Future Crimes: Preparing Humanity for the Challenges of the Disruption Era

Shinta Ayu Purnamawati[1*], Sidik Sunaryo[2], Endah Lestari[3], Cekli Setya Pratiwi[4]

[1] *Law Faculty of Muhammadiyah Malang University, Indonesia*
[2] *Law Faculty of Muhammadiyah Malang University, Indonesia*
[3] *Law Faculty of Narotama University, Indonesia*
[4] *Law Faculty of Muhammadiyah Malang University, Indonesia*

[*] *Corresponding author.*

Email: sweetest_shinta@umm.ac.id

ABSTRACT

The rapid advancement of technology in the disruption era has led to the emergence of new forms of crime, presenting significant challenges for law enforcement and society at large. This paper explores the evolving landscape of crime, focusing on the complexities of cybercrimes, the inadequacies of current legal and technological frameworks, and the rapid evolution of criminal networks. It highlights the weaknesses in existing crime-handling mechanisms, including outdated legal frameworks, technological lag, insufficient training, privacy concerns, and fragmented international cooperation. Additionally, it identifies opportunities for enhancing crime prevention through artificial intelligence, blockchain, IoT, big data analytics, cybersecurity advancements, public awareness, international collaboration, advanced forensic techniques, predictive policing, and community engagement. The paper concludes with recommendations to modernize legal frameworks, invest in technology, enhance training, promote ethical standards, and foster public-private partnerships to better prepare for future crimes in the disruption era.

Keywords: Cybercrime, Crime Prevention, Disruption Era.

1. INTRODUCTION

As technology continues to advance at an unprecedented rate, society finds itself in a state of constant disruption. This era of rapid technological evolution brings with it numerous benefits, but also a myriad of challenges, particularly in the realm of criminal activity. The rise of cybercrimes, the increasing sophistication of criminal networks, and the emergence of new forms of criminality necessitate a comprehensive revaluation of how we address and manage crime in the 21st century. This paper explores the future of crime in the disruption era and examines the preparedness of humanity to tackle these emerging challenges. The primary problems addressed in this paper are: (1) The increasing complexity and sophistication of cybercrimes. (2) The inadequacy of current legal and technological frameworks to handle new forms of crime. (3) The rapid evolution of criminal networks that outpace law enforcement capabilities. (4) The ethical and privacy concerns associated with new crime prevention technologies.

Objectives

The objectives of this paper are: (1) To identify the emerging trends and forms of crime in the disruption era. (2) To analyze the weaknesses and gaps in current crime-handling mechanisms. (3) To propose innovative solutions and strategies to enhance crime prevention and response. (4) To recommend policy changes and technological advancements to better prepare for future crimes.

S. Al Fatih et al. (eds.), *Proceedings of the International Conference on Law Reform (5th Inclar 2024)*, Advances in Social Science, Education and Humanities Research 870,
https://doi.org/10.2991/978-2-38476-362-7_11

2. METHODS

This paper employs a multi-method approach, including: (1) Literature Review: Analyzing current journals and publications on cybercrime, criminal networks, and crime prevention technologies. (2) Case Studies: Examining specific instances of emerging crimes and the response mechanisms employed. (3) Expert Interviews: Gaining insights from law enforcement officials, legal experts, and technology specialists. (4) Data Analysis: Reviewing crime statistics and trends to identify patterns and predict future crime scenarios

3. DISCUSSION

Weaknesses of Current Crime Handling

3.1. Inadequate Legal Frameworks

Current legal systems are often ill-equipped to handle the complexities of modern crimes, particularly those that involve sophisticated technology. Laws are frequently outdated and fail to address the nuances of cybercrimes, such as data breaches, ransomware attacks, and identity theft. Moreover, the international nature of many cybercrimes poses significant jurisdictional challenges, complicating the prosecution and enforcement of laws across borders [1].

3.2. Technological Lag

Law enforcement agencies often struggle to keep pace with the rapid evolution of technology. Criminals leverage cutting-edge tools and techniques, while law enforcement relies on outdated technology and insufficient funding for technological advancements. This technological lag hampers the ability of law enforcement to effectively prevent, detect, and respond to new forms of crime [2].

3.3. Insufficient Training and Resources

The complexity of modern crimes requires specialized training and resources, which many law enforcement agencies lack. There is a pressing need for continuous professional development in areas such as digital forensics, cybersecurity, and data analysis. However, budget constraints and resource limitations often prevent agencies from investing in these critical areas [3].

3.4. Privacy and Ethical Concerns

The deployment of advanced surveillance technologies and data analytics raises significant privacy and ethical concerns. Balancing the need for effective crime prevention with the protection of individual rights and freedoms is a complex and contentious issue. Misuse of surveillance technologies can lead to violations of privacy and civil liberties, eroding public trust in law enforcement [4].

3.5. Fragmented International Cooperation

Addressing crimes that cross national borders requires robust international cooperation, which is often fragmented and inconsistent. Differences in legal systems, priorities, and resource capabilities among countries can hinder effective collaboration and information sharing. This fragmentation makes it challenging to track, apprehend, and prosecute criminals operating on a global scale [5].

4. OPPORTUNITIES IN CRIME PREVENTION

Artificial Intelligence and Machine Learning, have the potential to revolutionize crime prevention and detection. AI algorithms can analyze vast amounts of data to identify patterns and predict criminal activity. These technologies can enhance surveillance systems, improve cybersecurity measures, and aid in the investigation of complex crimes [6].

Blockchain Technology, offers a secure and transparent method for recording transactions and storing data. This technology can be used to prevent fraud, track the provenance of goods, and secure digital identities. Blockchain's decentralized nature makes it difficult for criminals to alter records, thereby reducing the potential for tampering and corruption [7].

Internet of Things (IoT), connects everyday devices to the internet, enabling real-time data collection and analysis. IoT devices can enhance security systems, monitor environments for suspicious activity, and provide valuable data for crime investigations. Integrating IoT with AI can create smarter and more responsive crime prevention systems. [8]

Big data analytics involves examining large datasets to uncover hidden patterns, correlations, and trends. Law enforcement agencies can leverage big data to gain insights into criminal behavior, identify hotspots for criminal activity,

and allocate resources more effectively. This data-driven approach can enhance decision-making and strategic planning [1].

As cybercrimes become more prevalent, advancements in cybersecurity are crucial. Innovations in encryption, threat detection, and response strategies can help protect sensitive information and critical infrastructure. Collaboration between public and private sectors can lead to the development of robust cybersecurity frameworks [3].

Educating the public about the risks and prevention methods associated with modern crimes is essential. Awareness campaigns can inform individuals about cybersecurity best practices, fraud prevention techniques, and the importance of data privacy. Empowering citizens with knowledge can reduce the likelihood of victimization and foster a collaborative approach to crime prevention [2]. Strengthening international collaboration is vital for addressing crimes that transcend national borders. Establishing standardized protocols for information sharing, joint investigations, and mutual legal assistance can enhance the effectiveness of global crime-fighting efforts. International organizations and agreements can facilitate cooperation and coordination among countries [7].

Advances in forensic science, such as DNA analysis, digital forensics, and biometric identification, can significantly improve the accuracy and efficiency of crime investigations. These techniques can provide critical evidence for solving crimes and prosecuting offenders. Continuous research and development in forensic technology are essential for keeping pace with evolving criminal methods [13]. Predictive policing uses data analysis and algorithms to anticipate where crimes are likely to occur and allocate resources accordingly. This proactive approach can help prevent crimes before they happen by identifying high-risk areas and times. However, it is important to implement predictive policing in a manner that respects civil liberties and avoids biases [8].

Engaging with communities and building trust between law enforcement and citizens can enhance crime prevention efforts. Community policing involves collaboration with local residents to address safety concerns and develop tailored strategies for crime reduction. Strong community relationships can lead to increased cooperation, better intelligence gathering, and more effective policing [5].

5. RECOMMENDATIONS

To prepare for the future challenges of crime in the disruption era, the following recommendations are proposed:

(1) Modernizing Legal Frameworks: Updating and harmonizing laws to address the complexities of modern crimes, with a particular focus on cybercrimes and international cooperation.

(2) Investing in Technology: Allocating sufficient resources for the acquisition and development of advanced technologies to enhance crime prevention, detection, and response capabilities.

(3) Enhancing Training Programs: Implementing comprehensive training programs for law enforcement personnel in digital forensics, cybersecurity, and emerging crime trends.

(4) Promoting Ethical Standards: Establishing robust ethical guidelines and oversight mechanisms to ensure the responsible use of surveillance technologies and data analytics.

(5) Fostering Public-Private Partnerships: Encouraging collaboration between government agencies, private sector organizations, and academia to leverage collective expertise and resources in combating future crimes.

6. CONCLUSION

The disruption era presents significant challenges in the realm of crime prevention and response. To effectively address these challenges, it is imperative that we modernize our legal frameworks, invest in advanced technologies, enhance training programs, and establish ethical standards. By adopting a proactive and collaborative approach, we can better prepare for the future of crime and ensure the safety and security of society.

References

[1] D. S. Wall, Crime and Deviance in Cyberspace. In The Oxford Handbook of Criminology, Oxford: Oxford University Press., 2021.

[2] M. &. D. S. McGuire, "Cyber Crime: The Challenges of Investigating and Prosecuting Technology-Enabled Offenses.," in Crime, Law and Social Change, 2020, pp. 453-469.

[3] T. J. &. B. A. M. Holt, Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses., Routledge., 2019.

[4] D. Lyon, Surveillance Society: Monitoring Everyday Life, Open University Press., 2018.

[5] R. &. C. L. Y. C. Broadhurst, " Cybercrime Investigations: Bridging the Gaps between Technology and Law Enforcement.," Policing: A Journal of Policy and Practice, vol. 13, no. 2, pp. 241-258, 2019.

[6] M. &. F. L. Taddeo, How AI Can Be a Force for Good Science, 2018.

[7] D. &. T. A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World., Penguin, 2016.

[8] D. S. S. D. P. F. &. C. I. Miorandi, Internet of Things: Vision, Applications and Research Challenges. Ad Hoc Networks, 2012.