INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1229-1235

e-ISSN : 2583-1062

Impact Factor: 5.725

ROLE OF CYBER FORENSICS IN INVESTIGATION OF CYBER CRIMES

Sneha Nigam[1], **Annya Dixit**[2]

[1,2]National P.G College, India.

ABSTRACT

Digital crimes are become more prevalent as computers and internet technology advance. It is important to maintain the security of all online communication channels, including chat rooms, email accounts, and cloud storage. If not, hackers will have an easier time obtaining personal data, including credit card numbers, bank account credentials, and passwords. Cyber forensics is a field that blends information technology with legal elements to gather and analyze data from source computers, networks, and other storage devices in a way that makes it admissible in court.

This research paper will describe cyber forensics, also known as computer forensics, which is a subdivision of digital forensic science, relating to evidence detection in computers and digital storage media. Cyber forensics is the forensically sound examination of digital material with the aim of presenting, analyzing, recovering, identifying, and preserving facts and views pertaining to the digital information. Computer forensics is often associated with the investigation of cybercrimes, although it can also be applied in civil cases.

Data engineering and machine learning may improve cyber security in criminal investigations. It uses modern data engineering, machine learning, and AI to identify cyber dangers in criminal data. The study is based on four main ideas: Forensic Cyber psychology, which focuses on understanding psychological aspects of cybercriminal behaviour; Digital Forensics, involving the collection and analysis of digital evidence from cyber incidents; Predictive Modelling, which utilizes historical data and patterns to anticipate potential cyber threats; and the Cyber Behavioural Analysis Metric (CBAM) and Cyber Behavioural Score (CBS), tools designed for evaluating and scoring ASNs based on their behaviour in terms of cyber security threat risks.[1]

Keywords: Forensic Cyber psychology; Cyber forensics; Cybercrime, Data Engineering, Machine Learning, Artificial Intelligence.

1. INTRODUCTION

Cyber Forensic: A New Approach to Combat Cyber Crime

Cybercrime refers to illegal activities carried out by users of computer networks or the internet. This might entail a variety of actions, such as hacking into computers, obtaining private data, and deceiving others online. It also involves disseminating malicious malware or other applications that impair computers. Cybercrime can encompass actions such as cyber stalking and cyber bullying. [2] Cybercrime is increasing at lightning fast speed in the current era. The computers are used from basic to international level such as, in agriculture to nuclear power are run by the computers. "The modern thief is more likely to steal with a machine than with a sword. The terrorist of tomorrow may be able to do more harm with a keyboard than with a bomb." [3]

Cyber psychology is the study of how new technologies affect how people behave. It includes topics like social media, virtual reality, and artificial intelligence psychology as well as human aspects in cyber security.[4] Investigative At the intersection of psychology and cyber security, cyber psychology is a young and innovative field that focuses on the psychological elements of cybercriminal conduct, such as online victim logy, cyber deviancy, and offender motivations and actions. Understanding the psychological foundations of illicit cyber behaviours and dangers is the focus of this specialized section of the cyber behavioural sciences, which also entails developing techniques for online investigative procedures to minimize and prevent cybercrime. [5] Identification, recording, and interpretation of computer media are all part of cyber forensics, which uses the media as evidence and/or to reconstruct crime scenes4.

The process of locating, gathering, safeguarding, evaluating, and presenting computer-related evidence in a way that a court will find acceptable is known as computer forensics.[6]

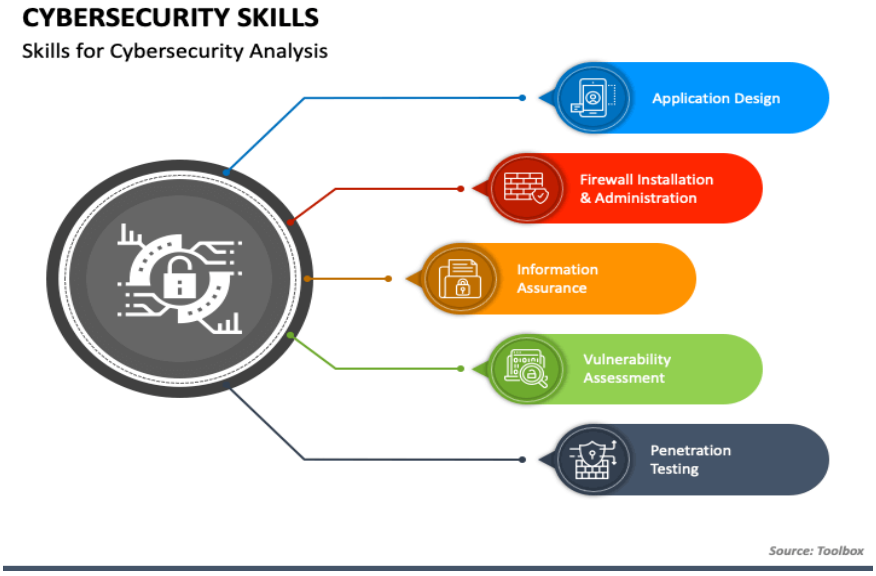


Fig1. Cyber security Roadmap [7]

1.1 What is Cybercrime?

Sussman and Heuston first proposed the term “Cyber Crime” in the year 1995. Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conducts. [8] These actions are predicated on a material offense object that has an impact on computer systems or data. These are the unlawful activities in which a digital device or information system is either a target or a tool, or both. Cybercrime is often referred to as high technology crime, information age crime, computer-related crimes, electronic crimes, e-crime, etc. Cybercrimes, to put it simply, are offenses or crimes committed using electronic communications or information systems. [9] The peculiarity of cybercrime is that there may never be direct communication between the victim and the perpetrator

People tend to believe that cybercrimes can only be done online or through cyberspace.

The twenty-first century saw the continuing discovery of new patterns in computer crime and cybercrime. New, extremely sophisticated ways of committing crimes, like "phishing"[10] and "botnet attacks,"[11] as well as the growing use of technology that makes it harder for law enforcement to handle and look into, like "voice-over-IP (VoIP) communication"[12] and "cloud computing,"[13] dominated the first ten years of the new millennium. The impact was altered in addition to the approaches. With the ability to automate attacks, the quantity of offenses escalated. In response to the escalating concerns, nations as well as regional and global organizations, have made cybercrime response a top priority.

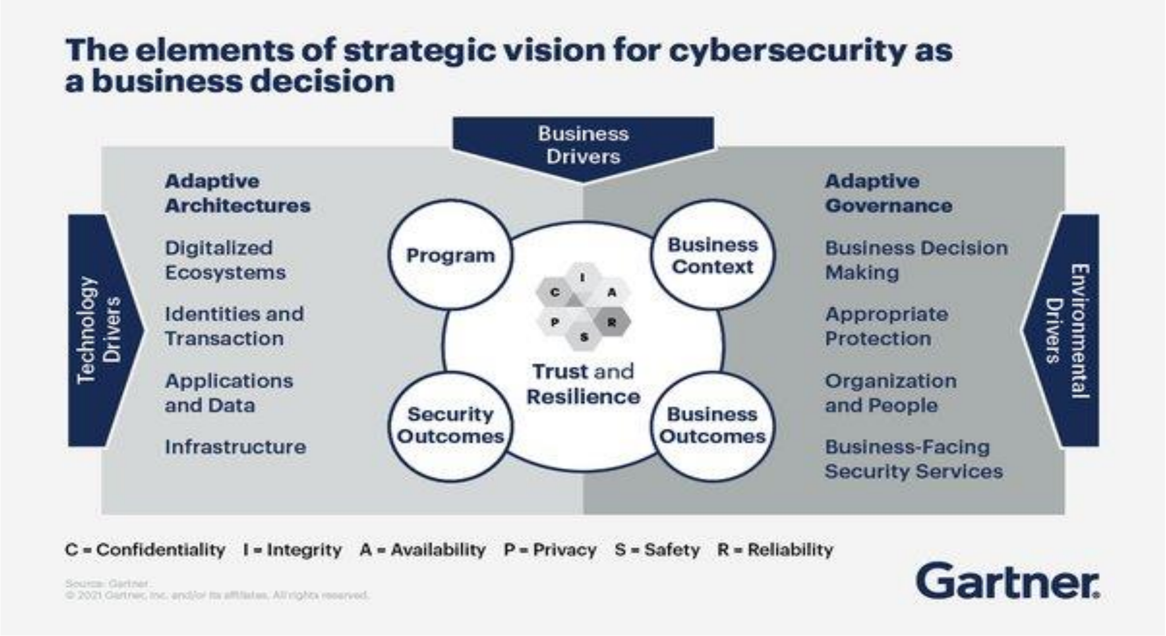
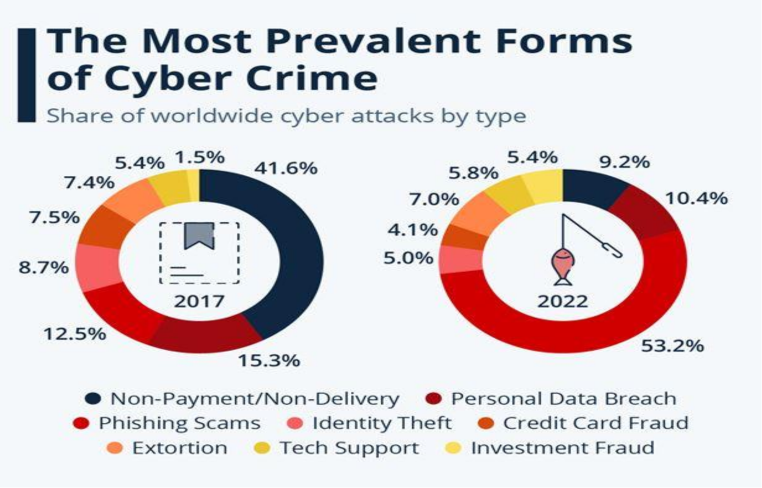


Fig2. Cyber security as a Business [14]

1.2 Kinds of Cybercrime

Some major kinds of cyber-crimes are as follows:

1.2.1 Illegal Access (Hacking, Cracking): The term "hacking" typically refers to gaining unauthorized access to a computer system, making it one of the first offenses using computers. [15] Hacking offenses encompass cracking the password of websites that require authentication and evading password protection on a computer system. However, actions associated with the term "hacking" also encompass preparatory actions such as installing hardware- and software-based key logging methods (e.g., "key loggers") that record every keystroke, thereby recording any passwords used on the computer and/or device, and using defective hardware or software to obtain a password to enter a computer system illegally. [16]

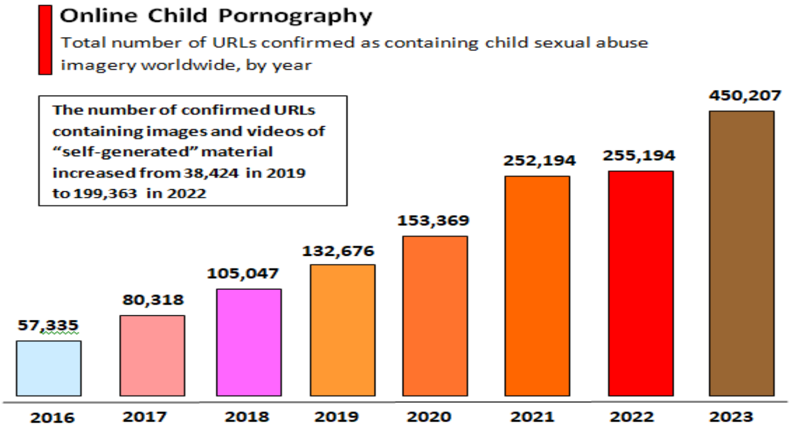

The Most Prevalent Forms of Cyber Crime

Share of worldwide cyber attacks by type

Fig3. Illegal access results these prevalent forms of Cyber Crimes [17]

1.2.2 Erotic and Pornography Material (Excluding Child Pornography): One of the earliest types of content to be commercially delivered over the Internet was sexually explicit information. This has benefits for sellers of erotic and pornographic content, including as To varying degrees, erotic and pornographic content is illegal in several nations. In an effort to safeguard children, some nations allow adults to communicate pornographic materials, only criminalizing it when minors have access to it. Research suggests that exposing children to pornographic content may have a detrimental effect on their development. "Adult verification systems" have been created to adhere to these requirements. Other nations, which do not target particular demographics (like children), make it illegal to exchange pornographic materials, even among adults. [18]

1.2.3 Child Pornography: The Internet is nowadays being highly used as a medium to sexually abuse the children. Children are a feasible and vulnerable target for cybercrime. Since computers and the internet are now necessities in every home, children have easy access to it. Pornographic content is also easily accessible on the internet. Pedophiles try to meet youngsters for sex or snap pictures of them in their underwear, sometimes even engaging in sexual poses, after luring them in with pornographic material. Sometimes, by pretending to be teenagers or kids their own age, pedophiles approach children in chat rooms, gain their trust, and gradually become more amiable. After then, pedophiles gradually begin having intercourse to get attention. [19]


Online Child Pornography

Total number of URLs confirmed as containing child sexual abuse imagery worldwide, by year

The number of confirmed URLs containing images and videos of "self-generated" material increased from 38,424 in 2019 to 199,363 in 2022

Fig4. Online Child Pornography status Yearwise [20]

1.2.4 Cyber Stalking: Generally speaking, stalking is defined as persistent acts of harassment directed at the victim, such as calling or following them, causing damage to their property, or leaving written notes or objects behind. Serious violent behaviors, such as physically harming the victim, may occur after stalking. Cyber stalking refers to the cybercriminal's persistent use of online services to harass or threaten the victim. All personal information about the victim, including name, family history, phone number, etc., is gathered by stalkers. The stalker may be a stranger to the victim or one of their acquaintances. He can readily obtain this information if he knows the victim. If he does not know the victim, he gathers information from online sources. [21]

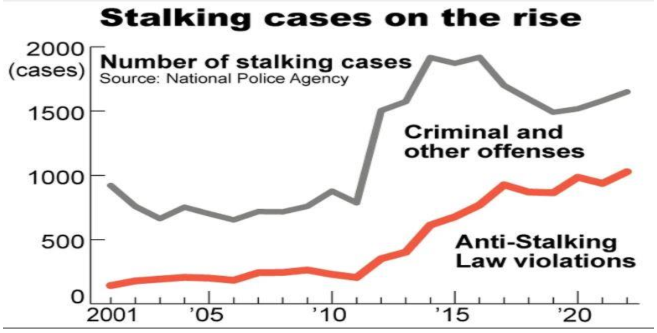
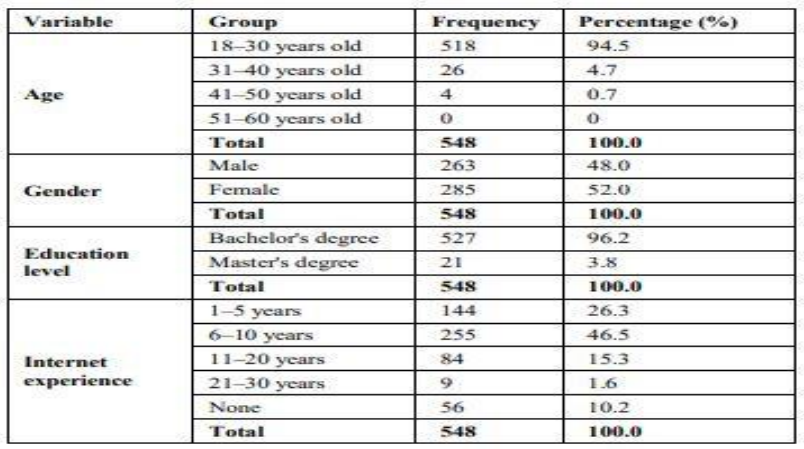


Fig5. Facts and Figures related to Cyber Stalking [22]

2. RESULTS

To achieve the objectives of this research given the nature of the data collected, five analysis tools were utilized: **the frequency distribution of variables**, **multiple response analysis**, **factor analysis for grouping different types of security**, **a reliability test**, and **descriptive analysis**. The following paragraphs provide more details for each tool. **Table I** shows the demographics of the survey participants, revealing that the majority of respondents were 18–30 years old (94.5 percent) or 31–40 years old (4.7 percent). Overall, most respondents were between the ages of 18 and 30, indicating that a younger generation was more engaged in this study. **Table I** shows that the female population (52.0%) was somewhat greater than the male population (50.0%). In terms of educational attainment, the biggest cohort (96.2 percent) had a bachelor's degree, followed by a master's degree (96.2 percent) (3.8 percent). Finally, 46.5 percent of participants had 6–10 years of experience using the Internet, followed by 26.3 percent with 1–5 years of experience, and 15.3 percent with 11–20 years of experience.[23]

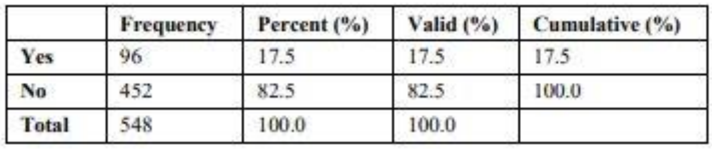
Table 1. Respondent Details [24]



Variable	Group	Frequency	Percentage (%)
Age	18–30 years old	518	94.5
	31–40 years old	26	4.7
	41–50 years old	4	0.7
	51–60 years old	0	0
	Total	**548**	**100.0**
Gender	Male	263	48.0
	Female	285	52.0
	Total	**548**	**100.0**
Education level	Bachelor's degree	527	96.2
	Master's degree	21	3.8
	Total	**548**	**100.0**
Internet experience	1–5 years	144	26.3
	6–10 years	255	46.5
	11–20 years	84	15.3
	21–30 years	9	1.6
	None	56	10.2
	Total	**548**	**100.0**

The results in **Table II** show that 82.5% of students do not know what cyber security means.

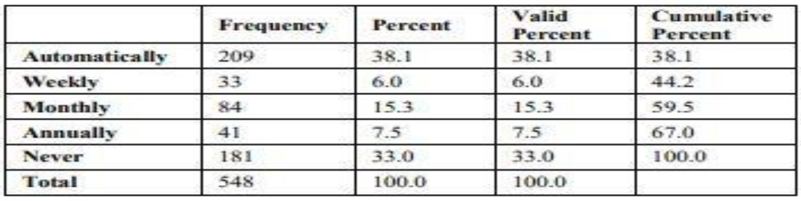
Table 2. Results For “Do You Know What the Cyber Security Means” [25]



	Frequency	Percent (%)	Valid (%)	Cumulative (%)
Yes	96	17.5	17.5	17.5
No	452	82.5	82.5	100.0
Total	548	100.0	100.0	

Considering the behavior of maintaining up-to-date protection software, the results (**Table III**) show a variation in the participants' responses. Here, 38.1% of the participants automatically update their protection software. However, 40% fail to update their software. In addition, just over 10% annually update their software.

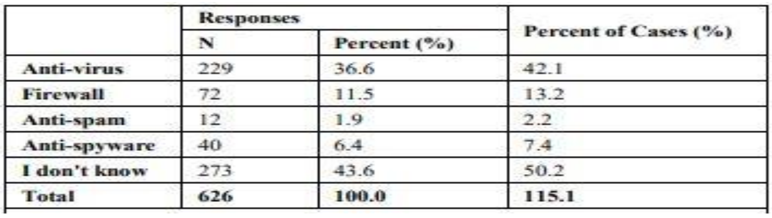
Table 3. Results for "How Often do You Update Protection Software" [26]



	Frequency	Percent	Valid Percent	Cumulative Percent
Automatically	209	38.1	38.1	38.1
Weekly	33	6.0	6.0	44.2
Monthly	84	15.3	15.3	59.5
Annually	41	7.5	7.5	67.0
Never	181	33.0	33.0	100.0
Total	548	100.0	100.0	

A multiple response analysis was utilized to answer the question, "What types of protection software do you use?" As shown in Table VII, 43.6% of respondents do not know what protection software they are using for protection. In addition, 36.6% of respondents use an anti-virus program for software protection, and 11.5% of respondents use a firewall for software protection. Only 6.4% use anti-spyware software, and 1.9% use anti-spam software

Table 4 . Results for "What Type of Protection Software do You Use" [27]



	Responses		Percent of Cases (%)
	N	Percent (%)	
Anti-virus	229	36.6	42.1
Firewall	72	11.5	13.2
Anti-spam	12	1.9	2.2
Anti-spyware	40	6.4	7.4
I don't know	273	43.6	50.2
Total	626	100.0	115.1

REVIEW

In actuality, the invention of computers brought about the rise of cybercrimes. The primary problem with cybercrime is that the perpetrator or suspect can remain anonymous within the crime scene or network. The term "Modus Operandi," which refers to the methods used by criminals to carry out their crimes, describes the variety of cybercrimes that have been documented worldwide. Thus, the requirement for an investigator becomes crucial as the degree of harm increases. "Relating to or denoting the application of scientific methods to the investigation of crime" is how the Oxford Dictionary defines "forensic." Since forensic science has been effective in resolving several conventional cases, it can also be applied to computer crimes, or cybercrimes. Forensic inquiry is carried out with a scientific methodology and legal foundations. "Analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of computer media or data which is stored or encoded for finding evidences" [28] is another definition of digital forensics. The field of forensics is vast. Proposed forensic models illustrate the intricacy of the digital forensic procedure. While most concentrate on the inquiry, another approach that focuses on processing and analyzing digital evidence is presented. This paradigm is divided into four phases: reconstruction, preservation, classification, and recognition [29]. This model also focuses on the forensic process's investigation domain.

Why Digital Forensic- The rise in cybercrimes and the vast number of unresolved cases highlight the significance of digital forensics. The proliferation of digital devices and cybercrimes has led to the establishment of digital forensic units and divisions in almost all governments. Forensic teams are now available to even corporate companies to handle internal issues (Ahmadi, Mourad, Tawil, and Awada, 2018). The consequences in the other regions are comparable to this as well. The majority of the people were being hacked without even realizing it. This resulted in several crimes, including murder trials. Finding the truth in those cases is made possible in large part by digital forensics. Thus, in today's world, digital forensics is essential. That much is now without dispute.

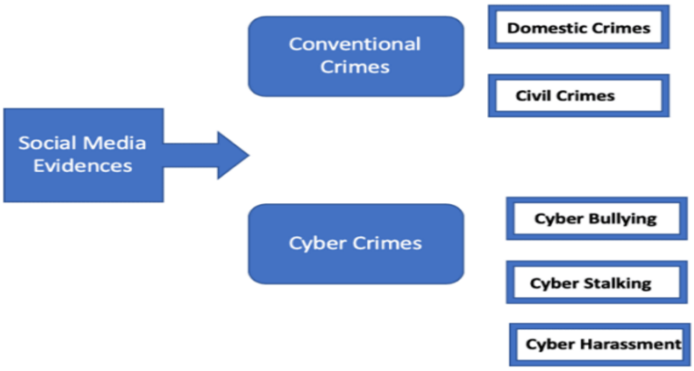


Fig6. Social media evidence in traditional and cyber crimes [30]

3. CONCLUSION

The world has become more digitally connected in the modern day, which has created an infinite amount of new opportunities and potential. It makes no difference where you are in the world. With the right abilities and a digital gadget and an internet connection, you may take use of all the limitless opportunities that the modern era has to offer. However, as is always the case, there are more and more challenges to global peace. In the past, you could close down a whole town. To accomplish it, you'll need an army of soldiers and weaponry. However, in a matter of seconds, one person may now shut down an entire nation. In recent years, the rate of cybercrimes has doubled and tripled Nowadays, the majority of nations have their own specialized forces to combat cybercrimes. Growing numbers of cybercrimes have opened up the crucial discipline of digital forensics. Digital forensic is necessary if you want to stop similar cyberattacks from occurring or if you need to identify the attacker. This is similar to how forensic services are necessary to solve crimes. However, this forensic takes place online. These days, digital forensics is a massive industry.

Because of all these factors, the work of digital forensic professionals has become essential to maintaining peace and order in contemporary society. Legal institutions need to be altered, and new laws need to be made in order for digital forensic specialists to carry out their duties and combat the masterminds of today's crime. The majority of nations have already enacted a sizable number of regulations to combat the rise in cybercrimes, but they are still insufficient.

An expert in digital forensics is also relevant in this situation. To stop these cybercrimes from occurring, they need to educate people and provide fresh solutions.

The proliferation of digital devices and the internet have presented a new set of difficulties for digital forensic specialists higher users translate into higher data generation in terms of volume and speed of data generation. Building new tools is necessary to address this. The issues that a digital forensic specialist faces include the explosion of complexity, the establishment of standards, privacy-preserving investigations, legitimacy, and the advent of anti-forensic tools.

4. REFERENCES

[1] An_Interdisciplinary_Approach_to_Enhancing_Cyber_T.pdf

[2] “Cybercrime Investigation,” DIGITPOL. [Online]. Available: https://digitpol.com/cybercrime-investigation/

[3] David Mugisha, Role and impact of digital forensics in cyber-crime investigations, 13 INT’L J. CYBER CRIMINOLOGY 43-47 (2019)

[4] Capitol Technology University. Doctor of Philosophy (PhD) in Cyberpsychology. Capitol TechnologyUniversity. Available online: https://www.captechu.edu/degrees-and-programs/doctoraldegrees/cyberpsychology-phd (accessed on [10/23/2023]).

[5] Capitol Technology University. Doctor of Philosophy (PhD) in Forensic Cyberpsychology. Capitol Technology University. Available online: https://www.captechu.edu/degrees-and programs/doctoraldegrees/ forensic-cyberpsychology-phd (accessed on [10/23/2023]).

[6] Ibrahim M. Baggily, Richard Mislan, Marcus Rogers, Mobile Phone Forensics Tool Testing: A Database Driven Approach, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2.

[7] https://cdn.sketchbubble.com/pub/media/catalog/product/optimized1/2/c/2c34cafa480e68e3a6830c40ab2a4cff93fb1e0501a7fbd24661387a00787b8b/cybersecurity-skills-mc-slide1.png

[8] https://www.tutorialspoint.com/information_security_ cyber law/introduction.html

[9] http://www.academia.edu/7781826/IMPACT_OF_SOCI AL_MEDIA_ON_SOCIETY_and_CYBER_LAW

[10] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions.

[11] Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4

[12] Simon/Slay, Voice over IP: Forensic Computing Implications, 2006

[13] Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499

[14] https://purplesec.us/wp-content/uploads/2021/10/zero-trust-cyber-security-strategy.png

[15] See Levy, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf.

[16] Musgrove, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

[17] https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.statista.com%2Fchart%2F30870%2Fshare-of-worldwide-cyber-attacks-by-type%2F&psig=AOvVaw1iMMYe-77B598dzPqYsFOT&ust=1709750633431000&source=images&cd=vfe&opi=89978449&ved=0CBMQjRxqFwoTCPju667j3YQDFQAAAAAdAAAAABAE

[18] 2006 Draft Law, Regulating the protection of Electronic Data and Information and Combating Crimes of Information (Egypt): Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty

[19] Gupta AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology. 2012 Jun; 3(2):97-101.

[20] https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.statista.com%2Fchart%2F30964%2Ftotal-number-of-urls-confirmed-as-containing-child-sexual-abuse-imagery%2F&psig=AOvVaw3C6vfq-06FZnCa7ZR2PtkD&ust=1709752429013000&source=images&cd=vfe&opi=89978449&ved=0CBMQjRxqFwoTCNDzi4fq3YQDFQAAAAAdAAAAABAE

[21] Gupta AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology. 2012 Jun; 3(2):97-101.

[22] https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.asahi.com%2Fajw%2Farticles%2F14865574&psig=AOvVaw0GeAkGVitBSalJe8eTnPla&ust=1709752649088000&source=images&cd=vfe&opi=89978449&ved=0CBMQjRxqFwoTCJi6_-_q3YQDFQAAAAAdAAAAABAE

[23] A. Bryman and E. Bell, "Business research methods (Vol. 4th)," Glasgow: Bell & Bain Ltd, 2015.

[24] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," in 2021 26th International Conference on Automation and Computing (ICAC), 2021, pp. 1-6.

[25] D. Gefen, G. M. Rose, M. Warkentin, and P. A. Pavlou, "Cultural diversity and trust in IT adoption: A comparison of potential e-voters in the USA and South Africa," Journal of Global Information Management (JGIM), vol. 13, pp. 54-78, 2005

[26] A. Bryman and E. Bell, "Business research methods (Vol. 4th)," Glasgow: Bell & Bain Ltd, 2015.

[27] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," in 2021 26th International Conference on Automation and Computing (ICAC), 2021, pp. 1-6.

[28] Harbawi, M, Varol, A. "The role of digital forensics in combating cybercrimes." Digital Forensic and Security (ISDFS), 2016 4th International Symposium on. IEEE, 2016.

[29] Casey, E.: Digital Evidence and Computer Crime, 2nd Edition, Elsevier Academic Press, 2004

[30] Upguard.com. 2021. What is Digital Forensics? | UpGuard. [online] Available at: [Accessed 12 March 2021].