


The Influence of Fintech on the National Security System: Law, Economic Potential and Digital Defense Strategy

Ngasiman Djoyonegoro¹, Muhammad Noor Harisudin², Hariyanto^{3*}

¹ Faculty of Science and Technology, Institut Sains dan Teknologi Al-Kamal, Jakarta, Indonesia.

² Faculty of Sharia, Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember, Jember, Indonesia.

³ Faculty of Law, Universitas Islam Negeri Profesor Kiai Haji Saifuddin Zuhri Purwokerto, Purwokerto, Indonesia.

 : hariyanto@uinsaizu.ac.id
Corresponding Author*



Abstract

Introduction: Fintech has emerged as a transformative force in the financial sector, bringing significant changes encompassing economic potential and challenges to national security strategies.

Purposes of the Research: This research wants to explore the efforts that have been made by countries in dealing with the impact of Fintech on security.

Methods of the Research: This research uses a qualitative method with a descriptive analysis approach. This research focuses on qualitative methods and is researched to see the extent of the challenges posed by fintech to the country's resilience system

Results of the Research: The increasing adoption of Fintech also presents challenges to national security digital defense strategies. Threats to data security, cyberattacks, and misuse of financial technology can jeopardize national financial infrastructure, threaten the stability of the financial system, and pose risks to national security. Thus, concerted efforts from governments, financial institutions, and Fintech companies are required to enhance digital defense. Governments need to implement stringent regulations to safeguard Fintech user data and privacy and closely supervise Fintech operations to mitigate the risks of financial technology misuse. Collaboration between governments, financial institutions, and Fintech companies in sharing security intelligence is essential to tackle increasingly complex and organized threats. Additionally, investing in advanced security technology, raising user awareness about security, and strengthening oversight of critical infrastructure are crucial steps in digital defense strategies. Fintech has exerted significant influence on national security, offering vast economic potential while presenting intricate challenges to digital defense strategies. Acknowledging both the potential and challenges, governments and stakeholders must collaborate to create a secure, reliable, and sustainable Fintech ecosystem that fosters economic progress and bolsters overall national security.

Keywords: Digital Defense Strategies; Fintech; National Security System.

Submitted: 2024-07-18

Revised: 2025-06-19

Accepted: 2025-06-26

Published: 2025-06-29

How To Cite: Ngasiman Djoyonegoro, Muhammad Noor Harisudin, and Hariyanto. "The Influence of Fintech on the National Security System: Law, Economic Potential and Digital Defense Strategy." SASI 31 no. 2 (2025): 95-106. <https://doi.org/10.47268/sasi.v31i2.2244>

Copyright © 2025 Author(s)  Creative Commons Attribution-NonCommercial 4.0 International License

INTRODUCTION

Fintech, or financial technology, has experienced rapid development and has significantly impacted the country's security system. The emergence of various financial technology innovations, including digital payment platforms, online lending services, and crypto assets, has fundamentally changed the financial landscape. Despite providing economic potential and easy access to financial services, the development of Fintech also raises new challenges related to data security, consumer privacy, and cyber risks.¹

¹ Chen, A. "Proactive Cybersecurity Strategies: Collaboration and Intelligence Sharing". *Cybersecurity Policy Review*, (2019).

Therefore, it is important for the government and related institutions to proactively face and manage the security implications posed by Fintech to ensure the stability and resilience of the country's security system amidst the ongoing era of digital transformation.²

Some of the changes brought about by Fintech on state security systems include a profound transformation in the way financial transactions are carried out, an increased level of connectedness between financial institutions and users, and a surge in the volume of data that must be processed and protected.³ With the increasingly widespread adoption of financial technology, the country's security system is faced with new challenges in overcoming increasingly sophisticated and complex cyber threats. Apart from that, the presence of Fintech also brings new risks, such as digital fraud, money laundering and cyber-attacks, which can threaten stability and trust in the national financial system. Therefore, collaborative efforts and adaptive cyber defense strategies are key in dealing with the growing impact of Fintech on the country's security system.

Fintech has brought new economic potential by providing a solid impetus for financial inclusion, expanding the accessibility of financial services for various levels of society, and stimulating innovation in various economic sectors. By combining modern technology with traditional financial services, Fintech has presented various new products and services that are more efficient, cost-effective and easily accessible to individuals and businesses.⁴ Providing online loan services, digital payment platforms, and application-based financial solutions are examples of Fintech's contribution in driving the economy and creating new opportunities for inclusive and sustainable economic growth.⁵ Thus, Fintech becomes an essential catalyst in strengthening the country's economic competitiveness and brings significant benefits to the development of broader economic sectors.

However, on the other hand, Fintech also poses complex security challenges. As financial services become increasingly connected via digital platforms, countries face data security risks, fraud, money laundering and cyber attacks that can threaten the financial system's stability and national security. As financial services become increasingly connected via digital platforms, countries face complex data security risks that threaten the integrity and confidentiality of financial information. The increase in electronic financial transactions also opens up opportunities for potential fraud, money laundering, and other financial crimes that can harm the public and financial institutions. The threat of cyber attacks is also a major concern, considering that the country's financial infrastructure and sensitive data are attractive targets for malicious cyber actors.⁶

In facing this challenge, the country must strengthen its cyber defense strategy holistically and proactively. Data protection, identification and prevention of financial criminal activity, and investment in advanced cybersecurity technology are crucial to maintaining financial system stability and national security. In addition, cooperation and information exchange between financial institutions, regulators, and cybersecurity authorities is essential to detect and deal with threats more effectively.⁷ With awareness of increasingly complex risks, countries must take proactive steps in facing the digital

² Johnson, E. "Regulating Fintech for Security: A Policy Approach". *International Journal of Financial Regulation*. (2017).

³ Kim, D. "The Cybersecurity Challenges of Fintech Adoption". *Journal of Cybersecurity*. (2019).

⁴ Tan, A. "The Evolution of Fintech: A Comprehensive Analysis". *Journal of Financial Innovation*. (2019)

⁵ Lee, S. "The Impact of Fintech on Financial Inclusion: Evidence from Emerging Markets". *Journal of Economic Perspectives*. (2020).

⁶ Tan, J. "Cybersecurity Challenges in the Age of Fintech: An Analysis of Emerging Threats". *Journal of Cybersecurity Studies*. (2021).

⁷ Wong, A. "The Efficiency Revolution: How Fintech is Transforming Financial Services". *Journal of Financial Innovation*. (2018).

transformation era and ensure that digitally connected financial infrastructure remains safe, reliable and dependable to support sustainable economic growth and national security.

In Indonesia, Fintech is regulated in Law Number 4 of 2023 concerning the development and strengthening of the financial sector. The previous fintech regulation was only listed at a lower regulatory level, such as financial services authority regulation 10/POJK.05/2022 concerning information technology-based joint funding services. Likewise, we can see the regulation of the minister of communication and information number 10 of 2021 concerning amendments to the minister of communication and information number 5 of 2020 concerning the implementation of private electronic systems.

This research wants to explore the efforts that have been made by countries in dealing with the impact of Fintech on security. A comprehensive cyber defense strategy and careful regulation of digital financial services are priorities for the government to face this challenge. Collaboration between governments, financial institutions, and Fintech companies is also important in creating a robust security ecosystem. By combining economic and security aspects, this research provides a holistic view of the impact of Fintech on the country's security system.⁸

METHODS OF THE RESEARCH

This research uses a qualitative method with a descriptive analysis approach. According to Strauss and Corbin, qualitative research can be used to study people's lives, history, behavior, and functions of organizations, social movements, or kinship relationships that produce discoveries that cannot be achieved using statistical procedures or quantitative methods.⁹ This research focuses on qualitative methods and is researched to see the extent of the challenges posed by fintech to the country's resilience system. The approach method used in the preparation of this research is normative juridical research (normative legal research method) too. The normative juridical research method is library legal research conducted by examining library materials or secondary data only. Thus the object analyzed with a qualitative approach is a research method that refers to the legal norms contained in the laws and regulations.¹⁰ The researcher chose a qualitative approach through detailed data collection from information sources. The data obtained comes from sources related to the object of literature review. This method is used to find a broad view of various information relevant to the object under study through published data such as publications of international organizations, journals, books, academics, and university reports, as well as official documents related to fintech.

RESULTS AND DISCUSSION

A. The Influence of Fintech on the Country's Economic Potential

The influence of Fintech on a country's economic potential has become an important topic in the digital transformation era. Fintech has brought about significant changes in the financial sector, opening up new opportunities and driving financial inclusion. Fintech has become a transformational force in the financial sector worldwide. Fintech innovation has

⁸ Tan, S. "Money Laundering and Terrorism Financing Risks in the Age of Fintech". *Journal of Financial Crime*. (2018)

⁹ Nugrahani, F, *Metode Penelitian Kualitatif*. (Solo: Cakra Books, 2014).

¹⁰ Soerjono Soekanto and Sri Mahmudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, (Jakarta: Raja Grafindo Persada, 2003), p.

brought about significant changes and created new opportunities that are changing the way business and financial transactions are conducted. Digital technology and mobile applications have facilitated economic growth and expanded access to financial services for various levels of society, known as financial inclusion.¹¹

Fintech has shaped the financial sector by creating efficiencies and convenience that cannot be ignored. Financial transactions can be carried out quickly and easily through Fintech platforms, reducing operational costs and increasing accessibility for communities previously marginalized from the conventional financial system. In addition, Fintech has opened up new opportunities for business innovation and business models that were previously unthinkable. Fintech startups and companies have created financial products and services that galvanize traditional industries to innovate and adapt. No less critical, Fintech has become a major driver in efforts to realize financial inclusion. Through the application of technology and affordable digital financial services, Fintech has brought financial services to those previously difficult to reach by traditional financial institutions.¹² The ability to open accounts, access loans and make digital payments has increased people's financial empowerment and reduced economic inequality.

However, despite the benefits, using Fintech also raises several challenges, such as data security risks, consumer protection and regulatory imbalances. In this context, addressing regulatory and safeguard issues is key to ensuring that Fintech can deliver economic benefits and financial inclusion sustainably and responsibly. Fintech has brought about a paradigm shift in the financial sector, opening up new opportunities and strengthening financial inclusion. By remaining focused on innovation, efficiency and equal access, Fintech has the potential to become a driving force for sustainable and inclusive economic growth for society globally.¹³

The following is an analysis of the influence of Fintech on the country's economic potential: a) Increasing Accessibility of Financial Services: Fintech has enabled the accessibility of financial services for communities that were previously difficult to reach by traditional financial institutions. Through mobile applications and online platforms, Fintech provides banking, digital payment, and investment services to individuals and small businesses without relying on physical infrastructure such as bank branches. Case in point: Fintech companies like Ant Financial (Alipay) in China have enabled access to financial services for millions of rural residents who do not have access to traditional banking; b) Driving Financial Inclusion and Economic Growth: Fintech has increased financial inclusion in various countries by enabling digital financial transactions and services. Greater financial inclusion opens up opportunities for more people to access financial services, such as credit, savings and insurance, supporting economic growth through greater consumption and investment. Case in point: In India, Fintech companies like Paytm have provided access to financial services to millions of previously unbanked citizens; c) Facilitating the Growth of Small and Medium Enterprises (SMEs): Fintech has supported the growth of SMEs through online loan services and peer-to-peer lending platforms. SMEs can access funds more easily and quickly, allowing them to increase production, expand their business and create new

¹¹ Wong, M. "Data Security and Consumer Protection in the Era of Fintech". *Journal of Financial Technology*, (2020). Read A H Ilman, G Noviskandariani, and Nurjihadi, M. "Peran Teknologi Finansial bagi Perekonomian Negara Berkembang". *Jurnal Ekonomi Dan Bisnis Indonesia*, 4 no 1 (2019).

¹² Deloitte. (2020). Cybersecurity in Fintech: Addressing New and Evolving Threats. <https://www2.deloitte.com/global/en/pages/financial-services/articles/cybersecurity-in-fintech.html>

¹³ Wong, M. Data Security and Consumer Protection in the Era of Fintech. *Journal of Financial Technology*. (2020)

jobs. Case in point: In Kenya, Fintech company M-Pesa has provided microloan services to SMEs and helped improve economic prosperity in rural areas; d) Increasing Efficiency and Productivity: Fintech has brought technological innovations that increase efficiency and productivity in the financial sector. Artificial intelligence technology, extensive data analysis and blockchain technology have reduced operational costs and accelerated business processes, resulting in significant economic benefits. Case in point: Blockchain technology has been used in the logistics and supply chain industry, such as in Singapore, to increase efficiency and transparency in logistics and distribution processes

The influence of Fintech on the country's economic potential is very positive. Through increasing the accessibility of financial services, encouraging financial inclusion, facilitating the growth of SMEs, and increasing efficiency, Fintech has brought broad economic benefits. However, it should be remembered that Fintech development must also be balanced with efforts to mitigate cyber security risks and consumer protection to ensure its sustainability and positive impact on economic growth and country stability.

B. The Regulation about Fintech in Indonesia

We can read some regulations in Indonesia. For example, Henri Christian Pattinaja wrote about Regulation of Financial Technology In Indonesia. This study concludes that the evolution of FinTech seen lately actually began with the innovation of credit cards in the 1960s, debit cards and terminals that provide cash, such as Anjungan Tunai Mandiri, ATMs in the 1970s. Then the credit card era was followed by the emergence of phone banking in the 1980s and various financial products following the deregulation of capital and bond markets in the 1990s. Next came internet banking which then encouraged branchless banking and long distance banking activities. Next, mobile technology emerged to facilitate financial transactions. And finally e-wallet technology emerged, with two companies known in Indonesia as Go-Pay and OVO. The legal protection itself is embodied in the Law of the Republic of Indonesia No. 7 of 2014 on Trade, Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, Law of the Republic of Indonesia No. 8 of 1999 on Consumer Protection, and Law of the Republic of Indonesia No. 7 of 2011 on Currency. The latest additional regulatory protection from Bank Indonesia itself is by issuing Bank Indonesia Regulation No.19/12/PBI/2017 on the Implementation of Financial Technology.¹⁴

The journal entitled Legal Protection of Financial Technology Consumer Data Security in Indonesia was written by Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono. The results of his research state that legal protection of personal data of Fintech consumers is regulated by the Ministry of Communication and Information of the Republic of Indonesia through Minister of Communication and Information Regulation Number 20 of 2016, by OJK through POJK No. 77 of 2016, POJK No. 13 of 2018 and its implementing regulations, namely OJK Circular Letters. Data that must be protected: 1) Individual personal data. 2) Corporate personal data. 3) Material non-public data and information. 4) Data and information related to financial transactions. 5) Data and information related to contracts/agreements.¹⁵

¹⁴ Henri Christian Pattinaja. "Pengaturan Hukum Financial Technology di Indonesia", *SELISIK* 7, no 2 (2021). Abubakar, L., & Handayani, T. *Financial Technology: Legal Challenges for Indonesia Financial Sector*, (2018).

¹⁵ Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono, "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology di Indonesia", *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (2019).

Journal entitled “Regulation of Financial Technology (Fintech) in Indonesia” written by Baginda Persaulian. In this research, he explained that the existence of a company that organizes financial technology (Fintech) causes confusion in choosing a company that suits their needs. One of the most important considerations that must be considered by the public is legality. Public understanding is caused by public knowledge about financial technology (Fintech), literature and socialization that discusses financial technology regulations (Fintech) and socialization, especially regarding regulations, is still limited. Therefore, the purpose of this paper is to provide an overview and understanding of the regulation of financial technology (Fintech) in Indonesia.¹⁶

The journal was written by Diva Salasa Anastasia with the title Urgency of Fintech Law Formation to Provide Legal Protection to Consumers in Online Loans. This research explains that this Fintech (Online Loan) Business has potential vulnerabilities such as. First, in the payment process, consumer data (banking and personal) will be entered into the database of the service provider company, it is feared that there will be data loss carried out by irresponsible parties; Second, not only Indonesian citizens, but foreign citizens can also register themselves as investors, if there are efforts to resolve disputes, the provisions between countries and service provider companies must be considered properly; Third, information on credit assessment procedures and procedures by service provider companies still has shortcomings in explaining the entire process and there is also no guarantee by insurance,¹⁷ and the last, it's about the importance of strengthening regulations to accelerate digital transformation in Indonesia, both in the banking sector and others.¹⁸

C. The Influence of Fintech on Digital Defense Strategy

The influence of Fintech on digital defense strategies has become an essential issue in the era of digital transformation and rapid growth of the financial technology industry. Fintech has brought fundamental changes in how financial transactions and services are carried out. Still, its impact has also created new challenges in maintaining the security and integrity of the country's financial system. Fintech has driven innovation in technological security, including the application of biometric technology, strong data encryption, and artificial intelligence in detecting and preventing cyber threats. Case in point: Fintech company PayPal uses advanced security systems to protect their transactions and user data. In some cases, Fintech has enabled the accessibility of increased security for consumers by providing easy-to-use security solutions, such as two-factor verification to protect user accounts. Case in point: Fintech banking apps like Revolut use two-factor verification via smartphones to secure user account access.

Fintech collects and stores sensitive user data, including financial and personal information. This increases the potential risk of data leaks and privacy breaches if the security system is not strong enough. Case example: Cases of data leaks in online loan-based Fintech applications have resulted in identity theft and misuse of users' personal information. Attacks on Fintech Infrastructure: Due to its reliance on digital technology, the

¹⁶ Baginda Persaulian, “Regulasi Teknologi Finansial (Fintech) di Indonesia”, *Jurnal Fundamental* 10, no 2 (2021).

¹⁷ Diva Salasa Anastasia, “Urgensi Pembentukan Hukum Fintech Untuk Memberi Perlindungan Hukum Kepada Konsumen Dalam Pinjaman Online”, *Jurnal Hukum dan HAM Wara Sains* 2 no. 2; 136-151. Basuki, F. H., & Husein, H. “Analisis SWOT Financial Technology Pada Dunia Perbankan Di Kota Ambon”. *Manajemen dan Bisnis*, 2 (2018).

¹⁸ L. Abubakar, and Handayani, T. “Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan di Era Ekonomi Digital”. *Masalah-Masalah Hukum*, 51 no. 3 (2022): 259-270.

Fintech industry is a potential target for cybercriminals for attacks such as ransomware or DDoS attacks that can disrupt operations and harm the country's economy. Case in point: Ransomware attacks on digital payment platforms can result in service disruptions and financial losses for users and service providers.

Countries must increase efforts to ensure that Fintech companies have high security standards in protecting user data and transactions. Strict regulations and security standards must be enforced to ensure the safety of infrastructure and data. Collaboration between governments, financial institutions, and Fintech companies is essential to share intelligence about security threats and confront them together. Effective information exchange can help identify and address threats more quickly and efficiently. Digital security education and awareness must be increased among Fintech users so that they are more aware of the risks and actions to take to protect themselves and their personal information.

The influence of Fintech on digital defense strategies has both positive and negative aspects. While Fintech has driven technological security innovation, it has also increased the potential for threats to data and infrastructure.¹⁹ To deal with the complex impacts of Fintech, digital defense strategies must include strengthening system security, collaboration, and information exchange, as well as security education and awareness. Only through integrated and holistic efforts can countries optimally exploit the potential of Fintech while maintaining the security and integrity of the national financial system.²⁰

D. Security Threats from Using Fintech

The use of Fintech has brought significant benefits in expanding the accessibility of financial services and increasing the efficiency of financial transactions.²¹ However, like other technologies, Fintech also presents various security threats that must be considered. In this analysis, we will highlight several potential security threats from using Fintech along with relevant case examples.

There are several security threats from the use of Fintech, including:²² a) Data Leaks and Privacy Breach: Fintech use involves exchanging sensitive data, including financial and personally identifiable information. The threat of data leaks or privacy violations can lead to identity theft, fraud, or misuse of user data. Case in point: In 2017, Fintech credit company Equifax experienced a data breach that resulted in the personal information of more than 147 million people being exposed; b) Phishing and Malware Attacks: Cybercriminals often use phishing and malware attacks to steal Fintech users' login and password information. They can send fake emails or text messages that appear genuine to lure victims into disclosing sensitive information. Case in point: Phishing attacks on Fintech banking applications have resulted in the loss of funds and users' personal data; c) Ransomware and Data Hostage: Ransomware attacks can hold data hostage and threaten to release it to the public unless a ransom is paid. These threats can cause financial and reputational losses for victimized Fintech companies. Case in point: In 2020, Fintech insurance company CNA Financial fell victim to a ransomware attack that disrupted their operations; d) DDoS Attacks and Service Disruption: DDoS (Distributed Denial of Service) attacks can cause

¹⁹ Zavarsky, P., Kekelyova, P., & Ondrus, J. "Cybersecurity in Fintech: A Systematic Literature Review". *Computers & Security*, 82, (2019): 199-211.

²⁰ CNN Business. *Colonial Pipeline Ransomware Attack*. (2021).

²¹ CNA Financial. (2020). *Cybersecurity Incident*. Diakses dari <https://www.cna.com/web/guest/cybersecurity-incident>

²² European Banking Authority. (2021). *The Impact of FinTech on Payment Institutions' and E-Money Institutions' Business Models*. <https://eba.europa.eu/eba-report-impact-fintech-payment-institutions-and-e-money-institutions-business-models>

service disruptions and result in downtime on Fintech platforms. Cybercriminals or competitors can carry out these types of attacks to damage a company's reputation or cause financial losses. Case in point: In 2016, a DDoS attack caused service disruption on the financial services platform Fintech Lending Club.

Meanwhile, strategies for overcoming security threats from the use of Fintech can be carried out by:²³ a) Strengthening System Security: Fintech companies must implement solid technological security measures, including data encryption, two-factor verification, and suspicious activity monitoring, to protect sensitive information and prevent security threats; b) User Education: Increasing security awareness among Fintech users is essential. Companies must educate users about good security practices and how to identify fraud attempts; c) Collaboration with Security Experts: Fintech companies must collaborate with cybersecurity experts to identify and address potential security threats. They must also continually update their systems and infrastructure to meet evolving threats.

The use of Fintech brings various security threats that need to be addressed seriously. Data leaks, phishing attacks, ransomware, and service disruptions are potential threats that can harm Fintech companies and their users. By strengthening system security, educating users, and collaborating with security experts, Fintech companies can reduce risks and create a safer environment for digital financial transactions.

E. Fintech Efforts to Improve Digital Defense to Face Fintech Challenges

The rapid influence of Fintech has brought new challenges in digital defense for the financial system. In response to the growing complexity of threats, relevant parties, including governments, financial institutions, and Fintech companies, have sought to improve digital defenses to protect financial infrastructure and user information²⁴. This abstract reviews the efforts made to improve digital defense as well as relevant case examples. Several efforts to improve digital defense include:²⁵ a) Enforcement of Regulations and Security Standards: Governments and regulatory bodies play an essential role in implementing strict security rules and standards for Fintech companies. These regulations include protecting users' data, preventive measures against cyber attacks, and requirements for using advanced security technologies; b) Collaboration and Information Exchange: Collaboration between financial institutions, Fintech companies, and cybersecurity parties forms the foundation for the exchange of intelligence about detected cyber threats and attacks. By sharing information, relevant parties can jointly face and overcome threats that may impact the financial sector; c) Investments in Security Technology and Cybersecurity Policies: Financial institutions and Fintech companies should increase investment in cutting-edge security technologies, such as artificial intelligence solutions and advanced analytics, to detect suspicious behavior and unexpected cyberattacks. In addition, companies must also design a comprehensive cybersecurity security policy to reduce potential risks.

Some examples of cases of efforts by several countries to improve digital defenses in facing financial challenges include (Bangladesh Bank Cyber Heist: Timeline of Events, 2016): a) The Bangladesh Bank Heist: In 2016, a cyberattack through Bangladesh Bank's Fintech

²³ Financial Fraud and Cyber Threats in the Age of Fintech. (2021). *Europol*. <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/financial-fraud-and-cyber-threats-in-age-of-fintech>

²⁴ McKinsey Global Institute. *Digital Finance for All: Powering Inclusive Growth in Emerging Economies*, (2019).

²⁵ Miller, A. & Selvadurai, V. "Cybersecurity Risks and Mitigation for Financial Technology (FinTech) Companies". *Journal of Corporate Accounting & Finance*, 32 no. 4 (2020): 116-122.

banking network resulted in the theft of funds amounting to 81 million dollars. The attackers used Fintech banking software to manipulate financial transactions and transfer funds to personal accounts in various countries. This incident highlights the importance of strengthening digital defenses to protect the country's financial system from detrimental cyber attacks; b) Cyber Threats to Digital Payment Platforms: Fraud and phishing attacks on digital payment platforms such as PayPal and Alipay have increased in recent years. These attacks target user information, including credit card and bank account data, to steal funds or access personal information.

In the face of growing Fintech challenges and cybersecurity threats, improving digital defenses is critical to protecting financial systems and user information from potential risks. Relevant parties strive to create a safe, reliable, and trustworthy financial ecosystem for all stakeholders through regulatory enforcement, collaboration, and investment in advanced security technology.

F. Potential Development of Fintech in the Future and Its Impact on National Security

Fintech has been a transformational force in the financial industry, and its potential for continued growth offers significant opportunities and challenges for national security. This abstract investigates the potential future development of Fintech and its impact on national security by considering the cyber security challenges that may arise. Fintech continues to drive innovation in financial services by utilizing the latest technologies, such as artificial intelligence, blockchain, and the Internet of Things (IoT). The potential for this technological development can create more efficient and affordable financial services and expand financial accessibility for the entire community.²⁶

Fintech is expected to become increasingly integrated in various economic sectors, such as international trade, health, transportation, and logistics. This has the potential to open up new economic opportunities but also increases complexity and security risks to the country's critical infrastructure. With the rapid growth of Fintech, data security risks are becoming increasingly complex. Data leaks and cyber attacks on Fintech companies can result in financial losses and damage public confidence in the security of the country's financial system. The potential development of Fintech technology can also be misused by irresponsible parties for criminal purposes, including money laundering, terrorism financing, and other illegal activities. Strict supervision and regulation are needed to address these risks.²⁷

In 2021, a DarkSide ransomware attack targeted the Colonial Pipeline in the United States, causing fuel pipeline closures and disrupting supplies in several regions.²⁸ This attack shows how the security of critical infrastructure, including the financial sector that countries rely on, can be threatened by cyberattacks. Another case of the increasing popularity of peer-to-peer (P2P) lending platforms in Fintech has attracted the attention of fraudsters to commit fraud or misuse funds from borrowers and investors. This kind of fraud has harmed many people and requires more robust security measures to prevent it.²⁹

²⁶ Xiang, L., & Meng, Q. "A Review of Cybersecurity Threats and Defense Strategies for Fintech Ecosystems". *IEEE Transactions on Services Computing*, 14 no. 3 (2021): 601-615.

²⁷ World Bank. (2021). *The Global Findex Database 2021: Measuring Financial Inclusion and the Fintech Revolution*. <https://globalfindex.worldbank.org/>

²⁸ International Telecommunication Union. (2020). *Global Cybersecurity Index 2020*.

²⁹ World Economic Forum. (2021). *Cybersecurity: An Essential Opportunity for Fintech and Blockchain*. <https://www.weforum.org/agenda/2021/01/cybersecurity-an-essential-opportunity-for-fintech-and-blockchain/>

Fintech's potential for future development offers excellent economic opportunities but also presents security challenges for the country. In dealing with the impact on national security, cooperation between the government, financial institutions, and Fintech companies is the key to creating a safe, reliable, and sustainable Fintech ecosystem.³⁰ Strict monitoring, investment in the latest security technologies, and increased awareness of cybersecurity threats will be essential steps to face challenges that may arise in the future.

CONCLUSION

Fintech has become a transformational force in the financial sector by bringing significant changes, including economic potential and digital defense strategy challenges for the country. In this conclusion, a comprehensive picture of the impact of Fintech on the state security system will be presented. Fintech has opened up new economic opportunities by encouraging financial inclusion, increasing the accessibility of financial services, and stimulating innovation in various economic sectors. The increasing use of Fintech also presents digital defense strategy challenges for the country. Data security threats, cyber-attacks, and misuse of financial technology can damage the country's financial infrastructure, threaten the financial system's stability, and pose national security risks. Therefore, there needs to be severe efforts from governments, financial institutions, and Fintech companies to improve digital defense. The government needs to implement strict regulations to protect the data and privacy of Fintech users, as well as closely monitor the operations of Fintech companies to reduce the risk of misuse of financial technology. Fintech has significantly impacted the country's security system, with significant economic potential and complex digital defense strategy challenges. By recognizing the potential and challenges, the government and relevant stakeholders must work together to create a safe, reliable, and sustainable Fintech environment for the country's overall economic progress and security.

REFERENCES

- A H Ilman, G Noviskandariani, and Nurjihadi, M. "Peran Teknologi Finansial bagi Perekonomian Negara Berkembang". *Jurnal Ekonomi Dan Bisnis Indonesia*, 4 no 1 (2019).
- Baginda Persaulian, "Regulasi Teknologi Finansial (Fintech) di Indonesia", *Jurnal Fundamental* 10, no 2 (2021).
- Basuki, F. H., & Husein, H. "Analisis SWOT Financial Technology Pada Dunia Perbankan Di Kota Ambon". *Manajemen dan Bisnis*, 2 (2018).
- CNA Financial. (2020). *Cybersecurity Incident*. Diakses dari <https://www.cna.com/web/guest/cybersecurity-incident>.
- CNN Business. *Colonial Pipeline Ransomware Attack*. (2021).
- Chen, A. "Proactive Cybersecurity Strategies: Collaboration and Intelligence Sharing". *Cybersecurity Policy Review*, (2019).
- Deloitte. (2020). *Cybersecurity in Fintech: Addressing New and Evolving Threats*. <https://www2.deloitte.com/global/en/pages/financial-services/articles/cybersecurity-in-fintech.html>.

³⁰ Kaspersky. *Fintech and the Future of Cybersecurity: Protecting the Financial Industry in the Age of Fintech*, (2020).

- Diva Salasa Anastasia, "Urgensi Pembentukan Hukum Fintech Untuk Memberi Perlindungan Hukum Kepada Konsumen Dalam Pinjaman Online", *Jurnal Hukum dan HAM Wara Sains* 2 no. 2,: 136-151.
- European Banking Authority. (2021). *The Impact of FinTech on Payment Institutions' and E-Money Institutions' Business Models*. <https://eba.europa.eu/eba-report-impact-fintech-payment-institutions-and-e-money-institutions-business-models>.
- Financial Fraud and Cyber Threats in the Age of Fintech. (2021). *Europol*. <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/financial-fraud-and-cyber-threats-in-age-of-fintech>.
- Henri Christian Pattinaja. "Pengaturan Hukum Financial Technology di Indonesia", *SELISIK* 7, no 2 (2021).
- International Telecommunication Union. (2020). Global Cybersecurity Index 2020.
- Johnson, E. "Regulating Fintech for Security: A Policy Approach". *International Journal of Financial Regulation*. (2017).
- Kaspersky. *Fintech and the Future of Cybersecurity: Protecting the Financial Industry in the Age of Fintech*. (2020).
- Kim, D, "The Cybersecurity Challenges of Fintech Adoption". *Journal of Cybersecurity*. (2019).
- Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono, "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology di Indonesia", *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (2019).
- L. Abubakar, and Handayani, T. "Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan di Era Ekonomi Digital". *Masalah-Masalah Hukum*, 51 no. 3 (2022): 259-270.
- Lee, S. "The Impact of Fintech on Financial Inclusion: Evidence from Emerging Markets". *Journal of Economic Perspectives*, (2020).
- McKinsey Global Institute. *Digital Finance for All: Powering Inclusive Growth in Emerging Economies*, (2019).
- Miller, A. & Selvadurai, V. "Cybersecurity Risks and Mitigation for Financial Technology (FinTech) Companies". *Journal of Corporate Accounting & Finance*, 32 no. 4 (2020): 116-122.
- Nugrahani, F, *Metode Penelitian Kualitatif*. (Solo: Cakra Books, 2014).
- Soerjono Soekanto and Sri Mahmudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, Jakarta: Raja Grafindo Persada, 2003.
- Tan, A. "The Evolution of Fintech: A Comprehensive Analysis". *Journal of Financial Innovation*. (2019).
- Tan, J. "Cybersecurity Challenges in the Age of Fintech: An Analysis of Emerging Threats". *Journal of Cybersecurity Studies*. (2021).
- Tan, S. "Money Laundering and Terrorism Financing Risks in the Age of Fintech". *Journal of Financial Crime*. (2018).

- Wong, A. "The Efficiency Revolution: How Fintech is Transforming Financial Services". *Journal of Financial Innovation*. (2018).
- Wong, M. Data Security and Consumer Protection in the Era of Fintech. *Journal of Financial Technology*. (2020).
- World Bank. (2021). *The Global Findex Database 2021: Measuring Financial Inclusion and the Fintech Revolution*. <https://globalfindex.worldbank.org/>.
- World Economic Forum. (2021). *Cybersecurity: An Essential Opportunity for Fintech and Blockchain*. <https://www.weforum.org/agenda/2021/01/cybersecurity-an-essential-opportunity-for-fintech-and-blockchain/>
- Xiang, L., & Meng, Q. "A Review of Cybersecurity Threats and Defense Strategies for Fintech Ecosystems". *IEEE Transactions on Services Computing*, 14 no. 3 (2021): 601-615.
- Zavarsky, P., Kekelyova, P., & Ondrus, J. "Cybersecurity in Fintech: A Systematic Literature Review". *Computers & Security*, 82, (2019): 199-211.

Conflict of Interest Statement: The author(s) declares that research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest,

Copyright: © AUTHOR. This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. (CC-BY NC), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

SASI is an open acces and peer-reviewed journal published by Faculty of Law Universitas Pattimura, Ambon, Indonesia.

