International Journal of Future Generation Communication and Networking
Vol. 12, No. 5, (2019), pp. 285- 293

CYBER EXPERTS AWARENESS, PREVENTION MEASURES AND SUGGESTIONS TO MANAGE CYBERCRIMES IN INDIA

[1]Ishwar Navalagund, [2]Dr.G.S. Venumadhava
[1]Research scholar, Department of Studies and research in Criminology and forensic science, Karnatak University, Dharwad; [2]Assistant professor and coordinator, Department of Studies and research in Criminology and forensic science, Karnatak University, Dharwad

Abstract:

Cybercrime security experts are those people who use to known cyber-world absolutely, understood completely and aware absolutely, practice and professional authorized to protect all legal platforms in cyber world. A forensic team must have in-depth know-how of every investigation. The present study gathered opinion and suggestions from cyber experts which comprised of primary data was collected through questionnaire from 50 respondents (Cyber Experts) in different parts of Karnataka. The results were analyzed using chi-square tests. Results revealed that a large Majority of the cyber experts had awareness about computer related crimes. This paper gives detailed information regarding cyber experts who had awareness regarding economic frauds. Majority of the cyber experts had awareness related to cybercrimes related to privacy. Not disclosing personal information, public appraisal regarding cybercrimes, strict enforcement of law, and protection of public sites from hacking were the suggestions offered by the cyber experts to manage cybercrimes.

Keywords: *cyber-world, forensic team, resources, security, suggestion, enforcement agencies.*

I. Introduction:

Cybercrime is an offense which involves the use of digital technologies in commission of crime, directed to computing and communication technologies over electronic speed entire globe. The modern technology that is proliferating towards the use of internet activity results in creating exploitation, vulnerability making a suitable platform for unlawful act. Cybercrime security experts are those people who use to known cyber-world absolutely, understood completely and aware absolutely, practice and work in the cyber world. The universal approach of network like web in any respect levels of network must get over committing criminality all told over the planet and to prevent the criminal nature by protective unlawful activity by implementing completely different level of firewall setting among its offline management for each nation so as to watch and prevent crimes committed in Internet. Network security controls area unit accustomed forestall the access of hackers in networks which incorporates firewall, virtual private networks and encryption algorithms. Out of those, the virtual non-public network plays a significant role in preventing hackers from accessing the networks.

Cyber-security may be a field that encompasses more than one kind of work and more than one occupation or profession. There are today large numbers of experts within organizations who have responsibility for cyber-security functions, like frontline IT support staff, for whom there might not be any formal education or accreditation requirements. The organizational context for cyber-security work is diverse, ranging from firms that have highly proficient cyber-security groups to ones where cyber-security is one of the responsibilities of general IT groups. There also are varying approaches to how work is split between the cyber-security workforce and therefore the broader IT workforce— some cyber-security positions are clearly hybrid in nature, blending cyber-security roles with other roles in IT, management, or law enforcement. Even during this case, however, the committee learned that not all agencies that employ digital forensics examiners currently favor external certification.

Given the good diversity of roles, responsibilities, and contexts, the very fact that expertize measures could also be warranted during a particular subfield and context shouldn't be confused with a broad need for professionalization. Those organizations that find professionalization helpful can certainly enforce some sort of certification or other professionalization measure for the workers they hire, and variety of organizations inside and outside government do so today. Other organizations, having given

this serious thought, may find other ways to optimize and customize their hiring and cyber-security workforce composition to best meet their specific needs.

The terms “cybercrime,” "computer crime", "Information Technology crime," and "high-tech crime" are often used inter-changeably to refer to two major categories of offenses: in the first, the computer is the target of the offense; attacks on network confidentiality, integrity and/or availability, i.e. unauthorized access to and illicit tampering with systems, programs or data – all fall into this category (Goodman, 2001). The other category consists of traditional offenses such as theft, fraud, and forgery – that are committed with the assistance of or by means of computers, computer networks and related information and communications technology. Computers can also play an incidental role in the commission of a traditional offense, as when a blackmailer uses a computer to generate blackmail letters (or e-mails) or a drug dealer who uses speedy tracking of drug purchases and sales. This is not to say that they pose no challenges for law enforcement; like the “true” cybercrime brethren, they will contribute to an enormous amount of cyber-forensic work which will soon become a routine part of criminal investigations, for which law enforcement is totally unprepared (Olson, 1997; Amis, 2001)

After an occurrence of cyber-attack, collecting all relevant evidence is of utmost significance in responding appropriately to the questions which were outlined above. A forensic examiner or investigator is primarily concerned with a specific piece of evidence, which is known as, international journal of research in engineering, it and social sciences latent data is also known as ambient data. In the cyber security world, ambient data is a type of data that is not easily accessible or visible at first glance at the scene of a cyber-attack. In simple terms, latent data requires an extra mile from a security expert for it to be accessed as significant evidence. An expert has to engage themselves in much more in-depth investigations to unearth this type of data. Ambient data has many uses to it, and it is equally important just like other types of data except that it is implemented such that access to it has been minimal (Ochieng, 2019)

The forensics team is expected to follow a given structure while executing their documentation process. The contents of their documents are required to be preserved, verified, and appropriately documented. Forensic team must have in-depth know-how of every investigation. This should be right from the beginning of the project and should cut through the scope, dimensions, and the various methods used for the investigation process. The methods used should be proper and legal such as the legal obtaining and collection of proper bit-stream “hash encrypted” copies of evidence. The linear nature of investigation should be primarily based on proper documentation and concrete supporting evidence to avoid unexpected results that technology might yield.

Covert policing is by no means the monopoly of state policing and security services. Private individuals, members of non-government organizations, and commercial entities have all engaged in investigation for a variety of motives, including a sense of civic responsibility, moral indignation, or commercial gain (Fronc, 2009; Tusikov, 2017)

In addition to law enforcement and security firms, every organization should develop the capacity to solve their basic issues and investigations internally. In the case where it is not possible to form a competent investigative team within the organization, then you can hire experts from small computer investigation firms to aid with investigations. An organization can also create their own investigative firm to supply computer forensic services. To do so, the following key people form part of your investigation team. Cybercrime is not restricted to the desktop alone; mobile devices have proliferated in recent years, and with them viruses, malware, and phishing scams. Because of its open marketplace, the android platform is home to a variety of malware in particular. In a recent survey, 72% of all apps for the computer operating system were regarded as suspicious, unwanted, or malicious, with Trojans making up the majority of threats (team, 2019).

By the mid-1980s, crime was a longtime channel to manage and destroy laptop systems, acquire data, and steals millions in money. Action was needed, and in 1986 the first cybercrime legislation was passed—the federal computer fraud and abuse act; making harmful computer activity a felony crime punishable by jail time and fines. Since those days, cybercrime has evolved and grown. Criminals vary from resolute hackers advanced networks of agents operating in unison to state-sponsored attacks across nations. Threats are ever present as the world

becomes more and more interconnected and with more connected devices every year, coupled with the emerging sector of the internet of things, the opportunities for cybercrime persist for the inventive and daring hacker. (Parker, 2000)

Cyber security challenges

a) Cyberspace has inherent vulnerabilities that cannot be removed
b) Innumerable entry points to internet.
c) Assigning attribution: Internet technology makes it relatively easy to misdirect attribution to other parties
d) Computer Network Defense Techniques, tactics and practices largely protect individual systems and networks rather than critical operations
e) Attack technology outpacing defense technology
f) Nation states, non-state actors, and individuals are at a peer level, all capable of waging attacks (Saraswat, 2019)

Impact of Cybercrime: It is estimated that cybercrime costs businesses more than $12.7 million annually in the United States alone, attacks on American businesses and organizations increased by 176 percent in 2014; that's 138 successful attacks each week. These attacks are also taking more time to resolve as well, with the worldwide average to detect an attack at 170 days, the longest average time at 259 days and the average time to resolve an incident at 45 days. Virtually every US industry deals with the impact of cybercrime, with the highest annual costs in the energy & utilities and defense industries. (Cybercrime & Security Overview, 2019).

- **Form of Cybercrime Impact**

a) Direct financial loss. b) Damage to company and brand reputation. c) Loss of sensitive data and intellectual property. d) Mitigation and recovery costs. e) Regulatory penalties. f) Customer compensation and g) Job loss.

This present study is focuses on the cyber exerts attitude towards cybercrime, as cyber-security in particular and national security at large scale. Cyber experts are the protector, oasis to the digital citizen of the any country present day cyber experts are 5th sector as well. Cyber experts are now United Nations defense sector as well because nowadays all defense equipment are controlled and managed by cyber technology only so for that reason cyber warfare is very important sector in present work that to there is plenty of opportunity for cyber experts in all sectors.

II. Sample size:

The study comprised of primary data which was collected through questionnaire from 50 respondents Cyber Experts in different part of Karnataka. A questionnaire has been prepared and interviewed the respondents to collect data. From said category 50 respondents were interviewed based on questionnaire for present study.

- **Tools Employed:**

a) Demography data:

The demography data comprised of the name, age, educational qualifications a) graduation b) post graduate c) above post graduate. Gender a) male b) female and c) others and profession, a) government employee and b) private employee

a) Awareness and suggestions among Cyber experts:

Following awareness and suggestion related questions were asked to the experts with the answering options of 'yes' or 'no'. The questions statements related to awareness are, q1a) Cyber bullying, b) Hacking, c) DDOS Attack, d) Botnet, e) Malvertising, f) Online Lottery Fraud g) Free Gift Offers, h) Credit Card Fraud, i) Debit Card Fraud, j) Online Transaction k) Email Spoofing, l) Identity Threat m) Computer Viruses, n) Spamming, o) Phishing, p) Child Pornography. The questions/statements regarding suggestions to manage cybercrimes were; q2. Do you feel one should avoid disclosing any

personal information to strangers via email or chat? q2) whether you prepare web servers running public sites must be physically separately protected from internet corporate networks q3) do you prepare an update antivirus software to guard against virus attacks q4) whether strict statutory laws need to be pass by the policy makers keeping in mind the interest of citizen q5) do you conduct proper procedure in investigation of cybercrimes q6) do you have sophisticated equipment to handle cybercrime q7) do you have resource persons to handle tools and equipment's of cybercrime q8) do you update regularly upcoming tools and technologies in cyber investigation q9) do you have intranet server to communicate to exchange the information one to other organization in cybercrime investigation q10) do you feel law enforcement authority has to outsource some cyber investigations to other experts and q11) do you think public have to appraised about cybercrimes and related problems. q12a) use strong passwords, q12b) use strong passwords, q12c) biometric password, q12d) use a firewall, q12e) click with caution, q12f) practices safe shopping, q12g) use comprehensive security software and keep your system updated, q12h) secure your wireless network, q12i) use common sense, q12j) use genuine antivirus and q12k) others, q13a) Prevention used Against Cybercrime, Use strong passwords, b) Biometric Password, c) Use a firewall, d) Click with caution, e) Practice safe shopping, f) Use comprehensive security software, g) Secure your wireless network, h) Use common sense using NET, i) Be suspicious, j) use Antivirus, k) Other

III. Theoretical Framework:

a) Burgess and Baker (2002) in a study on offline and online stalking studied 656 persons. Findings of the study indicated that 11 per cent had been harassed. 61% of the complainants were female in the age group of 17 to 42 years. 55 per cent belonged to the age group of 20 years and below. According to the
b) Budd and Mattinson (2000), studied on individuals between the age group of 16 and 24 years and found that those who living alone, students, those living in privately rented accommodation or flat and those living in low income of less than 15,000 $ per annum were vulnerable to cyber victimization
c) Fall (2012) also stated that victims were most often females and nine out of ten victims were females. Offenders were males and three-fourths of cyber stalking offenders were males.
d) Hutton and Haantz (2003) try to explain regarding cybercrime as anyone in any point in time be a victim in cyber space, but certain demographic groups such as women, youths, beginners to the internet and other specific vulnerable groups are more at danger compared to others.
e) Jaishankar and Sankary (2006) in their article discussed the characteristics of the victims of cyber stalking. the majority of the victims were females. victims belong to the age group of 18 – 32 years often involved in a real or imagined romantic or sexual relationship with the offender. according to the authors, the victims may be "member of a targeted minority group or special ethnic group, racial and religious minorities, gays and lesbians, cancer or other patients with serious illnesses, adoptive or birth parents, political or special interest group".
f) Mala and Ramdoss (2011) in an empirical study among female students of a university, found that 32% of the respondents were victims of cybercrimes (n=83). only 2% of them reported their victimization.
g) Sissing (2013), in her study found that majority of the cybercrime victims were females. the participants were young and belong to the age group of 18 to 25 years. the majority of the victims shared that they were cyber stalked through social networking sites by strangers. significantly, none of the participants were relatives or ever romantically involved with their cyber stalkers.
g) Waschke (2017), opined that traditional anti-virus software and private firewalls not suffice to ensure personal security. users who neglect to find out and adopt the new ways of protecting themselves in their work and personal environments put themselves, their associates, and their companies in danger of inconvenience, violation, reputational damage, data corruption, data theft, system degradation, system destruction, financial harm, and criminal disaster. this book shows what actions to require to limits the harm and get over the damage.
h) Dowdell (2017), commenting on specific cybercrime, a senior south Australian detective was quoted as warning "it is not appropriate for individuals to take matters into their own hands because no matter how well intentioned they may be, this can significantly obstruct and hinder what police are

empowered to do." noting the potential for violence in such matters, he added "there is a very real risk to both parties when someone chooses to take the law into their own hands".

the present study aims at assessing awareness and suggestions to manage cybercrimes where how cyber experts involves in having protected, means of information cyber professionals to the users of the virtual world.

IV. Statistical Tools:

a) Descriptive Statistics:

Frequency and percent statistics were used as descriptive statistics in the present study

b) Inferential Statistics: Chi-square test has been employed to find out the difference between 'yes' and 'no' frequencies for both awareness and suggestions statements.

V. RESULTS AND DISCUSSION

Table 1: Awareness regarding Computer related crimes
Frequency and percent responses on awareness on various 'computer related crimes' and results of chi-square tests

Sl. No.	Computer related crimes	Response	F	%	Chi-Square	P Value
	Cyber bullying	Yes	46	92.0	35.280	.001
		No	04	08.0		
	Hacking	Yes	50	100.0	-	-
		No	00	00.0		
	DDOS Attack	Yes	48	96.0	43.320	.001
		No	02	04.0		
	Botnet	Yes	47	94.0	38.720	.001
		No	03	06.0		
	Malvertising	Yes	45	90.0	32.000	.001
		No	05	10.0		

When the responses were calculated for knowledge regarding computer crimes, a majority of the cyber experts had knowledge regarding hacking (100.0%), DDOS attack (96.0%), Botnet (94.0%), cyberbullying (92.0%) and malvertising (90.0%). Chi-square tests revealed significant differences between 'yes' and 'no' responses for hacking, DDOS Attack, Botnet and Malvertising. The chi-square values obtained for 'yes' and 'no' responses for cyber bullying, DDOS attack, Botnet and malvertising were 35.280, 43.32, 38.72, and 32.00 respectively, which were significant at .001 level.

Table: 2 Awareness related to economic frauds
Frequency and percent responses on various 'Crimes related to economic frauds' and results of chi-square tests

Sl. No.	Economic Frauds	Response	F	%	Chi-Square	P Value
1.	Online Lottery Fraud	Yes		96.0	43.32	.001
		No	02	04.0		
2.	Free Gift Offers	Yes	48	96.0	43.32	.001
		No	02	04.0		
3.	Credit Card Fraud	Yes	50	100.0	-	-
		No	00	00.0		
4.	Debit Card Fraud	Yes	50	0.0	-	-
		No	00	.0		
5.	Online Transaction	Yes	50	0.0	-	-
		No	00	.0		

	Fraud					
6.	Scamming	Yes	48	.0	43.32	.001
		No	02	.0		
7.	Software Piracy	Yes	50	0.0	-	-
		No	00	.0		

All the cyber experts had the knowledge of frauds related to credit card (100.0%), debit cards (100.0%), online transaction (100.0%), and software piracy (100.0%), and large majority of them had awareness regarding online lottery frauds (96.0%), free gift offers (96.0%) and scamming (96.0%). Chi-square tests revealed significant differences (X^2= 43.320, 43.320 & 43.320; p=.001, .001 & .001 respectively) between 'yes' and 'no' responses for Online Lottery Fraud, Free Gift Offers, and for Online Lottery Frauds. However, all of the cyber experts knew about the credit card fraud, debit card fraud, online transaction fraud and about software piracy.

Table 3: Awareness regarding Crimes related to privacy
Frequency and percent responses on various 'Crimes related to privacy' and results of chi-square tests

Sl. No.	Crimes related to privacy	Response	F	%	Chi-Square	P Value
	Email Spoofing	s	45	90.0	32.000	.001
			05	10.0		
	Identity Threat	s	50	100.0	-	-
			00	00.0		
	Computer Viruses	s	50	100.0	-	-
			00	00.0		
	Spamming	s	40	80.0	15.680	.001
			10	20.0		
	Phishing	s	49	98.0	46.080	.001
			01	02.0		
	Child Pornography	s	50	100.0	-	-
			00	00.0		

When awareness cybercrime related to privacy were analyzed following results were observed. All the respondents knew about identity theft, computer viruses and child pornography. A large majority of them knew about Phishing (98.0%), email spoofing (90.0%) and spamming (80.0%). Chi-square tests revealed significant differences (X^2= 32.000, 15.680 & 46.080; p=.001, .001 & .001 respectively) between 'yes' and 'no' responses for knowledge regarding email spoofing, spamming and phishing.

Table 4: Preventive Measures among cyber experts
Frequency and percent responses on various 'Crimes related to privacy' and results of chi-square tests

Sl. No.	Preventive Measures	Response	F	%	Chi-Square	P Value
1	Prevention like; Use strong passwords	Yes	47	94.0	38.720	.001
		No	3	6.0		
2	Biometric Password	Yes	47	94.0	38.720	.001
		No	3	6.0		
3	Use a firewall	Yes	44	88.0	28.880	.001
		No	6	12.0		
4	Click link with caution	Yes	42	84.0	23.120	.001
		No	8	16.0		
5	Practice safe shopping	Yes	47	94.0	38.720	.001

		No	3	6.0		
6	Use comprehensive security software	Yes	38	76.0	13.520	.001
		No	12	24.0		
7	Secure your wireless network	Yes	44	88.0	28.880	.001
		No	6	12.0		
8	Use common sense using NET	Yes	47	94.0	38.720	.001
		No	3	6.0		
9	Be suspicious in virtual world	Yes	48	96.0	42.320	.001
		No	2	4.0		
10	Using Antivirus	s	48	96.0	42.320	.001
			2	4.0		
11	Other	s	1	2.0	46.080	.001
		No	49	98.0		

When the responses were calculated for knowledge regarding preventive measures, a majority of the cyber experts had knowledge regarding use strong password, Biometric Password, Practice safe shopping, Use common sense using NET (94.0%), ($X^{2=}$ 38.720–P= .001). Use a firewall (88.0%), Click link with caution (84.0%), Use comprehensive security software (76.0%), Be suspicious in virtual world and Using Antivirus (96.0%) (X^2= 28.880/ 23.120/ 13.520/ 42.320 & 42.320; p=.001, .001, .001,. 001 & .001 respectively). Chi-square tests revealed significant differences between 'yes' and 'no' responses for use strong password, Biometric Password, Practice safe shopping, Use common sense using NET. The chi-square values obtained for 'yes' and 'no' responses for ($X^{2=}$46.080) which were significant at .001 level.

Table 5: Opinion and Suggestion among Law Enforcement (Police)
Frequency and percent responses on various 'remedies to avoid cyber crimes' and results of chi-square tests

Sl, No.	Opinion and Suggestion among cyber experts	Response	F	%	Chi-Square	P value
1	Avoiding disclosing any personal information to strangers	Yes	50	100.0	-	-
		No	0	0.0		
2	Web servers Running Public Sites must Separately Protected from Internet private Networks	Yes	42	84.0	23.12	.001
		No	8	16.0		
3	Updating Antivirus Software to Guard Against Virus Attacks	Yes	35	70.0	8.00	.005
		No	15	30.0		
4	Strict statutory cyber laws need to be pass by the policy makers keeping citizen safe	Yes	45	90.0	32.00	.001
		No	5	10.0		
5	Conducting proper Procedure in Investigation of Cybercrimes	Yes	39	78.0	15.68	.001
		No	11	22.0		
6	Availability of Sophisticated equipment to handle cyber crime	Yes	31	62.0	2.88	.090
		No	19	38.0		
7	Having specialists to handle tools and equipment of cyber crime	Yes	33	66.0	5.12	.024
		No	17	34.0		
8	Updating regularly upcoming tools and technologies in cyber investigation	Yes	33	66.0	5.12	.024
		No	17	34.0		
9	Having intranet server to communicate to exchange the information inter organization during cybercrime	Yes	27	54.0	0.32	.572
		No	23	46.0		

	investigation					
10	Law enforcement authority has to outsource some private cyber experts	Yes	44	88.0	28.88	.001
		No	6	12.0		
11	Public has to appraised about cybercrimes and related problems	Yes	48	96.0	42.32	.001
		No	2	4.0		

As far as suggestions from the cyber experts to manage cybercrimes are considered, all of the cyber experts opined that one should avoid disclosing personal information to the strangers, while the majority of cyber experts stated that the public has to be appraised about cybercrimes and related problems (92.0%), (X^2=42.320; P=.001), strict statutory cyber laws needs to be passed by the policy makers (90.0%), law enforcement authority has to outsource some private cyber experts (88.0%), web servers Running Public Sites must be Separately Protected from Internet private Networks (84.0%), conducting proper Procedure in Investigation of Cybercrimes (78.0%) (X^2=15.680; P=.001), 70.0% of the experts suggested updating Antivirus Software to Guard Against Virus Attacks, 66.0% have suggested specialists to handle tools and equipment of cyber-crime, 66.0% for updating regularly upcoming tools and technologies in cyber investigation (X^2=5.120; P=.024), 62.0% have suggested using sophisticated equipment to handle cyber-crime and 54.0% have suggested having intranet server to communicate to exchange the information inter organization during cybercrime investigation and lastly 96.0% of the experts suggested that public has to appraised about cybercrimes and related problems (X^2=42.32; P=.0001). For all these suggestions chi-square tests revealed that significant differences having more of YESresponses. However, chi-square tests revealed non-significant difference for having sophisticated equipment to handle cybercrime (X^2=2.880; P=.090), and having intranet server to communicate to exchange the information inter organization during cybercrime investigation (X^2=.320; P=.572).

DISCUSSION

Major findings

- A large Majority of the cyber experts had awareness about computer related crimes
- Most of the cyber experts had awareness regarding economic frauds.
- Majority of the cyber experts had awareness related to cybercrimes related to privacy
- Not disclosing personal information, public appraisal regarding cybercrimes, strict enforcement of law, and protection of public sites from hacking were the suggestions offered by the cyber experts to manage cybercrimes.

The present study focused on the cyber expert awareness, preventive Measures and suggestions here as data collected from respondent based on questionnaire method.

Shortage of trained cyber security men is of significant concern to India. In comparison to China, U.S. and Russia that have 125000, 91080 and 7300 trained cyber experts respectively; India has just 556 cyber consultants deployed in numerous government agencies (Pande-2017). In this research we find that the lack of cooperation so in this research result explore that government need to initiate and promote large that, there will be international organization establish and every country must part of cybercrime organization through this every country operate inter sharing their resources (equipment, man power and cyber experts), files (case file, evidences), information (case investigative methods, advance case handling methods and all other information regarding investigative purpose) and everything regarding cybercrime.

VII. References

1. Amis, D. (2001) The Net Now Has a National Court: This Month it's French, INTERNET FREEDOM NEWS, (Jan. 9, 2001)
2. Budd, T., &Mattinson, J. (2000). Stalking: finding from the 1998 British Criminal survey. London: Home office

3. Burgess, W. A. & Baker, T. 2002. "Cyberstalking," In: J. Boon and L. Sheridan (editors). Stalking and psychosexual obsession: Psychological perspectives for prevention, policing and treatment. London: Wiley, pp. 201-219.
4. Cybercrime & Security Overview: Terms, Trends, Statistics, and Takeaways. (2019, April 20). Retrieved from https://www.continuum.net/resources/mspedia/cybercrime-and-security-overview.
5. Dennis, M. A. (2019). Cybercrimes Law. Encyclopedia Britannica. Doi: Encyclopedia Britannica expert. BusinessDictionary.com. Retrieved November 19, 2019, from BusinessDictionary.com website: http://www.businessdictionary.com/definition/expert.html
6. Elizabeth G. Olson, (1997) Nations Struggle with How to Control Hate on the Web, N.Y. TIMES, (Nov. 24, 1997), available at http://www.nytimes.com/library/cyber/week/112497 racism.html.
7. Fronc, J. (2009). New York Undercover: Private Surveillance in the Progressive Era. Chicago IL:University of Chicago Press.
8. Goodman, M. D. (2001): Why the Police Don't Care About Computer Crime, Harvard Journal of Law and Technology, 10 (3), 465-494.
9. Hutton, S.,Haantz, S. (2003).Cyber stalking.Retrieved from http://www. nw3c.org
10. Jaishankar, K., & Uma Sankary. (2006). Cyber Stalking: A Global Menace in the Information Super Highway. Retrieved from http://www.erces.com /journal/articles/archives/volu me2/v03 /v02.html
11. Joshi, S. (2013). An IT superpower, India has just 556 cyber security experts. http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber security experts /article 48276 44.ece
12. Mala,G. &Ramdoss, S. (2011). "Attitude of female students towards cybercrimes: An Empirical study among university students". Indian journal of Criminology, vol 39 (1) & (2), January – July, 2011.
13. Ochieng, J. (2019). Computer Forensics – Everything you need to know. Retrieved from https://cyberexperts.com/computer-forensics/
14. Pande, J. (2017). Introduction to Cyber Security. Haldwani, Uttarakhand: Uttarakhand Open University. doi: http://www.uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf
15. Parker, D. B. (2000). Computer Crime: Criminal Justice Resource Manual (2nd ed.). Washington, D.C., USA: National Institute of Justice, U.S. Department of Justice. doi: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf
16. Saraswat,V. K. (2019). Cyber Security. Retrieved from https://niti.gov.in/sites/default /files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
17. Sissing, S. K. (2013). A criminological exploration of cyber stalking in South Africa. (Dissertation). University of South Africa
18. Dowdell, T. (2017). "Training and validating a deep convolutional neural network for computer-aided detection and classification of abnormalities on frontal chest radiographs," Investigative radiology, 52 (5), 281–287.
19. Tusikov, N. (2017).Chokepoints: Global Private Regulation on the Internet: Oakland CA: University of California Press.
20. Team, C. P. (2019). Cybercrime & Security Overview: Terms, Trends, Statistics, and Takeaways. Retrieved from https://www.continuum.net/resources/mspedia/cybercrime-and-security-overview
21. Waschke, M. (2017). Personal Cybersecurity: How to Avoid and Recover from Cybercrime (1st ed., Vol. 1). Bellingham, Washington, USA: Apress. doi: file:///C:/Users/pc/Downloads/Marvin Waschke (auth.) - Personal Cybersecurity_ How to Avoid and Recover from Cybercrime-Apress (2017).pdf