International Journal of Cyber Behavior, Psychology and Learning
Volume 13 • Issue 1

Varieties and Skills of Cybercrime

Tansif Ur Rehman, University of Karachi, Pakistan*
https://orcid.org/0000-0002-5454-2150
Sajida Parveen, Karachi Institute of Economics and Technology, Pakistan
Mehmood Ahmed Usmani, University of Karachi, Pakistan
Muhammad Ahad Yar Khan, University of Karachi, Pakistan

ABSTRACT

Several thousand organized groups, as well as gangs, are dedicated to cybercrime. The potential rewards for cybercrime can be immense, even for relatively simple crimes. The rapid advancement of technology means that cybercrime is constantly evolving, making it difficult to define and predict. While some may believe cybercrime to be the work of individual lone actors, the reality is quite different. Today, there are thousands of groups dedicated to cybercrime, attracted by its potential rewards. The pace of cybercrime globally is increasing rapidly, and resolving cybercrime is often more challenging than traditional crimes. Authorities worldwide receive thousands of complaints daily, and cybercriminals are becoming increasingly innovative, organized, and sophisticated. They work hard to uncover new vulnerabilities and avoid detection while consumers remain unaware of the risks. With the rapid expansion of ICTs, cybercriminals have unique opportunities to exploit, and the full extent of the dangers is still largely unknown.

KEYWORDS

Cybercrime, Hacking, Malware, Pharming, Phishing, Skills, Spyware

INTRODUCTION

Cybercrime refers to criminal activities that are conducted using electronic devices and the internet. It encompasses a wide range of illegal activities that involve the use of technology, such as hacking, phishing, identity theft, ransomware attacks, and malware distribution (Clancy, 2023; Hamerton & Webber, 2023). The emergence of the internet and other digital technologies has created new opportunities for criminals to engage in illegal activities. Cybercrime is a growing problem worldwide, affecting individuals, businesses, and governments. It is estimated that cybercrime costs the global economy billions of dollars every year (Dhaya & Kanthavel, 2023).

Cybercriminals use a variety of tactics to carry out their illegal activities, including social engineering, malware distribution, and network intrusion (Roy & Tripathy, 2023). They often target

DOI: 10.4018/IJCBPL.324091 *Corresponding Author

individuals and organizations with weak security measures, seeking to exploit vulnerabilities in software and computer systems (Alsmadi, 2023; Lorenzo-Dus, 2023). The fight against cybercrime is an ongoing challenge for law enforcement agencies, cybersecurity experts, and individuals alike (Lehto & Neittaanmaki, 2023). It requires a multi-faceted approach that includes education, awareness, and robust security measures to protect against cyber threats.

Cybercrime is a worldwide threat to individuals, businesses, and governments, as more activities are conducted online (Allum & Gilmour, 2023; Bancroft, 2019; Hamerton & Webber, 2023). Cybercriminals use various techniques and tools to carry out their illicit activities (Johansen, 2020; Troia, 2020), such as stealing personal information (Leukfeldt & Holt, 2019), hacking into systems (Steinberg, 2019; Troia, 2020), and disrupting critical infrastructure (Clancy, 2023; Lorenzo-Dus, 2023).

To effectively combat cybercrime, it is essential to understand the different varieties and skills involved (Dhaya & Kanthavel, 2023). The varieties of cybercrime refer to the various types of cyber-attacks that can occur, including phishing, ransomware, and distributed denial of service (DDoS) attacks (Roy & Tripathy, 2023). Each type of cybercrime requires different skills and techniques, such as social engineering, malware development, and network analysis (Alsmadi, 2023; Lehto & Neittaanmaki, 2023).

Understanding the skills involved in cybercrime is crucial to developing effective countermeasures (Sikos & Haskell-Dowland, 2023). Cybercriminals often possess high technical expertise and may use sophisticated tools and methods to evade detection and carry out their activities (Kumar et al., 2023; Scanlan, 2023). Some common skills cybercriminals use include programming, encryption, and network analysis (Hubbard & Seiersen, 2023; Shires et al., 2023).

Overall, studying the varieties and skills of cybercrime is essential to developing effective prevention and response strategies and protecting individuals, businesses, and governments from the damaging effects of cyberattacks. This paper will explore the different types of cybercrime and the skills required to carry them out to improve our understanding of this complex and evolving threat.

JUSTIFICATION OF THE RESEARCH

The study of the varieties and skills of cybercrime is essential for several reasons.

Firstly, cybercrime has become increasingly prevalent in recent years, with more individuals and organizations becoming targets of cyberattacks. Understanding the different types of cybercrime and the skills required to carry them out is crucial for developing effective prevention and response strategies.

Secondly, cybercrime is constantly evolving, with new techniques and tools being developed by cybercriminals all the time. By studying the different varieties and skills of cybercrime, researchers can stay current with the latest trends and technologies and help organizations and law enforcement agencies keep pace with these developments.

Thirdly, cybercrime often has severe consequences for its victims, both in terms of financial losses and damage to reputation. By understanding the varieties and skills of cybercrime, researchers can help to identify the most effective ways to mitigate these risks and protect individuals and organizations from cyber threats.

Overall, studying the varieties and skills of cybercrime is essential for developing effective strategies to prevent, detect, and respond to cyberattacks and protect the safety and security of individuals and organizations online.

FOCUS OF THE RESEARCH

Respective work focuses on 11 varieties and skills involved in cybercrime. Cybercrime statistics and the top 10 countries facing cybercrime are also highlighted. Cybercrime is a multifaceted problem requiring a comprehensive approach as the subject matter is far more complex to comprehend.

OBJECTIVES

1. To analyze the varieties and skills involved in cybercrime.
2. To elaborate on cybercrime statistics.
3. To discuss the types of cybersecurity services.
4. To explore cybersecurity solutions.
5. To highlight the obstacles overcome by cybersecurity.

RESEARCH METHODOLOGY

This research was formed by a systematic review method. This approach involves defining research objectives and conducting an extensive literature review on the subject matter (Komba & Lwoga, 2020). The research outcomes were categorized based on their content, and the information was included in the study using appropriate headings, following the method suggested by Petticrew and Roberts (2006). The study's coherence and structure were ensured by evaluating classified information and titles, as proposed by Rahi (2017). Therefore, the research's reliability was upheld by considering the subject matter's content, as Victor (2008) recommended.

VARIETIES AND SKILLS OF CYBERCRIME

Denial of Service Attacks (DoS)

DoS attacks involve overwhelming websites or servers to make them unusable, and they are often motivated by revenge, blackmail, or activism (Hubbard & Seiersen, 2023; Scanlan, 2023). Popular commerce sites may experience crashes due to too many people trying to buy simultaneously, which works on the same principle as a DoS attack. Hacking is about infiltrating computers and carrying out DoS attacks (Kumar et al., 2023).

Hacking of Computers

One of the most well-known forms of cybercrime is hacking, which refers to unauthorized access to a network or computer system (Allum & Gilmour, 2023; Lorenzo-Dus, 2023). In the contemporary era, the internet has revolutionized hacking and made it easier to access computers virtually (Clancy, 2023; Hamerton & Webber, 2023). Hacking is often directed toward government bodies and corporations rather than individuals (Alsmadi,2023; Lehto & Neittaanmaki, 2023; Sikos & Haskell-Dowland, 2023).

There are different types of hackers, such as white, black, and grey hats (Shires et al., 2023). Hacking is a complex phenomenon involving human behavior, and hackers can be categorized based on their experience level and motivations (Hubbard & Seiersen, 2023; Scanlan, 2023). These categories include novice, CyberPunk, Internas, virus writers, petty thieves, professional criminals, old-guard hackers, political activists, and information warriors (Dhaya & Kanthavel, 2023).

Distributed Denial of Services Attacks (DDoS)

DDoS attacks are similar to DoS attacks, but they involve multiple computers communicating through peer-to-peer networks, allowing for a more concentrated effort (Alsmadi, 2023; Shires et al., 2023). Hackers use "zombies" or "bots" to take over hacked computers and carry out attacks from different computers and IP addresses, making it more challenging for the server operator to respond (Hubbard & Seiersen, 2023).

Spyware

Spyware focuses on invading privacy rather than causing harm to the computer or stealing financial information, distinguishing it from viruses, worms, and trojans (Sikos & Haskell-Dowland, 2023;

Smith, 2018). Some examples of spyware include vital loggers, pop-ups, and website monitoring, although if it enables remote access, it could also be classified as a trojan (Lehto & Neittaanmaki, 2023). Unlike viruses, worms, and trojans, which individuals often create, spyware can be developed by legitimate companies, such as Apple, Microsoft, and Google, who have been accused of using spyware in the past (Alsmadi, 2023). Companies are willing to pay large sums for information about users' behavior, making spyware and tracking cookies a lucrative business (Beaver, 2017).

Malware

The second major attack against technology involves malware, software created for malicious purposes (Dunham, 2009; Hamerton & Webber, 2023). Malware can take many forms, including viruses and self-replicating programs that spread by attaching themselves to files or storage media (Allum & Gilmour, 2023). Worms are similar to viruses in that they self-replicate, but they are also autonomous and exploit internet connectivity (Lorenzo-Dus, 2023). On the other hand, Trojans are often disguised as legitimate software and trick users into loading and executing them on their systems (Clancy, 2023). Once a Trojan is installed, it can give a hacker remote access to the computer and allow them to take over its functions, such as the webcam (Scalan, 2023).

Destroying, Disclosing, and Accessing Data

There are two methods for data deletion, access or disclosure. The first occurs when a person or group gains access to a computer system without authorization and either deletes, accesses, or reveals data that they have discovered or infects a machine with malware to delete data (Dhaya & Kanthavel, 2023). The second occurs when a person with permission to use the computer unintentionally deletes or reveals data (Roy & Tripathy, 2023; Smith, 2018).

Offense Relating to Data

Offenses involving data are connected to this subject. Urbas and Choo (2008) state that although there may be some overlap, these are largely the following four issues:

1. Deleting data
2. Improperly obtaining access to data
3. Illegally revealing data
4. Intercepting data

Phishing

Phishing is using an email account to send fraudulent emails to gain access to confidential information, while pharming is creating a fake website that looks legitimate to redirect users to a rogue site through malware provision (Lehto & Neittaanmaki, 2023; Sandwell, 2010).

Sending fraudulent emails, texts, or messages that look to be from a reliable source, like a bank, social media site, or online merchant, is a common tactic used in phishing attacks. These communications frequently include a link to a bogus website that imitates a legitimate one and ask the victim to provide sensitive data (Sikos & Haskell-Dowland, 2023).

Phishing aims to obtain personal or financial information that can be used to steal money or commit other types of fraud. To protect against phishing, individuals are advised to be cautious when clicking on links or opening attachments in unsolicited messages and to verify the legitimacy of any requests for sensitive information before providing it (Alsmadi, 2023).

Misconduct in a Public Office

Misconduct in public office is another crime that violates the public's faith in the officeholder by purposeful wrongdoing or neglect (Beaver, 2017; Hamerton & Webber, 2023). This crime is treated

severely because it may damage the public's trust in institutions of governance and law enforcement (Allum & Gilmour, 2023). The punishment for this offense may vary depending on the jurisdiction, but it often carries severe consequences, such as imprisonment or dismissal from office.

Hate and Harm

'Hate speech,' a form of expression that is inherently repugnant and targets people based on characteristics like their religion, race, color, physical appearance (including disabilities), and sexual orientation, is a term used to describe the concept of hate (Dhaya & Kanthavel, 2023; Ogilvie, 2000).

However, some websites encourage "harm" or "self-harm," which might persuade people to engage in hazardous activities. Websites about suicide, self-harm, and eating disorders may be among them (Roy & Tripathy, 2023; Yar, 2013).

Both "hate speech" and "harm" websites include non-physical contact, contain offensive and repulsive content that is unquestionably morally wrong and unhealthy (Scalan, 2023), and share other characteristics.

Pharming

It refers to a technique called 'pharming,' in which a fake website is created instead of a fake email. The user believes they are accessing the actual website but is instead redirected to a rogue site (Sikos & Haskell-Dowland, 2023). It is achieved by manipulating the computer's technical processes, such as the Domain Name System (DNS), which allows users to navigate to specific sites. Malware provision is the most common method (Lehto & Neittaanmaki, 2023; Urbas & Choo, 2008).

The main problem with pharming is that users may need to realize they are accessing an illegitimate site, even if they take precautions such as accessing their online banking website. Another pharming method is using the 'fat finger' syndrome, where scammers create a duplicate website with a misspelled URL (e.g., meirto.com instead of merito.com) (Alsmadi, 2023). If a user types in the incorrect URL and the fake site appears similar to the legitimate site, they may trust it without verifying the web address.

CYBERCRIME STATISTICS

Alvarez Technology Group (2018), Devon Milkovich (2018), and Patrick Nohe (2018) all give startling cybercrime data. Some of the statistics they used include the following:

1. According to the Clark School at the University of Maryland, a cyber attack occurs in the US alone every 39 seconds.
2. 95% of records breaches occur in only three sectors worldwide: government, retail, and technology.
3. Data from Juniper Research indicates that by 2020, the average cost of a breach of data will surpass $150 million.
4. 43% of cyberattacks target small firms, while 64% of organizations have been subject to web-based attacks. Furthermore, 59% had malware and botnets, 62% had phishing and social engineering assaults, and 51% had denial of service attacks.
5. The DDoS attack size increased by 500%, reaching more than 26Gbps, as reported by Nexusguard's quarterly report, according to the Q2 2018 Threat Report.
6. Since 2013, an average of 3,809,448 records have been stolen daily from breaches.
7. Unfilled cybersecurity jobs worldwide are expected to reach 3.5 million by 2021.
8. Global cybersecurity spending is expected to reach approximately $6 trillion by 2021.
9. By 2020, the number of connected devices is expected to reach roughly 200 billion.
10. Human error accounts for 95% of cybersecurity breaches.
11. Cybercrime damages increased to over 1 trillion dollars in 2018.

12. 38% of large international organizations assert that they are ready to respond to an advanced cyber-attack.

TOP 10 COUNTRIES FACING CYBERCRIME

1. **United States:** The US is a significant target for cybercriminals due to its large economy, valuable data, and numerous high-profile organizations. The country has experienced large-scale cyber attacks on government agencies, corporations, and individuals.
2. **China:** China is both a victim and a perpetrator of cybercrime. The country is known for state-sponsored hacking, industrial espionage, and stealing intellectual property from foreign businesses.
3. **India:** India is one of the most significant targets for cybercrime due to its large population and growing economy. The country has seen increased cyber attacks on financial institutions, e-commerce websites, and government agencies.
4. **Russia:** Russia is known for state-sponsored cyber espionage and hacking, targeting foreign governments, businesses, and individuals. The country is also home to some of the most notorious cybercriminal groups, including APT28 and Cozy Bear.
5. **Brazil:** Brazil is a popular target for cybercriminals due to its large population and growing economy. The country has experienced numerous cyber attacks on financial institutions, e-commerce websites, and government agencies.
6. **United Kingdom:** The UK is a significant target for cybercrime due to its valuable data, high-profile organizations, and critical infrastructure. The country has experienced large-scale cyber attacks on government agencies, corporations, and individuals.
7. **Germany:** Germany is a significant target for cybercrime due to its large economy, valuable data, and numerous high-profile organizations. The country has experienced large-scale cyber attacks on government agencies, corporations, and individuals.
8. **Japan:** Japan is a significant target for cybercrime due to its advanced technology sector, valuable data, and numerous high-profile organizations. The country has experienced large-scale cyber attacks on government agencies, corporations, and individuals.
9. **South Korea:** South Korea is a significant target for cybercrime due to its advanced technology sector, valuable data, and numerous high-profile organizations. The country has experienced large-scale cyber attacks on government agencies, corporations, and individuals.
10. **Australia:** Australia is a significant target for cybercrime due to its valuable data, high-profile organizations, and critical infrastructure. The country has experienced large-scale cyber attacks on government agencies, corporations, and individuals.

TYPES OF CYBERSECURITY SERVICES

ReachOut Australia (2021) and Consolidated Technologies, Inc. (2018) both cite the importance of cybersecurity systems in defending against frequent cyberattacks. They are the procedures used to make sure that electronic records are secure and to protect against harmful use. The coordinating procedures utilized to attain this security and defend against common cyberthreats, on the other hand, are cybersecurity services.

The following are some instances of typical threats that cybersecurity companies commonly target, according to Forcepoint (2021):

1. **Malware:** It is a computer virus installed to compromise the availability, integrity, or confidentiality of records. One of the most serious outside dangers to company networks today, it frequently goes unnoticed.
2. **Ransomware:** This type of malware encrypts a computer device and then demands a ransom in exchange for decryption and access.
3. **Phishing:** By pretending to be an authorized business representative, cybercriminals employ phishing to collect data. They often send an email with an account warning and a link to a fake website that requests passwords or other personal information.
4. **DDoS:** These attacks cause website response times to be delayed by flooding a network with traffic requests. This technique can be used as a diversionary tactic when committing other crimes.

CYBERSECURITY SOLUTIONS

Cybersecurity employs various network security tools to protect data, networks, and applications from these attacks. The following are only a couple of the many cybersecurity options, according to IT Governance (2021):

1. **Encryption:** When data is encrypted, hackers cannot read it even though it has been hacked. Encryption is essential if a person moves data from one computer to another because data may be corrupted during the transition.
2. **Defense from data loss:** Data loss management processes make sure that the data is available because it is necessary for daily operations.
3. **Risk and compliance management:** For many businesses to adhere to governmental requirements or industry norms, cybersecurity services are necessary. A dedicated approach that meets these conditions is risk and security evaluation.
4. **Firewalls:** It helps protect against malicious attacks and untrusted networks; firewalls control outgoing and incoming network traffic flow.
5. **Web filtering:** It stops workers from unintentionally exploiting unauthorized resources on the corporate network and erasing data.
6. **Anti-malware and anti-virus software:** These two types of cybersecurity tools are among the most widely used in computer networks.
7. It protects files by scanning the device for threats and preventing viruses from accessing them.

OBSTACLES OVERCOME BY CYBERSECURITY

Juliana De Groot's (2020) research highlights that companies face multiple security risks daily, like:

1. **External threats:** Hackers can bypass traditional firewalls to steal data, but cybersecurity service providers can ensure that firewalls, anti-virus software, and other security tools are regularly updated and ready to protect networks.
2. **Unsecured cloud storage:** With the rise in cloud services, security breaches in cloud storage have become more common. Nearly 70% of breaches in 2017 were attributed to improperly set up cloud servers. Network surveillance companies guarantee that cloud networks are safe enough to guard against data intrusions.
3. **Employee negligence:** Data breaches are commonly caused by employee errors. To minimize the risk of such mistakes, cybersecurity strategies such as online filtering can prevent staff from accessing potentially harmful websites.

4. **Inadequate IT processes:** To stay up with evolving risks and the best practices for protection, small firms may require more resources or experience. Because they need more resources to hire a specialized IT team, many businesses jeopardize their infrastructure. However, outsourcing or using cloud-based cybersecurity solutions can be cost-effective in minimizing revenue loss in a security breach.
5. **Insider trading:** For companies of all sizes, internal data manipulation is intimidating. Security technologies ensure that only authorized personnel can access data, safeguarding it from unauthorized manipulation.
6. **Third-party app security:** Many third-party applications lack adequate security functionality and can pose a threat to a business's interests. Cybersecurity software identifies potentially harmful malware and adds security features to applications lacking.

SOLUTIONS AND RECOMMENDATIONS

1. It is crucial to provide accessible avenues for cybercrime victims to report e-offenses.
2. To avoid sharing personal information on social media, utilize privacy settings.
3. Refrain from opening links in emails received from unknown sources.
4. After logging out of an account, clear the browsing history.
5. The legal departments must have access to the latest investigation technologies.
6. Awareness should be spread by engaging the community and CBOs, NGOs, INGOs, and cyber vigilantism.
7. Terminate online sessions altogether.
8. Use a personal computer, and when using a public computer, avoid online transactions if possible.
9. Use security programs and protect passwords.
10. Update software package regularly.
11. The encryption of files and regular backups of essential data should be ensured.
12. We should limit the administrative powers of all accounts in case of a shared device.
13. Unknown Wi-Fi networks and Bluetooth connections should be avoided.
14. We should only visit trustworthy websites.
15. E-transactions must be entered via authentic websites, and data should not be saved on online servers.

FUTURE RESEARCH DIRECTIONS

1. Computer-assisted crimes
2. Criminal psychology
3. Cyberterrorism
4. Cybersecurity
5. Ethical hacking
6. Hacktivism
7. Incident response planning
8. Malware
9. Perceived and actual risks in the cyber world
10. Vulnerabilities in computing

CONCLUSION

As individuals rely more on technology, they become more vulnerable to cybercrime, which can lead to new issues. As cybercrime is a multifaceted problem, a multidimensional approach must understand the subject matter of the issue. It puts nations at risk of cybercrime due to inadequate technology, limited cooperation with international law enforcement agencies, and insufficient legislation and funding. Therefore, addressing these issues with international legal solutions and implementing comprehensive cyber laws is crucial. The dire need for ICT applications in privatized and government sectors is today's prerequisite because these applications have enhanced operational effectiveness. On the contrary, the intemperate usage of computer networks and their applications has amplified issues encompassing the phenomenon of cybercrime. Although many countries have established cyber laws, their enforcement is often weak, highlighting the urgent need for more robust measures.

LIMITATIONS OF THE STUDY

As technology continues to evolve at a rapid pace, new forms of cybercrime are constantly emerging. For example, the rise of cryptocurrencies has led to an increase in cryptojacking and other cryptocurrency-related crimes. However, studies may not always keep up with these new developments and may not cover all the latest cybercrime trends.

Another limitation is the difficulty in accurately measuring the extent of cybercrime. Many victims may not report cybercrime incidents to law enforcement agencies or other authorities. Additionally, some cybercriminals are skilled at covering their tracks, making it difficult to identify and prosecute them. As a result, the true scale and impact of cybercrime may be underestimated.

Another challenge is the lack of standardization in the definitions and classifications of cybercrime. Different countries and organizations may have varying definitions of what constitutes cybercrime, and this can make it difficult to compare and analyze data across different regions and jurisdictions.

Finally, some studies may focus only on specific types of cybercrime, such as phishing or malware attacks, while ignoring other forms of cybercrime, such as cyberbullying or online harassment. This can lead to a skewed understanding of the overall impact and nature of cybercrime.

REFERENCES

Alazab, M., & Broadhurst, R. (2014). *Spam and criminal activity. Trends and issues*. Australian Institute of Criminology.

Allum, F., & Gilmour, S. (Eds.). (2023). *The Routledge Handbook of transnational organized crime*. Routledge.

Alsmadi, I. (2023). *The NICE cyber security framework: Cyber security intelligence and analytics*. Springer International Publishing. doi:10.1007/978-3-031-21651-0

Alvarez Technology Group. (2018). *2018 top cybercrime facts and why you should care.* Alvarez. https://www.alvareztg.com/2018-cybercrime-statistics-reference-material/

Bancroft, A. (2019). *The darknet and smarter crime: Methods for Investigating criminal entrepreneurs and the illicit drug economy (Palgrave studies in cybercrime and cybersecurity)*. Palgrave Macmillan.

Bandura, A. (2007). Impeding ecological sustainability through selective moral disengagement. *International Journal of Innovation and Sustainable Development*, *2*, 8–35.

Bandura, A. (2007). Reflections on an agentic theory of human behavior. *Tidsskrift for Norsk Norsk Psykologforening.*, *10*, 995–1004.

Beaver, K. (2017). *Hacking for dummies* (5th ed.). For Dummies.

Brenner, S. W. (2014). *Cyberthreats and the decline of the nation-state*. Routledge.

Broadhurst, R., & Choo, K. K. R. (2011). *Cybercrime and online safety in cyberspace*. Routledge Handbook of Criminology.

Clancy, T. K. (2023). *Cyber crime and digital evidence: Materials and cases*. Carolina Academic Press.

Cloward, R., & Ohlin, L. (2013). *Delinquency and opportunity: A study of delinquent gangs*. Routledge.

Consolidated Technologies, Inc. (2018, October 26). What is a cybersecurity solution? https://consoltech.com/blog/cybersecurity-saas/

Cornish, D. B., & Clarke, R. V. (Eds.). (2014). *The reasoning criminal: Rational choice perspectives on offending*. Transaction Publishers.

De Groot, J. (2020, October 05). What is cybersecurity? Definition, best practices & more. *Digital Guardian.* https://digitalguardian.com/blog/what-cyber-security

Dhaya, R., & Kanthavel, R. (Eds.). (2023). *Internet of behaviours (IoB)*. CRC Press. doi:10.1201/9781003305170

Downes, D. M., & Rock, P. (2011). *Understanding deviance: A guide to the sociology of crime and rule-breaking*. Oxford University Press.

Dunham, K. (2009). *Mobile malware attacks and defense*. Syngress Publishing.

Ekblom, P. (2014). Designing products against crime. In *Encyclopedia of Criminology and Criminal Justice* (pp. 948–957). Springer.

Forcepoint. (2021). *What is cybersecurity? Cybersecurity defined, explained, and explored.* Forcepoint. https://www.forcepoint.com/cyber-edu/cybersecurity

Glenny, M. (2012). *Dark-market: How hackers became the new media*. Vintage Books.

Hagan, F. E. (2012). Introduction to criminology: Theories, methods, and criminal behavior. *Sage (Atlanta, Ga.)*.

Hamerton, C., & Webber, C. (2023). *Precarious futures: Crime, technology, and the web*. Springer International Publishing.

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk*. Wiley. doi:10.1002/9781119892335

Hutchings, A. (2013). *Theory and crime: Does it compute?* Griffith University.

Hutchings, A. (2013). *Theory and crime: Does it compute?* Griffith University.

Isajiw, W. W. (2013). *Causation and functionalism in sociology*. Routledge.

IT Governance. (2021). *What is cybersecurity? Definition and best practices.* IT Governance. https://www.itgovernance.co.uk/what-is-cybersecurity

Johansen, G. (2020). *Digital forensics and incident response: Incident response techniques and procedures to respond to modern cyber threats*. Packt Publishing.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757–780.

Komba, M. M., & Lwoga, E. T. (2020). *Systematic review as a research method in library and information science.* IGI Global. .10.4018/978-1-7998-1471-9.ch005

Kumar, A., Kudrati, A., & Kumar, S. (2023). *Managing risks in digital transformation: Navigate the modern landscape of digital threats with the help of real-world examples and use cases*. Packt Publishing, Limited.

Lehto, M., & Neittaanmaki, P. (2023). *Cyber security: Critical infrastructure protection*. Springer International Publishing.

Leukfeldt, R., & Holt, T. J. (2019). *The human factor of cybercrime*. Routledge. doi:10.4324/9780429460593

Lorenzo-Dus, N. (2023). *Digital grooming: Discourses of manipulation and cyber-crime*. Oxford University Press.

Maurushat, A. (2013). Discovery and dissemination of discovering security vulnerabilities. In *Disclosure of Security Vulnerabilities* (pp. 21–33). Springer.

McGuire, M. (2012). *Organized crime in the digital age*. John Grieve Centre for Policing and Security.

Milkovich, D. (2018, December 3). *13 alarming cybersecurity facts and stats.* https://www.cybintsolutions.com/cyber-security-facts-stats/

Moore, R. (2005). *Cybercrime: Investigating high technology computer crime*. Matthew Bender & Company.

Nohe, P. (2018, September 27). *Re-hashed: 2018 cybercrime statistics: A closer look at the web of profit.* The SSL Store. https://www.thesslstore.com/blog/2018-cybercrime-statistics/

Ogilvie, E. (2000). Cyberstalking. *Trends and Issues in Crime and Criminal Justice,* 166.

Pawson, R., Greenhalgh, T., Harvey, G., & Walshe, K. (2005). Realist review - A new method of systematic review designed for complex policy interventions. *Journal of Health Services Research & Policy*, *10*(1), 21–34. doi:10.1258/1355819054308530 PMID:16053581

Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide*. Blackwell Publishing., doi:10.1002/9780470754887

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues, and instruments development. *International Journal of Economics & Management Sciences*, *6*(2). doi:10.4172/2162-6359.1000403

ReachOut Australia. (2021). *Disclosing personal information.* ReachOut Australia. https://schools.au.reachout.com/articles/disclosing-personal-information

Roy, P. K., & Tripathy, A. K. (Eds.). (2023). *Cybercrime in social media: Theory and solutions*. CRC Press.

Sandwell, B. (2010). On the globalization of crime: The internet and new criminality. In Y. Jewkes & M. Yar, Handbook of internet crime (pp. 38-66). Willan Publishing.

Scanlan, D. (2023). *The hacker.* Head of Zeus.

Shires, J., Smeets, M., & Chesney, R. (Eds.). (2023). *Cyberspace and instability*. Edinburgh University Press.

Sikos, L. F., & Haskell-Dowland, P. (Eds.). (2023). *Cybersecurity teaching in higher education*. Springer International Publishing. doi:10.1007/978-3-031-24216-8

Smith. (2018). *Hacking pacemakers, insulin pumps, and patient's vital signs in real-time.* CSO Online. https://www.csoonline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-an d-patients-vital-signs-in-real-time.html

Steinberg, J. (2019). *Cybersecurity for dummies (For dummies computer/tech)*. John Wiley & Sons.

Sternberg, J. (2012). *Misbehavior in cyber places: The regulation of online conduct in virtual communities on the internet*. Rowman & Littlefield.

Troia, V. (2020). *Hunting cybercriminals: A hacker's guide to online Intelligence gathering tools and techniques*. Wiley. doi:10.1002/9781119541004

Urbas, G., & Choo, K. R. (2008). *Resource materials on technology-enabled crime*. Australian Institute of Criminology.

Victor, L. (2008). Systematic reviewing in the social sciences: Outcomes and explanation. *Enquire*, *1*(1), 32–46.

Webber, C. (2014). *Hackers and cybercrime. Shades of deviance: A primer on crime, deviance, and social harm*. Routledge.

Yar, M. (2013). *Cybercrime and society*. Sage Publishing Ltd.

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers*, 1–13.

KEY TERMS

Cybercrime: The use of a computer to commit a crime.
Denial of Service attack: It is an attack to shut down a machine or network, making it inaccessible to its intended users.
Distributed Denial of Service attack: It is a malicious attempt to disrupt regular traffic to make it impossible for a service to be delivered.
Malware: Any file or program that is harmful to a computer user as well as sensitive information.
Pharming: It is a cyber-attack that intends to redirect a website's traffic to a fake site.
Phishing: It is a fraudulent attempt to obtain sensitive information.
Spyware: It is unwanted software that infiltrates any computing device, stealing data.

Tansif ur Rehman has a Ph.D. in European Studies. He has several publications and has over 20 years of teaching as well as 14 years of research experience.