Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 1 – 10 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

THE CRIMINALIZATION OF THE INTERNET AND CYBERCRIME IN GENERAL: A COMPREHENSIVE STUDY

Ayepeku O. Felix[1], Omosola J. Olabode[1], James K. Ayeni[2]

[1]Dept. of Mathematical and Computing Science, Thomas Adewumi University Oko-Irese
[2]Dept. Of Computer Science, Kwara State Polytechnic, Ilorin

ABSTRACT: The internet's rapid growth has revolutionized connectivity and convenience, but it has also led to a rise in cybercrime. This study explores the complexities, implications, and challenges of cybercrime, analyzing its evolution, forms, and socio-economic impact. It examines the legal framework surrounding cybercrime, including international agreements, national legislation, and emerging jurisprudence. The study also highlights the need for international cooperation and cyber forensics advancements. It also examines the ongoing cybercrime arms race between cybersecurity professionals and cybercriminals, emphasizing the importance of proactive defense strategies, threat intelligence, and incident response protocols. The study underscores the urgency of addressing the criminalization of the internet and cybercrime, emphasizing the role of public awareness, collaboration, and innovative technological solutions in mitigating threats and ensuring a secure digital future.

KEYWORDS: criminalization, internet, cybercrime, comprehensive, study

1. INTRODUCTION

The internet's widespread proliferation over the last two decades has undeniably transformed how we communicate, work, and go about our everyday lives. This digital metamorphosis has ushered in an era of unprecedented connectivity, convenience, and innovation. However, as the internet continues to evolve, so too does the shadowy underworld of cybercrime, raising profound concerns about the criminalization of the digital realm.

With the rise of the internet, cybercrime has emerged as a global epidemic, transcending geographical borders and infiltrating nearly every facet of our interconnected world. Cybercriminals exploit the boundless opportunities offered by the digital landscape, perpetrating a diverse range of crimes with far-reaching consequences. From financial frauds and data breaches to disruptive ransomware attacks and state-sponsored cyberespionage, the spectrum of cyber threats is both broad and ever-evolving.

As we embark on this comprehensive study, it is imperative to recognize the gravity of the situation. Cybersecurity Ventures estimates that by 2023, cybercrime will have cost the global economy $8 trillion. Cybercrime would have a larger economy than China and the United States combined, ranking third in the globe, the gross domestic product of many nations (yeoandyeo, 2023). Moreover, the implications extend beyond financial losses, encompassing the erosion of privacy, the disruption of critical infrastructure, and even the compromise of national security Rybicki, P. (2023).

To combat the criminalization of the internet and cybercrime effectively, it is paramount to understand its multifaceted nature. This study aims to dissect the intricacies of cybercrime, ranging from its historical roots to the modern-day landscape. We will explore the various forms of cybercrime, including hacking, malware, social engineering, and the ever-elusive dark web marketplaces. In doing so, we will delve into the motivations driving cybercriminals, the methodologies they employ, and the profound socio-economic impact these activities have on individuals, organizations, and society at large.

In parallel, this study will scrutinize the evolving legal framework governing cybercrime, spanning international agreements, national legislation, and emerging jurisprudence. It will also examine the persistent challenges associated with the attribution of cybercrimes to specific actors and jurisdictions, emphasizing the pressing need for international cooperation and advancements in cyber forensics (Palmieri, M., Shortland, N., & McGarry, P. 2021)

Furthermore, we will investigate the perpetual cat-and-mouse game between cybercriminals and cybersecurity professionals. By analyzing the techniques employed on both sides of this digital divide, we will underscore the importance of proactive defense strategies, threat intelligence sharing, and the development of robust incident response protocols.

As we navigate this comprehensive study, it is our fervent hope that the insights gained will contribute to a broader understanding of the criminalization of the internet and cybercrime. Together, we can strive to safeguard the digital realm, ensuring that the boundless opportunities presented by the internet are not eclipsed by the shadow of cybercriminal activities.

1.1 MOTIVATION:

The criminalization of the internet and cybercrime in general is motivated by the need to understand, address, and mitigate the growing challenges posed by cybercriminal activities in our interconnected world. It serves as a means to inform, educate, and drive actions that enhance cybersecurity and promote responsible digital behavior.

1.2 HISTORICAL ROOTS OF CYBERCRIME

The origins of cybercrime can be traced back to the computing in its early days. As early as the 1960s and the 1970s, as computer technology began to emerge, the emergence of a new crime type started to take shape. Theft of private data and unlawful access to computer systems were early examples. Hacking as a concept, initially used to describe the activities of individuals exploring computer systems out of curiosity, began to evolve into a criminal enterprise.

One notable historical event was the first computer virus created in 1982 by Richard Skrenta, known as the Elk Cloner, which infected Apple II computers. This marked the beginning of malware as a tool for cybercriminals. As technology advanced, so did the sophistication and a wide range of cybercrimes, such as financial fraud and the dissemination of dangerous software.

1.3 TYPES AND EVOLUTION OF CYBERCRIME

Cybercrime encompasses a vast array of criminal activities, with hackers and cybercriminals continuously adapting to technological advancements. Some prominent categories of cybercrime include:

Hacking and Unauthorized Access: Unlawful entry into computer systems or networks with the intention of doing harm. Hacking has evolved from simple password guessing to more advanced techniques such as SQL injection, zero-day exploits , Brute forcing, Packet sniffing, Privilege escalation and _Exploiting software vulnerabilities (Naidoo & Jacobs, 2023)

Malware Attacks: Malicious software, including viruses, worms, Trojans, and ransomware, is used to compromise systems and steal data. Modern malware is highly sophisticated, capable of evading detection and encryption (Naidoo, R., & Jacobs, C. (2023).

Social engineering and Phishing: Cybercriminals use deceitful methods to trick people into disclosing critical information. Phishing attacks often target email recipients with fraudulent messages, while social engineering exploits human psychology (Sekhar Bhusal, 2021)

Financial Cybercrimes: In the digital era, criminal activity including credit card scams, theft of personal information, and internet fraud has exploded, costing individuals and organizations billions of dollars (Mohsin, K. 2021).

Ransomware: An increasing danger, encrypts information belonging to a victim and demands payment to unlock it Ransomware attacks have disrupted critical infrastructure and led to significant financial losses

State-Sponsored Cyber Espionage: Nation-states engage in cyber-espionage for political, economic, and military purposes. Notable examples include the Stuxnet worm and the alleged Russian interference in foreign elections (Gulyás, O., & Kiss, G. 2023).

2.0 THE MODERN CYBERCRIME LANDSCAPE

The modern cybercrime landscape is characterized by its scale, complexity, and constant evolution. The advent of the dark web has provided cybercriminals with a clandestine platform for conducting illicit activities, including the sale of stolen data, hacking tools, and cybercrime-as-a-service offerings (Palmieri, M., Shortland, N., & McGarry, P. 2021)

Cybercrime is not limited to individuals; well-organized cybercriminal groups operate globally. These groups often employ sophisticated tactics, tools, and even conduct research and development to stay ahead of cybersecurity defenses (Lusher, 2018).

Additionally, as the Internet of Things (IoT) expands, new exploitative opportunities are opened up by hackers. Vulnerabilities in IoT devices can be targeted to gain unauthorized access or launching extensive distributed denial-of-service (DDoS) assaults (Zarpelão, Miani, & Kawakani, 2017).

2.1 HACKING

Hacking, broadly defined as unauthorized access to computer systems or networks with malicious intent, is one of the oldest and most pervasive forms of cybercrime (Naidoo & Jacobs, 2023). It includes:

Ethical Hacking: Ethical hackers, often referred to as "white hat" hackers, legally and ethically assess system vulnerabilities to improve security.

Black Hat Hacking: Malicious hackers, or "black hat" hackers, break into systems for personal gain, damage, or theft.

Gray Hat Hacking: A gray area where hackers may breach systems without authorization but not necessarily for malicious purposes, sometimes seeking rewards or recognition

2.2 MALWARE ATTACKS

Malware, or malicious software, is designed to compromise systems or steal data (Naidoo, R., & Jacobs, C. (2023). It includes:

Viruses: Self-replicating programs that attach to other files and require user interaction to spread

Worms: Self-replicating programs that spread independently and exploit vulnerabilities in networked systems

Trojans: Malware disguised as legitimate software, often used for data theft or providing unauthorized access

Ransomware: Data-encrypting malware that severely disrupts operations by encrypting victims' data and demanding a fee to retrieve it

2.3 SOCIAL ENGINEERING

Social engineering exploits human psychology to manipulate individuals into revealing sensitive information or performing actions they wouldn't otherwise (Sekhar Bhusal, 2021). Techniques include:

Phishing: Cybercriminals use fraudulent emails or websites that mimic trusted entities to trick victims into revealing personal information.

Pretexting: Attackers create fabricated scenarios or personas to obtain sensitive information or access.

Baiting: Malicious software or media is offered to entice users to download it, compromising their devices

2.4 DARK WEB MARKETPLACES

The dark web provides anonymity through tools like Tor (The Onion Router), making it difficult to trace users or monitor activities. This anonymity enables cybercriminals to operate with relative impunity, though law enforcement agencies have made efforts to combat illegal activities on the dark web (Palmieri, M., Shortland, N., & McGarry, P. 2021)

The dark web, special browsers are needed to access this hidden part of the internet, hosts various illegal activities, including cybercrime marketplaces This includes:

Stolen Data Markets: Platforms where hackers sell stolen credentials, credit card information, and personal data.

Malware and Exploit Markets: Cybercriminals offer malware, zero-day exploits, and hacking tools for sale

Drugs and Weapons Markets: Beyond cybercrime, the dark web hosts illegal marketplaces for drugs, firearms, and other contraband

3.0 MOTIVATIONS DRIVING CYBERCRIMINALS

Cybercriminals are driven by a range of motivations, including financial gain, ideology, and personal vendettas. They employ various methodologies, from phishing to malware, to achieve their objectives. The socio-economic impact of cybercrime is extensive, affecting individuals, organizations, and society through financial losses, data breaches, reputation damage, and even national security risks.

Cybercriminals are motivated by a range of factors, often intertwined. Understanding these motivations is crucial to addressing cybercrime (Palmieri, M., Shortland, N., & McGarry, P. 2021)

Financial Gain: A primary motivation for cybercriminals is financial profit. This includes activities like stealing credit card information, conducting ransomware attacks, and selling stolen data on the dark web (Mohsin, K. (2021).

Hacktivism: Some cybercriminals have political or ideological motivations, engaging in hacktivism to promote a particular cause or express dissent (Nershi & Grossman, 2023)

Espionage: Nation-states engage in cyber espionage to gain a competitive advantage, steal intellectual property, or gather intelligence

Personal Vendettas: Cybercriminals may have personal grudges or vendettas against individuals or organizations, leading to targeted attacks.

Thrill-Seeking: For some, cybercrime provides a sense of excitement and achievement, akin to a high-risk game

4.0 METHODOLOGIES EMPLOYED BY CYBERCRIMINALS

Cybercriminals employ a wide range of methodologies and techniques to achieve their objectives (Naidoo, R., & Jacobs, C. (2023).

Phishing: Sending deceptive emails or messages to trick recipients into revealing sensitive information or downloading malware.

Malware: Developing and distributing malicious software like viruses, Trojans, and ransomware to compromise systems.

Exploiting Vulnerabilities: Identifying and exploiting software or hardware vulnerabilities, such as zero-day exploits.

Social Engineering: Manipulating individuals into revealing information or performing actions against their best interests through deception and persuasion.
Denial-of-Service (DDoS) Attacks: Overloading a target's server or network with traffic to disrupt services or operations.
Insider Threats: Exploiting the trust of insiders, such as employees or contractors, to gain unauthorized access or steal data.

4.1 SOCIO-ECONOMIC IMPACT OF CYBERCRIME

The socio-economic impact of cybercrime is far-reaching and profound, affecting individuals, organizations, and society as a whole (Rybicki, P. 2023).

Financial Losses: Cybercrime costs individuals and organizations billions of dollars annually in financial losses, including theft, fraud, and the expenses associated with data breaches.
Data Breaches: Data breaches compromise the personal and financial information of individuals, leading to identity theft and financial fraud.
Reputation Damage: Organizations often suffer reputational damage following a cyberattack, which can erode customer trust and shareholder confidence.
Operational Disruption: Cyberattacks can disrupt critical infrastructure, leading to downtime and lost productivity.
National Security Risks: State-sponsored cyber espionage and cyberattacks on critical infrastructure pose significant national security risks (Gulyás, O., & Kiss, G. 2023).
Economic Impact: The overall economic impact of cybercrime includes costs associated with cybersecurity measures, legal proceedings, and insurance premiums.
Psychological and emotional effects: Individuals who fall victim to cybercrimes, such as online harassment or cyberbullying, may suffer emotional and psychological distress.

4.2 INTERNATIONAL AGREEMENTS AND CONVENTIONS

The legal framework governing cybercrime is evolving rapidly to address the complex and global nature of cyber threats. International agreements, national legislations, and emerging jurisprudence collectively form a multifaceted approach to combating cybercrime and protecting individuals, organizations, and society at large. International agreements and conventions play a significant role in shaping the legal framework for addressing cybercrime on a global scale Arnell, P., & Faturoti, B. (2022). Key agreements and organizations include:

Budapest Convention: The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, is a milestone international treaty that harmonizes cybercrime legislation and facilitates international cooperation (Council of Europe, 2001).
United Nations (UN) Resolutions: Various UN resolutions, such as Resolution 55/63 and Resolution 58/199, call for international cooperation in combating cybercrime and protecting critical infrastructure (United Nations, 2000, 2004)
Interpol: The biggest international law enforcement agency in the world is that facilitates cross-border cooperation and information sharing among law enforcement agencies to combat cybercrime (Interpol, n.d.).

4.3 NATIONAL LEGISLATIONS

National legislations are essential for addressing cybercrime within individual countries. These legislations define cybercrimes, penalties, and enforcement mechanisms (“A Study of Cyber Crime Awareness for Prevention and Its Impact,” 2017) some notable examples include:

USA - Computer Fraud and Abuse Act (CFAA): The CFAA criminalizes unauthorized access to computer systems and networks and has been used to prosecute various cybercrimes. (Cybercrime and the law, 2020)
European Union - General Data Protection Regulation (GDPR): While primarily focused on data protection, GDPR includes provisions related to data breaches and imposes significant fines for non-compliance (European Union, 2016).
China - Cybersecurity Law: China's Cybersecurity Law imposes strict regulations on data protection, critical infrastructure, and the operations of technology companies (National People's Congress, 2016).

4.4 EMERGING JURISPRUDENCE

Emerging jurisprudence refers to legal precedents set by court decisions in cybercrime cases. As cybercrimes evolve, courts are increasingly confronted with novel legal challenges Some notable cases include:

United States v. Ross Ulbricht (Silk Road): This case involved the prosecution of Ross Ulbricht, the creator of the Silk Road, a dark web marketplace. It set a significant precedent for the legal treatment of dark web activities (United States v. Ulbricht, 2015).
Facebook, Inc. v. Power Ventures, Inc.: In this case, Facebook sued Power Ventures for violating the Computer Fraud and Abuse Act by accessing Facebook's data without authorization. The court's decision clarified the boundaries of authorized access (Facebook, Inc. v. Power Ventures, Inc., 2016).
Google Inc. v. Equustek Solutions Inc.: This case involved a dispute between Google and Equustek Solutions over the removal of search results. It set a precedent for the extraterritorial reach of court orders in the context of online activities (Google Inc. v. Equustek Solutions Inc., 2017).

4.5 CHALLENGES IN ATTRIBUTION OF CYBERCRIMES

Attributing cybercrimes to specific actors and jurisdictions is challenging due to factors like anonymity and cross-border nature. International cooperation and advancements in cyber forensics are essential for addressing these challenges effectively. A collective effort among nations, law enforcement agencies, and technology experts is necessary to combat cybercrime in an increasingly interconnected world. Attributing cybercrimes to specific actors and jurisdictions is a complex task due to several challenges

Anonymity and Pseudonymity: Cybercriminals often hide behind anonymous or pseudonymous online identities, making it difficult to link actions to real individuals.
Proxy Servers and Tor: The use of proxy servers and the Tor network allows cybercriminals to obfuscate their IP addresses and geographic location.
IP Spoofing: Cybercriminals can manipulate IP addresses, making it appear as if the attack originates from a different location.
Cross-Jurisdictional Attacks: Cybercrimes can be launched from one jurisdiction but target victims in another, creating jurisdictional challenges.
Technological Complexity: Cybercriminals employ advanced techniques to cover their tracks, including using compromised systems as intermediaries.
State-Sponsored Attacks: Nation-states often engage in cybercrimes but attempt to conceal their involvement, further complicating attribution.

4.6 PRESSING NEED FOR INTERNATIONAL COOPERATION

Addressing the challenges of attribution requires international cooperation among nations, law enforcement agencies, and technology companies (Haataja, 2022):

Information Sharing: Countries must collaborate to share intelligence and cyber threat information. Initiatives like the INTERPOL Digital Crime Centre facilitate such cooperation (INTERPOL, n.d.).
Cross-Border Legal Assistance: International legal frameworks must be strengthened to allow for the efficient exchange of evidence and assistance in investigations (Council of Europe, 2001).
Bilateral Agreements: Nations can establish bilateral agreements to streamline cooperation in cybercrime investigations (UNODC, 2013).
United Nations and Regional Organizations: The United Nations and regional organizations can provide a platform for member states to cooperate in addressing cybercrime (UNODC, 2019).

4.7 ADVANCEMENTS IN CYBER FORENSICS

Advancements in cyber forensics are vital for improving attribution capabilities (Casey, 2011):

Digital Evidence Collection: Cyber forensic experts use advanced tools to collect, preserve, and analyze digital evidence, which can assist in attribution.
Machine Learning and AI: Machine learning and artificial intelligence can aid in identifying patterns and anomalies in large datasets, helping to trace cybercriminals.
Blockchain Technology: Blockchain can be used for secure and tamper-proof evidence storage, enhancing the credibility of digital evidence.
Cybersecurity Collaboration: Collaboration between cybersecurity professionals, law enforcement, and private sector organizations can improve the detection and attribution of cybercrimes.

5.0 CYBERCRIMINALS VS. CYBERSECURITY PROFESSIONALS

The competition between cybercriminals and cybersecurity professionals is a cat-and-mouse game which is relentless and dynamic. As cybercriminals develop increasingly sophisticated techniques, cybersecurity professionals respond with innovative approaches to protect systems and data. This ongoing struggle underscores the importance of constant vigilance, collaboration, and staying ahead of emerging threats in the ever-evolving digital landscape.
Cybercriminals and cybersecurity experts are engaged in a continual state of invention and adaptation. Each side employs techniques to outwit the other. Below, we explore these techniques:

5.1 TECHNIQUES EMPLOYED BY CYBERCRIMINALS:

Sophisticated Malware: Cybercriminals continually develop advanced malware, including polymorphic and fileless malware, which can evade traditional security measures (Naidoo, R., & Jacobs, C. (2023).
Zero-Day Exploits: Cybercriminals seek and exploit vulnerabilities in software and systems before they are patched. This gives them an advantage in launching successful attacks.
Social Engineering: Cybercriminals manipulate human psychology through techniques like phishing, spear-phishing, and social media manipulation to deceive individuals and gain access to systems (Sekhar Bhusal, 2021)
Ransomware Innovations: Ransomware attacks continue to evolve, with criminals using encryption and anonymous cryptocurrencies to demand ransoms (Chen, Su, & Chen, 2018).

Dark Web Collaborations: Cybercriminals leverage the anonymity of the dark web to collaborate, buy/sell tools, and exchange stolen data (Palmieri, M., Shortland, N., & McGarry, P. 2021)

5.2 TECHNIQUES EMPLOYED BY CYBERSECURITY PROFESSIONALS:

Advanced Threat Detection: Security professionals employ advanced threat detection technologies, including machine learning and artificial intelligence, to identify and mitigate threats in real-time (Alharbi et al., 2022).
Behavioral Analysis: Analyzing user and network behavior helps in identifying anomalies that may indicate a security breach or insider threat
Patch Management: Cybersecurity teams actively manage software updates and patches to mitigate vulnerabilities before they can be exploited
Cyber Threat Intelligence: Gathering and analyzing threat intelligence helps organizations proactively prepare for emerging threats and vulnerabilities
Incident Response Plans: Organizations develop incident response plans to quickly detect, contain, and mitigate cyberattacks when they occur (NIST, 2018).
Collaboration and Information Sharing: Public and private sector organizations collaborate to share threat information, enabling a collective defense against cyber threats (IC3, 2021).

5.3 PROACTIVE DEFENSE STRATEGIES:

Proactive defense strategies are crucial for preventing cyberattacks and minimizing their impact when they occur. These strategies include:

Vulnerability Management: Continuously identifying and patching vulnerabilities in systems and software
User Training and Awareness: Educating employees about cybersecurity best practices to reduce the risk of falling victim to social engineering attacks (Sekhar Bhusal, 2021)
Security by Design: Building security into software and hardware products from the outset to prevent vulnerabilities
Zero Trust Architecture: Adopting a zero-trust approach that requires verification of every user and device trying to access resources (Forrester, 2018).

5.4 THREAT INTELLIGENCE SHARING:

Threat intelligence sharing involves the exchange of information about cyber threats and vulnerabilities among organizations, government agencies, and cybersecurity experts. It plays an essential function in improving cybersecurity Manavi, M. T. (2018). Key benefits include:

Detecting threats early: Shared threat intelligence enables organizations to detect emerging threats and vulnerabilities at the beginning phases.
Contextual Information: It provides context around threats, helping organizations recognize the type and severity of of potential attacks.
Collective Defense: Collaborative efforts to share threat intelligence strengthen the collective defense against cyber threats (IC3, 2021).

5.5 ROBUST INCIDENT RESPONSE PROTOCOLS:

Effective incident response protocols are essential for minimizing the impact of cyberattacks and ensuring a swift and coordinated response. Components of a robust incident response plan include:

Preparation: Developing an incident response plan, defining roles and responsibilities, and ensuring that the organization is prepared for potential incidents (NIST, 2018).
Detection and Analysis: Monitoring systems for signs of an incident, investigating incidents when detected, and determining their scope and impact
Containment and Eradication: Taking immediate actions to contain the incident and prevent further damage, followed by efforts to eradicate the threat from the network (NIST, 2018).
Recovery and Lessons Learned: Restoring affected systems and data, analyzing the incident for lessons learned, and updating security measures to prevent future incidents (NIST, 2018).

6.0 CONCLUSION

The study highlights the growing internet, which has improved connectivity and convenience but also led to an increase in cybercrime. It explores its evolution, forms, and socio-economic impact. The study also discusses the legal aspects of cybercrime, emphasizing the need for international collaboration and advancements in cyber forensics. It also highlights the ongoing arms race between cybersecurity professionals and cybercriminals, emphasizing the importance of proactive defense strategies and robust incident response protocols. The study calls for increased public awareness, collaboration among stakeholders, and innovative technological solutions to mitigate cyber threats.

REFERENCES:

1. A Study of Cyber Crime Awareness for Prevention and its Impact. (2017). International Journal of Recent Trends in Engineering and Research, 3(10), 240–246. https://doi.org/10.23883/ijrter.2017.3480.jtu50
2. Alharbi, S., Attiah, A., & Alghazzawi, D. (2022). Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends. Sustainability, 14(23), 16002. https://doi.org/10.3390/su142316002
3. Arnell, P., & Faturoti, B. (2022). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. International Review of Law, Computers & Technology, 37(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888
4. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
5. Cybercrime and the Law: Peter G. Berris, Computer Fraud and Abuse Act (CFAA) and the 116th Congress September 21, 2020
6. European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj
7. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016).
8. Forrester. (2018). The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2018.
9. Google Inc. v. Equustek Solutions Inc., 137 S. Ct. 1744 (2017)
10. Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84–90. https://doi.org/10.1016/j.procs.2023.01.267
11. Haataja, S. (2022). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. International Journal of Law and Information Technology, 30(4), 423–443. https://doi.org/10.1093/ijlit/eaad006
12. IC3 (Internet Crime Complaint Center). (2021). 2020 Internet Crime Report. Retrieved from https://pdf.ic3.gov/2020_IC3Report.pdf
13. INTERPOL. (n.d.). Digital Crime Centre. Retrieved from https://www.interpol.int/en/Crimes/Digital-crime/Digital-crime-centre
14. Lusher, D. (2018). Organised cybercrime: Key findings from the UK and beyond. University of Surrey.

15. Manavi, M. T. (2018). Defense mechanisms against Distributed Denial of Service attacks : A survey. Computers & Electrical Engineering, 72, 26–38. https://doi.org/10.1016/j.compeleceng.2018.09.001
16. Mohsin, K. (2021). The Internet and its Opportunities for Cybercrime – Interpersonal Cybercrime. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3815973
17. Naidoo, R., & Jacobs, C. (2023). Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework. European Conference on Cyber Warfare and Security, 22(1), 311–318. https://doi.org/10.34190/eccws.22.1.1443
18. Naidoo, R., & Jacobs, C. (2023). Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework. European Conference on Cyber Warfare and Security, 22(1), 311–318. https://doi.org/10.34190/eccws.22.1.1443
19. National Institute of Standards and Technology (NIST). (2018). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Special Publication 800-61 Revision 2.
20. National People's Congress. (2016). Cybersecurity Law of the People's Republic of China. Retrieved from http://www.npc.gov.cn/npc/c30834/201612/20de7ff8f7c9496b8fedf73d0f227643.shtml
21. Nershi, K., & Grossman, S. (2023). Assessing the Political Motivations Behind Ransomware Attacks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4507111
22. Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Computers in Human Behavior, 120, 106745. https://doi.org/10.1016/j.chb.2021.106745
23. Rybicki, P. (2023). Standardization In Combating Cybercrime Area. Cybersecurity & Cybercrime, 1(2), 109–130. https://doi.org/10.5604/01.3001.0053.8024
24. Scarfone, K., & Souppaya, M. (2006). Guide to Computer Security Log Management. National Institute of Standards and Technology (NIST)
25. Sekhar Bhusal, C. (2021). Systematic Review on Social Engineering: Hacking by Manipulating Humans. Journal of Information Security, 12(01), 104–114. https://doi.org/10.4236/jis.2021.121005
26. U.S. Department of Justice. (n.d.). Computer Crime & Intellectual Property Section (CCIPS) - Computer Crime & Intellectual Property Section (CCIPS). Retrieved from https://www.justice.gov/criminal-ccips
27. United Nations. (2004). Resolution 58/199: Creation of a global culture of cybersecurity. Retrieved from https://undocs.org/A/RES/58/199
28. United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2015).
29. UNODC. (2013). Model law against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition and explosives. Retrieved from https://www.unodc.org/documents/firearms-protocol/Model_Law_ENG_WEB.pdf
30. UNODC. (2019). Comprehensive Study on Cybercrime. Retrieved from https://www.unodc.org/unodc/en/cybercrime/study.html