ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2023-5.384 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-11

RESPONSIBILITY FOR ROBBERY OF OTHERS' PROPERTY USING COMPUTER TOOLS

Latipova Durkhonim Muxammadjon qizi
Master student of Tashkent State Law University

Abstract: This article explores the issue of cyber robbery—unlawful theft of digital property using computer tools—by examining the legal, ethical, and preventative responsibilities associated with it. Unlike traditional theft, cyber robbery allows criminals to steal financial assets, data, and intellectual property remotely, using tactics like phishing, malware, and ransomware. While international frameworks and national laws aim to prosecute offenders, challenges such as anonymity, evolving technology, and cross-jurisdictional complexities hinder effective enforcement. Organizations are also responsible for protecting data and can face legal consequences for negligence.

Keywords: cyber robbery, digital theft, computer crime, cybersecurity, legal responsibility, ethical responsibility, phishing, ransomware, international cooperation, data protection.

With the advent of the digital age, the nature of robbery has evolved far beyond physical theft and into the virtual realm, posing new challenges for law enforcement, lawmakers, and society at large. Cybercriminals today leverage computer tools to gain unauthorized access to individuals' and organizations' property, stealing sensitive data, financial assets, and intellectual property with little more than a few keystrokes. The responsibility for such acts is multifaceted, involving both individual culpability and systemic issues within our digital infrastructure. Understanding the nature, impact, and legal responsibilities associated with cyber robbery is essential for developing strategies to prevent such crimes and to hold offenders accountable. Traditional robbery is characterized by the unlawful taking of property from another person with intent to permanently deprive the owner of its use. Cyber robbery, while lacking physical confrontation, follows a similar principle but is executed through digital means. The evolution of technology has introduced numerous forms of cyber robbery, including identity theft, hacking, phishing, malware distribution, and ransomware attacks. Each form leverages a distinct method to infiltrate systems, obtain unauthorized access, and transfer or erase valuable data or funds. Unlike traditional crimes, cyber robbery can be committed remotely, with the attacker often concealed behind sophisticated methods that obscure their identity, complicating efforts to trace and prosecute.

National Laws on Cyber Robbery. Countries worldwide have enacted cybercrime legislation to address the growing threat of digital theft. For example, in the United States, the Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access to computer systems, while the Electronic Communications Privacy Act (ECPA) protects electronic communications from interception. Similarly, the United Kingdom’s Computer Misuse Act criminalizes unauthorized access to computer systems and data alteration. These laws have been instrumental in holding cyber robbers accountable, yet challenges remain, particularly in terms of cross-border cybercrime.

International Cooperation in Cybercrime Prosecution. Given the cross-jurisdictional nature of cybercrime, international cooperation is often necessary to pursue offenders. The

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2023-5.384 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-11

Budapest Convention on Cybercrime, established by the Council of Europe, is one of the most comprehensive international treaties on the subject. It provides a framework for nations to collaborate on cybercrime investigations, sharing information and resources to apprehend and prosecute cybercriminals. Although many countries are signatories, others, such as Russia and China, have abstained, which complicates international cooperation. This divergence highlights the need for globally standardized regulations and collaboration to effectively address cyber robbery.

Corporate Responsibility and Liability. Organizations also bear responsibility for safeguarding the data they hold. Failure to implement adequate cybersecurity measures can result in legal liability if a breach occurs. Companies are required to comply with regulations like the General Data Protection Regulation (GDPR) in the European Union, which mandates strict data protection measures. Non-compliance can lead to severe penalties, even if the company is itself a victim of cyber robbery. This creates a dual responsibility: companies must both protect their assets and those of their clients, and they must cooperate with authorities in the investigation and prosecution of cybercrimes. In some cases, companies may also pursue civil actions against perpetrators to recover stolen assets, though the success of such actions depends on the ability to identify the offender.

Challenges in Prosecuting Cyber Robbery. One of the primary obstacles in prosecuting cyber robbery is the anonymity afforded to perpetrators by the internet. Cybercriminals use various techniques to mask their identity and location, such as VPNs, proxy servers, and the dark web. This anonymity not only makes it difficult to identify and apprehend offenders but also complicates the attribution of responsibility. In some cases, law enforcement agencies may successfully trace the origin of an attack, only to find that it originated in a country with lax cybercrime laws or limited cooperation with international authorities. Another challenge is the rapid evolution of technology, which outpaces legislative processes. Laws that may have been effective five years ago may now be obsolete, leaving legal gaps that cybercriminals exploit. Additionally, the technical complexity of cyber robbery cases demands specialized knowledge on the part of law enforcement and the judiciary, which may not always be available. This can lead to inconsistencies in the prosecution and sentencing of cybercriminals.

Ethical Responsibility and Societal Impact. Beyond legal responsibility, there is an ethical dimension to cyber robbery that reflects on the integrity of both individuals and organizations in the digital age. Ethical responsibility includes respecting others' privacy, securing personal and organizational data, and avoiding exploitation of digital vulnerabilities. Those who commit cyber robbery disregard these ethical principles, often rationalizing their actions as victimless due to the absence of physical interaction. However, the impact of cyber robbery is far from victimless. It can devastate individuals financially, tarnish the reputation of businesses, and erode public trust in digital systems. Cyber robbery also imposes broader societal costs, as individuals and businesses must invest increasingly in cybersecurity measures. This creates a digital arms race where criminals develop new techniques to bypass security protocols, prompting organizations to continually enhance their defenses. The ethical responsibility to act with integrity in the digital realm is crucial in fostering a safe online environment, particularly as society becomes more reliant on digital systems for everyday activities.

The Role of Education and Prevention. Prevention is a critical component of addressing cyber robbery, as reactive measures alone are insufficient to curb the rising threat. Educational

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2023-5.384 ResearchBib IF: 8.848 / 2024

VOLUME-4, ISSUE-11

initiatives aimed at increasing awareness of cyber threats and teaching individuals and organizations how to protect themselves are essential. For individuals, understanding the risks associated with phishing scams, password reuse, and unsecured networks can significantly reduce vulnerability to cyber robbery. For organizations, investing in cybersecurity training for employees, implementing robust access controls, and maintaining up-to-date security software are all vital preventative measures. Law enforcement agencies also play a role in prevention through public awareness campaigns and initiatives to educate the public on recognizing and reporting cybercrimes. Such programs can empower individuals to take proactive steps in safeguarding their digital property and contribute to a collective resilience against cyber robbery.

Conclusion. Responsibility for cyber robbery lies primarily with the individuals who commit these crimes, but it also extends to organizations, lawmakers, and society as a whole. Legal frameworks are essential in holding perpetrators accountable, yet they must evolve to address the rapid pace of technological advancement and the global nature of cybercrime. International cooperation, comprehensive national laws, and corporate accountability are all necessary components of an effective response. However, prevention through education and proactive cybersecurity measures is equally important in minimizing the impact of cyber robbery. Cybercrime may be a complex and evolving issue, but through a combination of legal accountability, ethical responsibility, and public awareness, society can better protect itself against this pervasive threat. The responsibility to prevent and address cyber robbery ultimately rests with everyone involved in the digital ecosystem, from individual users to international governing bodies.

References:

1. Grabosky, P. N. (2007). The Internet, technology, and organized crime. Asian Journal of Criminology, 2(2), 145-161. https://doi.org/10.1007/s11417-007-9028-9
2. Holt, T. J., & Bossler, A. M. (2014). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Journal of Criminal Justice Education, 25(4), 443-460. https://doi.org/10.1080/10511253.2014.903878
3. Levi, M., & Williams, M. (2013). Multi-agency partnerships in cybercrime reduction:Mapping the UK information assurance network cooperation space. Journal of Financial Crime, 20(4), 386-398. https://doi.org/10.1108/JFC-04-2013-0022
4. McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Research Report 75. Home Office. Retrieved from https://assets.publishing.service.gov.uk
5. Wall, D. S. (2007). Cybercrime, media, and insecurity: The shaping of public perceptions of cybercrime. International Review of Law, Computers & Technology, 21(3), 203-209. https://doi.org/10.1080/13600860701588694