INTERNATIONAL JOURNAL OF
LAW
AND SOCIAL DEVELOPMENT

NAWALA

Volume 3, Number 1, 2024

Criminal Policy in Countering Cybercrime Based on Quantum Computing

Tofik Yanuar Chandra [1]

[1] Universitas Jayabaya, Jakarta, Indonesia

Abstract

Article history:
Received: January 7, 2024
Revised: February 23, 2024
Accepted: April 20, 2024
Published: June 30, 2024

Keywords:
Criminal Policy,
Cybercrime,
Digital Security,
Post-Quantum Cryptography,
Quantum Computing.

Identifier:
Nawala
Page: 73-89
https://nawala.io/index.php/ijlsd

This study examines criminal policy in countering cybercrime in the era of quantum computing through a literature study method on 11 academic sources. Quantum computing poses a major threat to digital security, especially the ability to solve conventional cryptographic systems that have been the backbone of data protection. However, on the other hand, this technology opens up huge opportunities through the implementation of new security solutions such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). This study found that criminal policy in the quantum era requires regulatory updates, integration of cutting-edge security technologies, strengthening international cooperation, and implementing anticipatory governance to anticipate the acceleration of technological development. Ethical aspects and human rights protection are important considerations so that quantum technology is not abused. This research recommends a multidisciplinary approach that combines technology, legal, and public policy perspectives to create a resilient, adaptive, and sustainable cybersecurity ecosystem in the face of the challenges of the quantum era.

*Corresponding author:
(Tofik Yanuar Chandra)

1. Introduction

The development of information technology has had a significant impact on the dynamics of cybercrime, where perpetrators take advantage of technological advances to carry out increasingly complex and difficult to track attacks. In this context, the emergence of quantum computing is a strategic factor that has the potential to fundamentally change the cybersecurity landscape. This technology, which utilizes the principles of superposition and entanglement, has an exponential computing capacity that can solve conventional cryptographic algorithms in a short time. This creates urgency for the state and law enforcement agencies to anticipate these potential threats through adaptive and evidence-based criminal policies. Criminal policy in countering cybercrime is a legal and strategic framework that aims to prevent, overcome, and take action against criminals in the digital realm.

However, the presence of quantum computing presents new challenges, especially related to the ability of this technology to decrypt previously secure data, bypass authentication systems, and hack critical infrastructure. This threat is not only technical, but also has legal, ethical, and geopolitical dimensions that require global coordination. On the other hand, quantum technology can also be used as a tool to prevent cybercrime. For example, the application of Quantum Key Distribution (QKD) is able to provide a level of security that is almost impenetrable with conventional hacking methods.[1] A number of studies have shown that the integration of quantum technology in cybersecurity policy can strengthen state and

[1] Tiago M. Fernández-Caramés. "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things." *IEEE Internet of Things Journal* 7, no. 7 (2019): 6457-6480.

private sector defenses against future cyber threats. Thus, criminal policy in the era of quantum computing must be dualistic: anticipating risks while taking advantage of existing opportunities.

From a public policy perspective, the response to the threat of quantum computing requires a cross-disciplinary approach involving policymakers, technology experts, law enforcement officials, and the industrial sector. This strategy includes regulatory reform, adoption of quantum-safe cryptography technology, as well as capacity building of human resources in the field of cybersecurity. Criminal policies that do not keep up with technological developments risk creating legal loopholes that can be exploited by cybercrime perpetrators. The international context shows that there are differences in readiness between countries in dealing with quantum computing threats. Developed countries such as the United States, the European Union, and China have developed a roadmap for the transition to quantum-resistant cryptography.

In contrast, many developing countries are still focusing on countering conventional cybercrime without considering these future threats. This inequality can pose global security risks, as quantum-based cybercrime knows no geographical boundaries and can take advantage of weak points in the global system. In addition to the technical aspects, there are also legal and ethical dimensions that need to be regulated. The application of quantum technology in digital forensic investigations, for example, raises questions related to privacy protection, data integrity, and human rights. Therefore, the formation of criminal policy in the quantum age requires a balance between security and civil liberties. This challenge is increasingly complex

because the development of quantum technology is taking place very quickly, while the process of legislation and policy harmonization between countries tends to be slow.

This research was prepared using a literature study method on various scientific publications from the last five years. The focus of the research is to identify challenges and opportunities in the formation of criminal policies for quantum computing-based cybercrime countermeasures. This study will examine relevant technical, legal, and policy aspects, as well as provide strategic recommendations for policymakers at the national and international levels. By referring to the current literature, it is hoped that this research can contribute to a more comprehensive understanding of the interaction between criminal policy and quantum technology. This is important to ensure that the policies taken are not only reactive to threats, but also proactive in building a sustainable and resilient cybersecurity ecosystem in the era of quantum computing.

2. Literature Review

The development of quantum technology has been a major concern in the cybersecurity literature and criminal policy. Csenkey[2] emphasizes that quantum threats have a timeline that must be anticipated long before the technology reaches full maturity. They highlight the potential of quantum algorithms, such as the Shor algorithm, to solve the asymmetric cryptography that is currently widely used on the

[2] Kristen Csenkey and Nina Bindel. "Post-quantum cryptographic assemblages and the governance of the quantum threat." *Journal of Cybersecurity* 9, no. 1 (2023): tyad001.

internet. Kop et al.[3] reinforces this argument by showing how the power of quantum computing can change the paradigm of global cryptography. In terms of policy, Mosca and Piani[4] stated that the government must adopt a policy approach that is proactive, not reactive. This is in line with the opinion of Tõnurist and Hanson,[5] who emphasize the importance of quantum-safe cybersecurity through regulation and incentives for the private sector. The transition to post-quantum cryptography requires not only technical changes, but also policies that support its implementation across the national digital infrastructure.

Some studies have focused on the use of quantum technology as a solution. Dewi[6] explained the application of Quantum Key Distribution (QKD) as a method of securing communication that is almost impossible to penetrate. Stanley et al.[7] develop a policy framework that integrates QKD in the national security system, especially to protect sensitive data in the government and defense sectors. However, the adoption of quantum technology also brings legal and ethical challenges. Dwivedi et al.[8] discuss the legal implications of the application of quantum

---

3 Mauritz Kop, Mateo Aboy, and Timo Minssen. "Intellectual property in quantum computing and market power: a theoretical discussion and empirical analysis." *Journal of Intellectual Property Law and Practice* 17, no. 8 (2022): 613-628.

4 Michele Mosca, and Marco Piani, "*2021 Quantum Threat Timeline Report*," Global Risk Institute (2022): 33.

5 Piret Tõnurist, and Angela Hanson, "*Anticipatory innovation governance. Shaping the future through proactive policy making,*" OECD Working Papers on Public Governance No. 44, 2020: 19.

6 Rafiqa Dewi. "Tinjauan Keamanan Informasi Pada Jaringan Komputer Kuantum." *Jurnal Elektro dan Telkomunikasi* 5, no. 2 (2018): 1-4.

7 Manoj Stanley, Y. Gui, D. Unnikrishnan, S. R. G. Hall, and I. Fatadin, "Recent progress in quantum key distribution network deployments and standards," In *Journal of Physics: Conference Series*, IOP Publishing, vol. 2416, no. 1, 2022: 012001.

8 Abhinav Dwivedi, Gurmeet Kaur Saini, and Usma Ibrahim Musa. "Cybersecurity and prevention in the quantum era." In *2023 2nd International conference for innovation in technology (INOCON)*, IEEE, (2023): 1-6.

technology, particularly related to privacy, data security, and human rights. Wibowo[9] emphasized the need to establish a legal framework that is in line with the development of quantum technology, so that criminal policies can regulate and facilitate innovation. The global aspect of coordination is also an important theme. Tunji[10] underlines that the threat of quantum-based cybercrime requires international coordination, as attacks can target weak points in countries that are not yet technologically prepared.

Chisty[11] warns that without policy harmonization, law enforcement against quantum cybercrime will be fragmented and ineffective. In addition, the literature also discusses the integration of quantum technology in digital forensic investigations. AlMudaweb[12] assesses that quantum technology can accelerate the analysis of forensic data, but risks violating due process principles if not properly regulated. Through the ETSI technical guidance emphasizes that criminal policy must be built in tandem with global technical standards to ensure consistent security. This literature review shows the existence of two main poles in the literature: (1) the threats posed by quantum computing to existing cybersecurity systems, and (2) the opportunities for the utilization of quantum technology to strengthen security and

9 Agus Wibowo. "Hukum di era globalisasi digital." *Penerbit Yayasan Prima Agus Teknik* (2023): 1-185.

10 Babatunde Tunji. "Quantum-Safe Cryptography Readiness in Enterprise Networks: Challenges and Roadmap." (2021).

11 Nur Mohammad Ali Chisty, Parikshith Reddy Baddam, and Ruhul Amin. "Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity." *Engineering International* 10, no. 2 (2022): 69-84.

12 Ahmed AlMudaweb, and Wael Elmedany. "Securing smart cities in the quantum era: challenges, solutions, and regulatory considerations." In *IET Conference Proceedings CP859*, Stevenage, UK: The Institution of Engineering and Technology, 20, no. 44, (2023): 484-491.

investigation. Both perspectives require a responsive, evidence-based, and internationally integrated criminal policy to address the challenges of cybercrime in the era of quantum computing.

3. Method

This study uses a literature review method to analyze criminal policies in countering cybercrime based on quantum technology. This method was chosen because the topics studied are multidisciplinary, covering technological, legal, and public policy aspects, so they require the collection and synthesis of knowledge from various credible scientific sources. The research stage begins with the identification of the topic and the formulation of the problem, namely analyzing how the development of quantum computing affects criminal policy in the context of cybersecurity, both in terms of threats and opportunities. Furthermore, relevant keywords were determined, such as cybercrime policy, quantum computing security, quantum-safe cryptography, quantum key distribution, post-quantum cryptography, and cyber law in the quantum era.

The literature search process was carried out through Google Scholar and Elsevier. The goal is to ensure that the literature used reflects the latest developments in the field of quantum technology and cyber policy. From the search results, a number of publications were obtained which were then selected using inclusion criteria: Articles came from reputable journals or proceedings that were indexed internationally. It has a primary focus on the relationship between policy, cybersecurity, and quantum technology. Contains an in-depth discussion related to

the threat and/or utilization of quantum technology. The exclusion criteria include articles that only discuss quantum technical aspects with no relevance to criminal policy, and non-academic opinion articles. After the selection process, 11 articles were obtained that met the criteria as the basis for analysis.

The next stage is content analysis to identify the main themes. The analysis was carried out by reading each article in full, noting key points, and grouping the findings based on three main dimensions: (1) the security threats posed by quantum computing, (2) the opportunities for the use of quantum technology for cybersecurity, and (3) the implications of criminal policies at the national and international levels. Once the themes were collected, a synthesis of findings was carried out to build a conceptual framework that explains the linkage between the development of quantum technology and the need for criminal policy reform. This synthesis is also used to identify research gaps, for example related to the lack of global regulation on post-quantum security or the lack of international coordination in law enforcement against quantum cybercrime.

The validity of the research is maintained by applying the principle of source triangulation, which is comparing findings from various articles to avoid bias and ensure the accuracy of information. In addition, each reference is cited in accordance with the APA format to maintain academic transparency. With this method, the research is expected to provide a comprehensive overview of the challenges and opportunities in the formation of criminal policies to face the quantum computing era. The literature review approach allows researchers to systematically integrate

technological, legal, and policy perspectives, so that the results can be a foundation for decision-makers and researchers to develop resilient cybersecurity strategies.

4. Results

4.1. Cybersecurity Threats from Quantum Computing

The development of quantum computing brings with it the potential for serious threats to existing cybersecurity systems. One of the most significant threats is the ability of quantum computers to crack asymmetric cryptographic algorithms such as RSA and ECC through the Shor algorithm. This means that almost all encrypted communications that are currently considered secure can be illegally accessed by parties with high quantum computing capabilities. This threat is not only theoretical, but has begun to be anticipated by state and non-state actors through the development of harvest now, decrypt later attack, which is the practice of collecting current encrypted data to be decrypted in the future when quantum technology matures. These threats put sensitive information including government, financial, and health data at high risk.

Wibowo[13] added that this challenge is exacerbated by the delay in the adoption of post-quantum security technologies in many countries. The unpreparedness of digital infrastructure, coupled with a lack of awareness at the policy-making level, magnifies the security gaps that cybercriminals can exploit. Tunji[14] underlines that

13 Agus Wibowo. "Hukum di era globalisasi digital." *Penerbit Yayasan Prima Agus Teknik* (2023): 1-185.

14 Babatunde Tunji. "Quantum-Safe Cryptography Readiness in Enterprise Networks: Challenges and Roadmap." (2021).

quantum threats are global and distributed, so attacks can come from jurisdictions that do not have extradition treaties or legal cooperation. This circumstance obscures traditional limitations in cyber law enforcement and demands an update to the international legal framework. In general, the results of the literature review show that quantum threats have three main characteristics: (1) the ability to crack conventional cryptography in a short period of time, (2) the potential for cross-border attacks without detection, and (3) trigger a technology race between state actors and criminal groups to master quantum technology first. This threat demands an immediate, strategic, and coordinated policy response across countries.

4.2. Opportunities for Leveraging Quantum Technology for Cybersecurity

Despite its threats, quantum technology also offers great opportunities in strengthening cybersecurity. One of the most important innovations is Quantum Key Distribution (QKD), which allows the exchange of cryptographic keys with the security guaranteed by the laws of quantum physics. Stanley et al.[15] shows that QKD can be integrated in national communication networks to protect government data and vital infrastructure. In fact, several countries such as China and Japan have begun to develop a nation-wide QKD network. The advantage of QKD lies in its ability to detect eavesdropping attempts in real-time, allowing for a rapid response to threats.

15 Manoj Stanley, Y. Gui, D. Unnikrishnan, S. R. G. Hall, and I. Fatadin, "Recent progress in quantum key distribution network deployments and standards," In *Journal of Physics: Conference Series*, IOP Publishing, vol. 2416, no. 1, 2022: 012001.

In addition to QKD, the development of post-quantum cryptography (PQC) is also an important opportunity. ETSI recommended the adoption of a PQC algorithm that is resistant to quantum attacks, which is currently being standardized by NIST. PQC allows for a gradual transition from the old cryptographic system to a new, more secure system. In the context of criminal policy, Mosca and Piani[16] argue that the application of quantum technology can be used in digital forensic investigations, for example to accelerate data analysis or track illegal transactions on encrypted blockchain networks. However, this utilization requires clear legal rules so as not to violate the principles of privacy and due process. The opportunities offered by quantum technology for cybersecurity include: (1) securing communications through QKD, (2) strengthening encryption systems with PQC, and (3) accelerating the digital investigation process. This utilization must be accompanied by a criminal policy framework that maintains a balance between the effectiveness of law enforcement and the protection of human rights.

4.3. Implications of Criminal Policy in the Era of Quantum Computing

The changing landscape of threats and opportunities due to quantum computing requires significant adjustments in criminal policy. Dwivedi et al.[17] emphasize the importance of updating cybersecurity laws to include categories of quantum-based crime, both those committed by utilizing quantum technology and those aimed at attacking quantum infrastructure. According to Tõnurist and

16 Michele Mosca, and Marco Piani, "*2021 Quantum Threat Timeline Report*," Global Risk Institute (2022): 33.

17 Abhinav Dwivedi, Gurmeet Kaur Saini, and Usma Ibrahim Musa. "Cybersecurity and prevention in the quantum era." In *2023 2nd International conference for innovation in technology (INOCON)*, IEEE, (2023): 1-6.

Hanson,[18] criminal policy should include regulations that encourage the adoption of post-quantum security technologies, incentivize the private sector to invest in research and development, and establish standardized security audit mechanisms. International coordination is a crucial factor. Tunji[19] reminds that without harmonization of regulations between countries, efforts to counter quantum cybercrime will face juridical obstacles, especially in the process of extradition and exchange of digital evidence.

Chisty[20] added that international cooperation can be facilitated through multilateral agreements that include technical standards, investigative procedures, and intelligence-sharing mechanisms. AlMudaweb[21] also shows the need for integration between criminal policy and technical standards set by international bodies such as the ITU, ETSI, and NIST. This integration ensures that policies are not only legally relevant, but also aligned with the latest technological developments. Thus, the implications of criminal policy in the quantum computing era include: (1) updating relevant laws and regulations, (2) strengthening international coordination, and (3) integrating policies with global technical standards. This approach will enable a comprehensive, adaptive and effective response to quantum-based cybercrime.

---

18 Piret Tõnurist, and Angela Hanson, "*Anticipatory innovation governance. Shaping the future through proactive policy making,*" OECD Working Papers on Public Governance No. 44, 2020: 19.

19 Babatunde Tunji. "Quantum-Safe Cryptography Readiness in Enterprise Networks: Challenges and Roadmap." (2021).

20 Nur Mohammad Ali Chisty, Parikshith Reddy Baddam, and Ruhul Amin. "Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity." *Engineering International* 10, no. 2 (2022): 69-84.

21 Ahmed AlMudaweb, and Wael Elmedany. "Securing smart cities in the quantum era: challenges, solutions, and regulatory considerations." In *IET Conference Proceedings CP859*, Stevenage, UK: The Institution of Engineering and Technology, 20, no. 44, (2023): 484-491.

5. Discussion

The results of this literature review show that the development of quantum computing poses challenges and opportunities that fundamentally change the criminal policy landscape in the field of cybersecurity. In terms of challenges, the main threat comes from the ability of quantum computers to solve conventional cryptography through algorithms such as Shor and Grover, which threaten the confidentiality of communications and data integrity.[22] These findings are consistent with the warnings of Mosca and Piani[23] that quantum threats have the potential to change the cybersecurity paradigm from a technology trust-based system to a quantum physics-based system.

In terms of opportunities, innovations such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) offer solutions to mitigate these risks. The integration of this technology in national security infrastructure has proven promising, as demonstrated by QKD network projects in China and Japan.[24] However, the adoption of this technology requires large investments, political awareness, and a supportive regulatory framework so that the benefits can be widely felt. Theoretically, these findings support the view of situational crime prevention theory, which emphasizes that changes in the technological environment can affect the chances of crime. Quantum computing, in this case, acts as a catalyst that

22 Kristen Csenkey and Nina Bindel. "Post-quantum cryptographic assemblages and the governance of the quantum threat." *Journal of Cybersecurity* 9, no. 1 (2023): tyad001.

23 Michele Mosca, and Marco Piani, "*2021 Quantum Threat Timeline Report*," Global Risk Institute (2022): 33.

24 Tiago M. Fernández-Caramés. "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things." *IEEE Internet of Things Journal* 7, no. 7 (2019): 6457-6480.

expands opportunities for criminals, but at the same time provides new means for law enforcement.

The criminal policy implications identified in this study show that an effective response requires three main components. First, the update of laws and regulations to include the definition and category of quantum-based crimes. Second, strengthening international cooperation to deal with the cross-border nature of this crime, which is in line with Tunji's[25] suggestion about the importance of harmonizing global regulations. Third, the integration of policies with international technical standards so that the steps taken are in accordance with technological developments. However, these discussions also highlighted the gap between technology readiness and policy readiness. Many countries are still in the early stages of understanding quantum threats, while the development of quantum technology is proceeding very quickly. This raises the risk of policy lag, where regulations lag far behind technological developments. This situation demands the adoption of anticipatory governance, which is a proactive and adaptive policy approach to new technological developments.

In addition, the integration of quantum technology in law enforcement raises ethical questions related to privacy, abuse of authority, and potential technological discrimination. Therefore, criminal policy in the quantum era must pay attention to the balance between the effectiveness of law enforcement and the protection of human rights. This discussion underscored that quantum computing is not only a

25 Babatunde Tunji. "Quantum-Safe Cryptography Readiness in Enterprise Networks: Challenges and Roadmap." (2021).

technical challenge, but also a legal, social, and ethical issue. A multidisciplinary approach that combines technology, law, and public policy is indispensable to create a resilient cybersecurity ecosystem in the quantum age. With the right response, the threats brought by these technologies can be transformed into opportunities to build stronger, more adaptive, and sustainable cybersecurity systems.

6. Conclusion

This research confirms that the development of quantum computing has a significant impact on the cybersecurity landscape and criminal policy. On the threat side, the ability of quantum computers to break conventional cryptographic systems has the potential to weaken the global digital security infrastructure, necessitating an update of cyber defense strategies. On the opportunity side, technologies such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) could become the new security foundation that is more resilient to quantum attacks, provided they are integrated with the right criminal policies. The literature study method successfully identified three important dimensions: quantum-based security threats, opportunities for the use of quantum technology for data protection, and criminal policy implications at the national and international levels. The synthesis of findings shows that criminal policy in the quantum age requires legal reform, technological capacity building, and strengthening global cooperation.

The gap between the acceleration of quantum technology and policy readiness shows the need for the adoption of proactive and adaptive anticipatory governance. Without these steps, the risk of policy lag will make countries vulnerable to quantum-

based cyberattacks. On the other hand, policy formation must consider ethical aspects and human rights protection so that the use of quantum technology does not lead to abuse of power. As such, the response to the quantum era must be multidisciplinary, incorporating technology, legal, and public policy perspectives. This approach will ensure that the threats presented by quantum computing can be managed effectively, while leveraging the potential of this technology to create a resilient, equitable, and sustainable cybersecurity ecosystem.

References

AlMudaweb, Ahmed, and Wael Elmedany. "Securing smart cities in the quantum era: challenges, solutions, and regulatory considerations." In *IET Conference Proceedings CP859*, Stevenage, UK: The Institution of Engineering and Technology, 20, no. 44, (2023): 484-491.

Chisty, Nur Mohammad Ali, Parikshith Reddy Baddam, and Ruhul Amin. "Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity." *Engineering International* 10, no. 2 (2022): 69-84.

Csenkey, Kristen, and Nina Bindel. "Post-quantum cryptographic assemblages and the governance of the quantum threat." *Journal of Cybersecurity* 9, no. 1 (2023): tyad001.

Dewi, Rafiqa. "Tinjauan Keamanan Informasi Pada Jaringan Komputer Kuantum." *Jurnal Elektro dan Telkomunikasi* 5, no. 2 (2018): 1-4.

Dwivedi, Abhinav, Gurmeet Kaur Saini, and Usma Ibrahim Musa. "Cybersecurity and prevention in the quantum era." In *2023 2nd International conference for innovation in technology (INOCON)*, IEEE, (2023): 1-6.

Fernández-Caramés, Tiago M. "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things." *IEEE Internet of Things Journal* 7, no. 7 (2019): 6457-6480.

Kop, Mauritz, Mateo Aboy, and Timo Minssen. "Intellectual property in quantum computing and market power: a theoretical discussion and empirical analysis." *Journal of Intellectual Property Law and Practice* 17, no. 8 (2022): 613-628.

Mosca, Michele, and Marco Piani. "*2021 Quantum Threat Timeline Report*." Global Risk Institute (2022): 5-45.

Stanley, Manoj, Y. Gui, D. Unnikrishnan, S. R. G. Hall, and I. Fatadin. "Recent progress in quantum key distribution network deployments and standards." In *Journal of Physics: Conference Series*, IOP Publishing, vol. 2416, no. 1, (2022): 012001.

Tõnurist, Piret, and Angela Hanson. *Anticipatory innovation governance. Shaping the future through proactive policy making,* OECD Working Papers on Public Governance No. 44, (2020): 9-29.

Tunji, Babatunde. "Quantum-Safe Cryptography Readiness in Enterprise Networks: Challenges and Roadmap." (2021).