitable. That's why a legislation specifically addressing the prevention of cybercrime is so crucial. Newline the term "cybercrime" is used to refer to any illegal activity that takes place using electronic means of communication, including but not limited to personal computers, tablets, smartphones, the world wide web, and cyberspace. However, these crimes are accessible even to folks who have little to no experience with technology.

Keywords: Cybercrime, Strategies, Education, Law Enforcement, Preventive Measures and Initiatives

INTRODUCTION

Cybercrime, in its most basic definition, refers to any illegal conduct that involves the use of a computer. Due to rising and fast digitalization in the economic, commercial and other domains, reliance on the internet and technology has become a necessity, which we can no longer ignore. This might imply less difficulty in doing business and a more pleasant way of life, but it also poses a greater threat to personal privacy and other sensitive data. Whether you realize it or not, the information you provide on social media may be used to track your whereabouts and personally identify you to the point that you might be blackmailed or threatened into doing anything such as sending money to an unknown account.

Hacking, cyber terrorism, and online fraud are all examples of cybercrime that may wreak havoc on economies and destroy lives. One may wonder what they may do to protect themselves against cybercrime. In this piece, I'll explain what you can do to protect yourself against online fraud and other forms of cybercrime. There may not be a foolproof means to prevent cybercrime, but it is worth noting that the Information Technology Act of 2000, the Indian Criminal Code of 1860, and other laws give the framework to prosecute and penalize those who commit such crimes. Hence, anytime you fall prey to a cybercriminal, it is imperative that you immediately notify the proper authorities.

The term "cybercrime" refers to the practice of using computers for nefarious purposes. Cybercrime, thus, encompasses any illegal conduct that directly or indirectly affects or makes use of any kind of electronic communication or data storage connected to the Internet. Hence, a computer might either be the instrument of the crime or its intended victim. Cybercrime may be seen as an evolution of more conventional forms of criminal activity. Cybercrime is distinct from other sorts of crime due to the fact that it does not include a physical assault and takes place in a non-local context. If someone in the United States gains access to a computer in India, they might potentially conduct a cybercrime from their own location. The reach of cybercrime often exceeds the authority of a single country, making its investigation and prosecution difficult.

Although cybercrime is generally concerned with non-monetary violations worldwide, in India the phrase has become synonymous with women. More often than not, women are the ones who fall prey to technology whims. While the IT Act of 2000 was passed in India as one of the few nations to address cybercrimes, problems specifically affecting women persist gravely. This law defines crimes like as hacking, posting pornographic content online, and data tampering quite broadly. The Act does not, however, address the most serious forms of abuse against women or threats to their safety. Historically, countries like India have paid particular attention to the issue of women's safety. India's crime rate has risen dramatically in recent years. Formerly, women only felt unsafe when they were away from home.

LITERARTURE REVIEW

Poulpunitha, Dr et.al 2020). The development of information and communication technologies has given women a remarkable chance to make the most of their skills and advance their own well-being and the greater good of society. E-mails are only one example of how the Internet has become a social and communication tool. Online crime against women and the spread of pornography are examples of how the Internet may be used to push harmful and discriminatory agendas, but feminists aren't doing enough to resist these uses. Addiction to and overuse of popular social networking sites like WhatsApp, Facebook, Twitter, MSN, and my space leaves many young people open to online predators. There has been a rise in cybercrime due to people's and businesses' reliance on the internet. We discover that in India there is hardly any formal education or training in this area, and this apathy toward technological progress has prepared the road for cybercrimes. Cybercrimes against women and girls are on the rise, but the authorities and police who investigate them often lack the training and knowledge to effectively combat them.

Biswal, Chandra et.al (2020). Its rapid evolution may be seen in a variety of contexts, from the rapidly expanding usage of the internet in educational institutions and new business ventures to the rise of the internet as a popular platform for sports and entertainment. If you want to learn something new but don't know how to use a computer or a smartphone, the internet is your best bet. There are benefits and drawbacks to using the internet. Cyber-crime is the internet's worst drawback. Cybercrime is a growing problem that endangers everyone who uses the internet or a computer. For this reason, governments, police forces, and intelligence agencies in a wide range of nations have become more reactive and stringent in the face of new cyber dangers and the proliferation of cybercrime. Many governments have begun implementing programs to combat cybercrime, cyberterrorism, and other forms of online criminality. Authorities in every nation, including India's, have begun establishing cyber units in every major city and training police officers in the art of preventing cybercrime. Our study primarily focuses on recent fraud and cybercrime incidents in India, as well as the many sorts of cyber-crimes and potential solutions to these problems.

SHAILENDRA GIRI (2019) Online services are vital to human existence since they simplify and improve our everyday lives, but they also provide a number of risks in the form of cyber intrusion, danger, and security. The use of information and communication technology (ICT) in the commission of serious crimes is on the rise. Government agencies, private persons, and businesses are all vulnerable to cybercrime and threats. Cyber intrusion and attack pose serious threats. Protecting e-government systems against intrusion and assault, as well as picking up on any irregularities, is made easier thanks to cyber security strategies, policies, plans, and laws. This article is to investigate cybercrime, cyberthreat, and cybersecurity methods and legislation. This study employs content analysis with survey data collection techniques. Expert examination of cybercrime, cyberthreat, cybersecurity, and cyberstrategies was recommended as a result of the research. Several cyber security laws and regulations have been reviewed in this piece. Strong security in the future relies on our ability to create systems that protect people from harm and recognize when practical solutions aren't enough.

MS. ANISHA (2017) The number of people using the internet in India is growing rapidly. It has sparked fresh possibilities in every area, from showbiz to manufacturing to sports to academia. The internet, like any other tool, offers both benefits and drawbacks; cybercrime is one of the latter. Every crime has far-reaching consequences for individuals, communities, nations, and the whole planet. By keeping an eye on the cybercrime phenomena, we see that, like other crimes before it, it has had a major impact on people's personal and professional lives. As computer technology and the internet are likely the point of genesis for cybercrime, studying their effects on individuals is essential to comprehending the phenomenon. Individuals and vital infrastructure pose constant threats to the IT security and service industry. The goals of social interactions have broadened from purely personal ones to include professional ones as individuals are now more receptive to talking to and working with others from many walks of life. These days, there is no one main reason why individuals use the internet to communicate with one another; rather, there are hundreds. Developing new technologies occurs in a gradual, incremental fashion. This article investigates cybercrime in India under several jurisdictions and examines the critical infrastructure situation in the country.

Manpreet Kaur, et.al (2017) The threat of cybercrime is becoming more severe every day. There is an urgent need to reassess current methods of combating this new phenomenon in the information age, as shown by the results of the 2002 Computer Crime and Security Study. In this article, we define cybercrime and examine the present state of the global effort to combat this growing threat using a variety of legal, organizational, and technical means. We analyze a case study of India's efforts to combat cybercrime and talk about the challenges that country faces. Lastly, we provide a number of suggestions on how the battle against cybercrime might be strengthened.

DEVELOPING A CYBERCRIME STRATEGY

Creating a plan to combat cybercrime may seem like an impossible challenge at first. Formulating a plan is easier with a defined design process to adhere to.

While there are a variety of frameworks from which to choose, the following steps are often included in formulating a policy design:

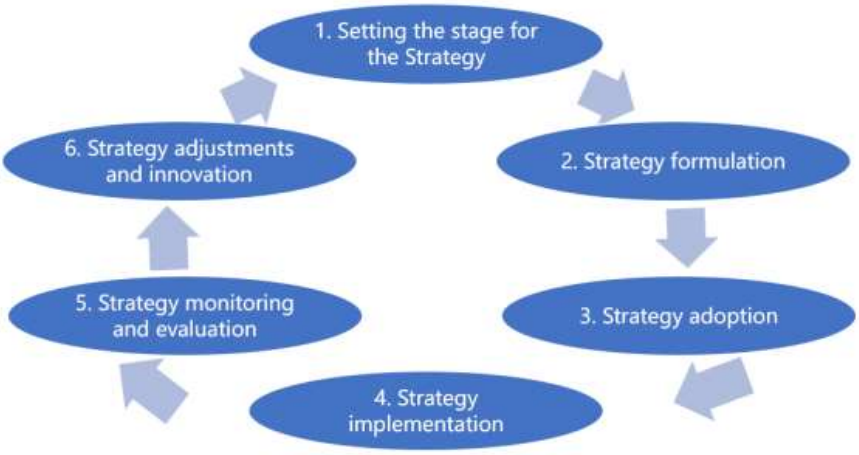
1. Setting the stage for the Strategy
2. Strategy formulation
3. Strategy adoption
4. Strategy implementation
5. Strategy monitoring and evaluation
6. Strategy adjustments and innovation

Figure 1: Strategy Life Cycle

Initializing the Plan of Action Identifying your motivations for implementing a cybercrime plan is the first step. The member nations of INTERPOL report that cybercrime is one of the most rapidly expanding types of international crime. A growing dependence on the Internet has increased dangers and vulnerabilities and opened up new opportunities for criminal conduct, despite the fact that ICT's fast expansion has facilitated economic and social progress. Due to the difficulty of conducting cross-border investigations, the complexity of applicable laws, and regional variations in available resources, law enforcement agencies around the world face difficulties in effectively responding to cybercrime, despite the fact that it knows no geographical boundaries. When faced with these difficulties, a nation may better safeguard its population against cybercrime if it has a well-defined plan in place. As can be shown in the next sections, there are several justifications for and advantages of establishing a cybercrime plan.

a) Cybercrime has a negative impact on the economy.

In the wake of the worldwide Not Petya outbreak in June 2017, ransomware affected logistics companies throughout the world and their clients. Up to $300 million (USD)23 was spent by Maersk on emergency rerouting, compensation, and maintaining the worldwide supply chain. Several of its customers were also adversely impacted, therefore the loss was not confined to the firm itself. Merck, a manufacturer of medical supplies, lost $870 million; FedEx's TNT Express, $400 million; and Cadbury, a producer of chocolate, lost $188 million (USD). In 2016, a distributed denial of service (DDoS) assault employing the Mirai botnet was launched against domain name provider Dyn, effectively shutting down the services of many of the company's 178,000 clients who had their Internet domains hosted by Dyn. Incidents like Stuxnet, a computer virus that affected at least four oil and gas corporations

(Baker Hughes, ConocoPhillips, Marathon, and Chevron), show how cybercriminals have developed and become more sophisticated and pervasive. Cybercrime losses might cost as much as $6 trillion (USD) by 202126, according to the World Economic Forum's Global Risk Report 2020. A cybercrime plan lays out the measures that must be taken to implement sound corporate data governance and sound personal cyber hygiene in order to mitigate the monetary damage caused by cybercriminals.

- The proliferation of cybercrime facilitates traditional criminal activity. The United Nations Office on Drugs and Crime (UNODC) reports that cybercrime is often coordinated by international internet crime networks that funnel the money they make from ransom payments and other illegal activities towards funding terrorism and other severe criminal activity. In addition to aiding CT/AML initiatives, cutting off financing sources for criminal organizations is another goal of a cybercrime strategy.
- Governmental operations are hampered, and even lives, by cybercrime. In every sector, ransomware assaults cause chaos. Several hospitals and government healthcare institutions have had patients' lives jeopardized because of computer system failures. The WannaCry ransomware outbreak in 2017 impacted the National Health Service (NHS) in the United Kingdom, disrupting hospital systems even as surgeons performed life-or-death procedures including open heart surgery. A similar ransomware attack occurred in September of 2020 against a hospital in Düsseldorf, Germany. A woman with a life-threatening illness was transported out of the hospital because of its closed systems, but she later died because of the delay in care. Together, a cybercrime plan and a cybersecurity strategy can guarantee that essential services will continue to run smoothly.
- the advantages of developing a plan in addition to its other advantages, having a strategy:
  a) educates those who can make positive contributions and reap the rewards;
  b) learns more about a country's vulnerabilities;
  c) shows that progress is being made in confronting the cybercrime challenge;
  d) provides a framework for preventing, detecting, and responding to cybercrime; and
  e) increases awareness.
- Requirements for a strategy

Establish a project authoritySecuring and sustaining the commitment of necessary stakeholders is a frequent difficulty in implementing a cybercrime strategy. Determining who will be in charge of the cybercrime strategy's creation, rollout, and revision requires the selection of a "project authority" that includes a high-ranking official (preferably a minister) and a project team. The higher-ranking official is responsible for maintaining the document and ensuring that:

a) The project team has the support of all relevant parties, and there are enough resources to put the plan into action. The Minister of Home Affairs, for instance, may play the role of the senior official, while the national cybercrime unit's members could make up the project team. The project group might also be a collaborative group. The person in charge of the project is included in the steering committee. Successful implementation of the cybercrime strategy depends on having the correct leader and project team.

b) Get support from inside your own government. Effective strategy creation calls for collaboration inside an organization. The task may be challenging and calls for strong leadership, efficient teamwork, and, in many cases, compromise. For the cybercrime strategy to be successfully drafted and implemented, internal agency collaboration at all phases of the project is essential. The project management team should reach out to the appropriate partner agencies to solicit advice and support for the undertaking. After consensus is reached on the project's overall idea, the project authority should put in place a system to facilitate collaboration across different levels of government. As part of this structure for collaboration, all relevant parties may periodically convene, such as in the form of a steering committee Before beginning the project, be sure that all necessary partner agencies have given their approval.

c) Get your hands on a significant amount of money and materials Government organizations often face budget and resource limitations. As a result, progress on a national plan to combat cybercrime may be slowed. Successful completion of the project depends on careful preparation and the allocation of sufficient resources. Expenditures (in the form of a set budget) and human resources are included (i.e. dedicated project staff). Similarly, the cybercrime plan can't be put into action without a sufficient investment of time and money Before beginning the project, make sure you have all the necessary materials.

d) Create SMART targets. Objectives in the cybercrime strategy life cycle should be SMART30, or Specific, Measurable, Attainable, Relevant, and Time-Bound. So, the first step of the project is to set concrete, time-bound objectives, complete with concrete, quantifiable milestones and firm delivery deadlines. For instance, within that time frame, you may determine who needs to be involved in each phase of your cybercrime plan. Think about using this tactic to help you get your thoughts straight, narrow your focus, make the most efficient use of your time and energy, and boost the odds of success for your project and your plan.

b) Strategy formulation

For the reasons and gains outlined above, this is the stage when the cybercrime strategy is developed.

Determining Who Should Be on the Steering Committee and Listing Other Important Parties Stakeholder participation and management have been shown to be crucial to the effectiveness of public policies31. It's common practice to ignore or underinvest in strategies that fail to win over key stakeholders. To begin, it's helpful to form a steering committee consisting of the project authority and other relevant senior-level officials. These individuals should be chosen based on their ability to provide strategic oversight and guidance throughout the various phases of the cybercrime strategy life cycle. The steering group should draw up a list of everyone who needs to have input on the cybercrime strategy. The consulting community's stakeholders ("the consultants") would generally hail from the public and nonprofit sectors. Agencies within the government:

Other Law Enforcement Agencies to help with regional issues and processes for investigating cybercrime, like e-evidence collection; Relevant senior official(s) from applicable mi to help with exchanging information on cybercrime investigations; The National Cybercrime Unit to facilitate the exchange of information on cybercrime investigations; The lead agency for cybersecurity to share experience in cyber incident response and drafting of cybersecurity policies including strategies; Ministry of Home Affairs and Ministry of Law or Justice personnel, for example;

• Prosecutorial and judicial authorities who may provide guidance on the implementation of national cyber legislation;

• Other appropriate government personnel and teams, including fraud investigation departments, ICT ministries, public safety and security agencies, etc. Groups Outside of Government:

It is the technology and industry organisations that are in the best position to identify the greatest hazards affecting companies, while civil society groups are most suited to assist increase public awareness.

• Organizations at both the regional and international levels should collaborate to discuss cybercrime in their respective regions. The cybercrime strategy might benefit from having a solid groundwork if the correct experts are chosen to address the demands of all stakeholders. If key players weren't involved from the start but are brought in later, they might potentially derail the whole process. First, consultants are found, and then, from among them, only those most suited for the drafting activity are chosen to create the strategy

Taking inventory, doing an evaluation, and analyzing In order to effectively fight cybercrime, it is essential for a government to assess the methods, resources, and capabilities at its disposal. We may learn a lot about our weaknesses through this activity as well. By doing so, a nation may better understand its existing cybercrime scenario and take steps toward its intended future of increased cyber defense capacity. The following factors should be considered during the stocktaking audit:

Humans and machinery Cybercrime-related functions, such as cybercrime and digital forensics professionals, cybersecurity workers, and CERTs, are evaluated in this audit. The following are some examples of possible organizations to include:

Departments and units of the National Police Agency

Authorities at the national level in charge of cyber defense (if any) CSIRT/CERT (Computer Emergency Readiness Team) of the National Institute of Standards and Technology Central Authority for Managing Mutual Legal Assistance Treaties

- Justice or Law Ministry on the National, Regional, and State/Provincial Levels o Specialized Cybercrime Judges o Specialized Cybercrime Prosecutors o Specialized Cybercrime Investigations Unit (MLATs) Authorities at the national level in charge of combating cybercrime include:
- Security and intelligence agencies;
- Other relevant national departments (e.g. fraud, exploitation, etc.)
- Additional law enforcement agencies at the state or provincial level that have cybercrime investigative sections. The following should be reported by each of these departments:
- An explanation of the structure and goals of their organization and the relevant department What kinds of cybercrime do they investigate? What laws do they follow? What anti-cybercrime programs do they now have in place? Think at each organization's technical capacities as well; do they have the necessary tools and expertise to complete the task at hand?

Production The creation of the cybercrime strategy is the most time-consuming part of the strategy's life cycle. This Handbook is intended to serve as a model for use by nations as they undertake the task of crafting their own

Conversations with relevant parties The Focus Areas should be presented to the stakeholders ("consultants") in an iterative process. Participants in the strategy development process are given a chance to have their voices heard about the best means by which the Focus Areas may be advanced, and hence the Strategic Goals

This is the preliminary version of our plan to combat cybercrime. Here, the cybercrime strategy's designated group of drafters begins to construct an initial version of the plan, taking into account the considerations and advantages indicated in section and the findings of the stocktaking reported

It's common procedure for a plan to go through several revisions after being written, discussed, reviewed, and tweaked. When this is done carefully, the final plan has a better chance of being supported by all relevant parties. Cybercrime Strategy Template provides a suggested outline for the document that may be used as a guide by the drafters.

Take-up of Strategy After the conclusion of the plan development phase, the finished cybercrime strategy document may be submitted officially for acceptance and execution. The specifics of this procedure will vary depending on the nation. Before being offered for endorsement, e.g., approved in Parliament/National Congress/Assembly, or sent to the Head of Government/State, the plan may need to be discussed in a national assembly, parliament, or other public policy forum in certain nations.

Strategy and Policy Making Implementing the cybercrime plan successfully requires a methodical strategy. The specifics of the rollout will vary by nation, but often include the following:

the details of how the Strategic Goals will be achieved Creating individual plans for each Action Item committing sufficient time, money, and people to the endeavor. In order to achieve the project's Strategic Goals, the project management team and the consultants must create Action Items and an implementation strategy, assigning responsibility for each action item to a particular individual or department Representatives from the departments or organizations most suited to carry out their actions should be given responsibility for them.

These individuals or groups would subsequently be responsible for carrying out the strategy that had been delegated to them. Plans for implementation should be described in a way that makes them easily understandable to the agencies tasked with putting them into action (action owners). Sometimes it's up to the project manager to make sure all the plans are put into action in tandem. The steering group may have to help get enough money to carry out all the ideas. That will guarantee that the work done up to that point was not for nothing. The progress of each Action Item may be tracked by referring to the implementation plans, which should contain appropriate metrics and success indicators.

The Evaluation and Supervision of Strategies

To maintain forward momentum, the project authorities and the consultants should prepare for the cybercrime strategy to be reviewed and assessed at regular intervals, as outlined in the SMART objectives section (4.1.5.4). If the implementation efforts are not constantly monitored, not just the individual Action Items, but the whole project, might be in danger. Maintaining momentum in the execution of the cybercrime strategy requires regular communication between the action owners and reporting on the predetermined KPIs. Details on the availability of resources, potential obstacles, and lessons learned should all be tracked as part of the monitoring process. If there are going to be any holdups, the project manager should be informed as soon as possible so that they can begin making adjustments. On the flip side, accomplishments have to be communicated to the project authorities so that they may be acknowledged.

Strategies To Prevent Cybercrime

- The ideal method to deal with these cybercrimes would be a collaborative effort combining the actions and measures made by the Government and other legislative authorities to combat such crimes.

- Cyberstalking may be avoided if you don't give out any identifying information about yourself online.

- Crimes against women have been linked in part to the practice of exchanging private photos with chat partners, both known and unknown. It is crucial that you refrain from doing anything illegal.

- It is very prudent to protect the privacy of customers' credit and debit card information. If you want to be sure the deal, you're making is legit, you need to verify several reputable sites.

- Protect and safeguard women and children against the occurrence of such heinous crimes by empowering and educating them with the information and awareness they need.

- The use of firewalls may be a good initial line of protection against these kinds of intrusions. Make sure that security measures are used securely. While dealing with potential dangers, you should always use the router's built-in firewall and remember to be alert and cautious. Ignore your whims

- Be well-versed in the developments in technology and the internet to avoid damage, and learn the legal structure and processes associated with such offenses so you can respond quickly if you're ever caught.

PREVENTION OF CYBER CRIME: INITIATIVES

1. Accountability Principle: For the sake of everyone's peace of mind, it's important to lay out in detail the roles and responsibilities of those responsible for maintaining the integrity of factual systems, including users, employees, and owners.

2. Awareness Principle: Users, providers, users, and other parties should be able to easily attain adequate, consistent with preservation of security, awareness and learning about the presence and common amount of part, routine, and method for the privacy of information systems in order to promote assurance in those systems.

3. Ethics Principle: It's important to distribute and use information and security systems in a way that respects the privileges of others.

4. Multidisciplinary Principles: All relevant applications and aspects, including technical, policymaking, managerial, functional, economic, and legal ones, should be considered and accounted for when developing standards, form, and techniques for protecting information systems.

5. Proportionality Principle: It is important to strike a good balance between the value and degree of dependence on the information system, as well as the severity, likelihood, and wide scope of capacity that can be harmful as the necessity vary build upon the information system, when determining appropriate levels of insurance, finances, routine, and methods.

6. Integration Principle: It is important for companies to develop a well-balanced security system, which requires that laws and regulatory techniques for the privacy of information system be associated and united with each other and other principles of the businesses.

7. Timeliness Principle: To prevent and respond to information security gaps, public and private actors on a national and international scale should work together in an efficient and coordinated manner.

8. Reassessment Principle: These are the periodic recognitions that call for a reevaluation of the security of information systems, and that moment is now.

9. Democracy Principle: In a free society, the security of information networks must be compatible with the free flow of information.

CONCLUSION

There are more and more cases of identity theft, hacking, and harmful malware every day. Inscrutable security, which employs a unified system of software and hardware to verify any information that is accessed via the Internet, is one of the greatest methods to thwart these thieves and safeguard important information. The government has taken many measures, including publishing alerts on cyber dangers and establishing Cyber Swacchta Kendra, among others. The boundaries of cyberspace are infinite. Offenders may remain anonymous on the web, making it difficult, if not impossible, to track down a sophisticated hacker. This means that individuals need to exercise the same level of caution online as they would in the real world. As a result of reading this article, you should be better equipped to safeguard yourself against cybercrime and reduce the dangers connected with it.

REFERENCES

1. Poulpunitha, dr & kalidasan, manimekalai & p., veeramani. (2020). Strategies to prevent and control of cybercrime against women and girls. International journal of innovative technology and exploring engineering. 9. 2278-3075. 10.35940/ijitee.k2408.019320.

2. Biswal, chandra & pani, dr. Subhendu. (2020). Cyber-crime prevention methodology. 10.1002/9781119711629.ch14.

3. Shailendra giri (2019) cyber crime, cyber threat, cyber security strategies and cyber law in nepal. Issn no: 2249-2976

4. Ms. Anisha (2017) awareness and strategy to prevent cybercrimes: an indian perspective | issn - 2249-555x

5. Manpreet kaur, gurinder kaur, er. C.k. Rain (2017) cyber crime and its preventive measures issn (online) 2278-1021 issn (print) 2319 5940

6. Bagyavati (2009) 'social engineering' in lech j.janczewski and andrew m.colarik cyber warefare and cyber terrorism

7. Bargavi and sheeba (2009 november) 'safety issues in orkut for girls', unpublished.

8. Brunker, m. (2009). 'sexting' surprise: teens face child porn charges, 6 pa. High school students busted after sharing nude photos via cell phones. Retrieved on 26th january 2010.

9. Dittrich, dave. "the "stacheldraht" distributed denial of service attack tool." university of washington. University of washington, 31 dec. 1999. Web. 28 nov. 2011.

10. High technology crime investigation association. "2010 report on cybercrime investigation." high technology crime investigation association. Htcia, inc., 2010. Web. 28 nov. 2011

11. Nature and impact of cybercrime against college girls in karaikudi, published centre for women's studies, 2013

12. Snell, p.a. And e.k. Englander, 2010. Cyber bullying victimization and behaviors among girls: applying research findings in the field. J. Soc. Sci., asian social science, vol. 8, no. 15; 2012, canadian centre of science and education

13. Mulligan, d.k. & schnelder, f.b.(2011). Doctrine for cybersecurity. Daedalus 140(4), 70-92. Doi:10.1162/daed_a_00116.

14. Pandey, b. P.(2017), challenges of the grievance handling in public service delivery and the use of information technology, journal of personnel training academy. Lalitpur: pta, nepal. 5(l). 1, pp. 124-136.

15. Godbole, n., belapure, s. (2011) cyber security, ‘understanding cybercrimes’, computer forensics and legal perspectives, wiley india pvt. Ltd., (1st ed.), isbn: 978-81-265-2179-1