Formosa Journal of Social Sciences (FJSS)
Vol.4, No.2, 2025: 263-280

Reformulation of Digital Protection Against Loan Crime Illegal Online as a Pillar of National Defense in the Cyber Era

Adelisca Pramesti[1*], Hikmat Zakky Almubaroq[2], Editha Praditya Duarte[3]
Republic of Indonesia Defense University, Jakarta
Corresponding Author: Adelisca Pramesti pramesti.adelisca@gmail.com

ARTICLEINFO

Keywords: Illegal Online Loans, Cyber Protection Strategy, National Defense, Institutional Synergy, National Morale

Received : 9 April
Revised : 16 May
Accepted: 22 June

ABSTRACT

The phenomenon of illegal online lending crime in Indonesia has developed into a multidimensional threat that damages the economic, psychological, and social structures of society. This study aims to formulate an adaptive digital protection strategy as an integral part of the national defense system in the cyber era. The main problems identified include the increasing number of illegal lending entities, weak financial literacy of the community, and dysfunctional coordination between institutions in handling digital crimes. Through the literature review method, this study examines empirical data from state institutions, investigative reports, and digital propaganda theory to identify communication patterns used by illegal lenders. Propaganda strategies such as glittering generalities, emotional appeal, repetition, influencers, bandwagon, and the use of fraud have proven effective in misleading the public, especially the productive age group with low digital literacy. The main findings of this study indicate that weak institutional synergy and low protection of personal data are crucial factors in fostering the digital crime ecosystem. The proposed reformulation of digital protection includes strengthening cyber regulations, integrating cross-sector reporting systems, and increasing community-based digital literacy. This study recommends the formation of a National Task Force, ratification of the Illegal Fintech Law, and digital literacy education as preventive efforts. With a multidimensional approach, digital protection is not only a technical defense tool but also a reflection of the nation's capacity to maintain an inclusive and sustainable national defense

DOI: https://doi.org/10.55927/fjss.v4i2.370
ISSN-E: 2830-0246
https://mryformosapublisher.org/index.php/fjss

INTRODUCTION

Illegal online lending crime in Indonesia is one of the strategic threats that has emerged in the current era of digital transformation. Propaganda of illegal loan offers spread through social media, short messages, and unofficial applications targets groups of people with low financial literacy. This condition causes various risks, ranging from threats, violence, and the spread of borrowers' personal information as a form of gender-based abuse (Puteri et al., 2023:5-6). On a macro level, these crimes have the potential to disrupt the stability of public trust in the national digital ecosystem. Therefore, risk management through digital protection reformulation is very important in the context of strengthening national defense.

The escalation of illegal online lending crimes in Indonesia is increasingly worrying, with the numbers continuing to increase. Based on the Financial Services Authority (OJK) report, in the period from June to July 2024, the PASTI Task Force blocked 1,001 illegal financial entities, consisting of 850 illegal online loan applications and 59 illegal personal loan offering content (Financial Services Authority, 2024). From 2017 to July 31, 2024, the total number of illegal financial entities stopped reached 10,890, including 9,180 illegal online lending and personal lending (pinpri) entities and 1,459 illegal investment entities (National Digitization Commission, 2004). In addition, the PASTI Task Force also blocked 65 illegal investment offers that used fraudulent methods by imitating the names, sites, or social media of licensed entities (Financial Services Authority, 2024). This data shows the scale of the problem faced in overcoming the rampant illegal online loans operating without official permits in Indonesia.

LITERATURE REVIEW

Responding to the increasing status of number of illegal online loan crimes in Indonesia, the urgency of compiling a digital protection strategy against illegal online loan crimes needs to be accelerated. A digital protection strategy against illegal online loan crimes must be designed as a main component of a national defense system that is responsive to the complexity of today's cyber threats. It is not enough to just have a repressive approach in the form of blocking illegal entities; the state needs to build a proactive digital security policy in digital defense by strengthening the entire ecosystem against potential violations and exploitation (Victor-Mgbacchi, 2024:74). On the other hand, the cybersecurity approach must not be separated from the principles of human rights and personal data protection so as not to give birth to digital authoritarianism. Digital authoritarianism undermines democracy and human rights by allowing governments to control the flow of information, so that they can silence criticism and suppress online opposition (Sherman, 2021:107; Heister & Yuthas, 2022:35). Such as the implementation of regulatory strengthening that can reach new crime modes, increasing interoperability between institutions, and utilizing artificial intelligence for early detection and risk mitigation.

In this context, government agencies organize advisory, monitoring, and information exchange agendas on cybersecurity threats to keep organizations informed about new attack techniques, real-time. Multi-party synergy as strategic partners for supervision will create an inclusive national digital governance model by building a system run by its designers and builders, supported by technology and resource suppliers, operated by operators, driven by key supporters, funded by sponsors, and under the full responsibility of its owners (Tate & Lofgren, 2023:2). In this cyber era, every individual has a role as a "defense actor" who is able to protect themselves and their environment from digital threats. Thus, digital protection is not only a technical instrument, but also a reflection of the nation's capacity to build a comprehensive and sustainable national defense.

This article identifies how digital propaganda from illegal online lending crimes targets people with low financial literacy through various online channels, accompanied by inhumane debt collection practices and illegal distribution of personal data, conditions that create serious mental stress and open up space for the spread of disinformation and agitation that threaten social stability. Weak coordination between related institutions, such as financial institutions, law enforcement, and security, shows institutional dysfunction that creates loopholes for cybercriminals to continue operating and indirectly weakens the legitimacy and public trust in the national security system. For this reason, the state defense strategy must be directed at strengthening digital protection that includes improving the cybersecurity system, adaptive digital regulations, and public digital literacy in order to build a collective psychological and moral defense. Integrated digital protection not only protects the country's strategic infrastructure and data but also acts as a bulwark against the erosion of information sovereignty and social stability.

Considering the complexity of the threat of illegal online loans, the reformulation of digital protection must include three main aspects: adaptive regulation, strengthening cyber infrastructure, and increasing digital literacy of the community. Adaptive regulation is needed to respond to new modus operandi that continue to develop in the digital realm, including strict law enforcement against the perpetrators and platforms involved. Strengthening cyber infrastructure is important to ensure that the national digital system can ward off attacks and infiltration from illegal actors. Meanwhile, increasing digital literacy is crucial so that the community can recognize, avoid, and report illegal online lending practices. Through this multidimensional approach, it is hoped that it can provide strategic recommendations for the development of digital defense and security policies in Indonesia. At the same time, Indonesia can strengthen its strategic position at the regional and global levels. It is hoped that these efforts will be able to maintain national sovereignty and stability in the face of future cyber challenges.

METHODOLOGY

This research method uses an approach of literature review by processing and analyzing data from various academic sources and current policies related to illegal online loan propaganda and integrated digital protection. Primary data in the form of theories and concepts of propaganda techniques were taken from previous studies such as Russo et al. (1981), McClintock (2005), Lee & Hong (2016), Donnellan (2016), Kang & Ma (2020), and Pereira (2023). The analysis was conducted to identify the patterns and propaganda strategies used in illegal online loan marketing, as well as the social and economic implications arising from these practices.

In addition, this study also refers to data on policies and integrated digital protection approaches as pillars of national defense processed from Raieste et al. (2024). This approach includes institutional strategic dimensions, digital infrastructure security, and technological risk mitigation, which are the framework for understanding policy synergies in dealing with digital threats from illegal online loans. Thus, this study integrates theoretical and policy studies as a basis for a comprehensive analysis of the issues raised.

RESULT AND DISCUSSION

Illegal Online Loan Propaganda Crime

Digital transformation in Indonesia brings with it new threats in the form of non-traditional crimes, one of which is through illegal online loan propaganda. The form of illegal online loan propaganda is usually in the form of advertisements that promise easy and fast access to funds without collateral, often spread through social media, short messages (SMS), and unofficial third-party applications (Tempo.co, 2021). They also use personalized messaging tactics that adapt to the profile of potential victims, leveraging illegally obtained personal data. In addition, there is the spread of fake testimonials and deceptive low-interest claims, so that people with low financial literacy are easily attracted and trapped (Antara News, 2023). This phenomenon shows that the spread of illegal online loan propaganda has become a form of systemic and structured digital crime.

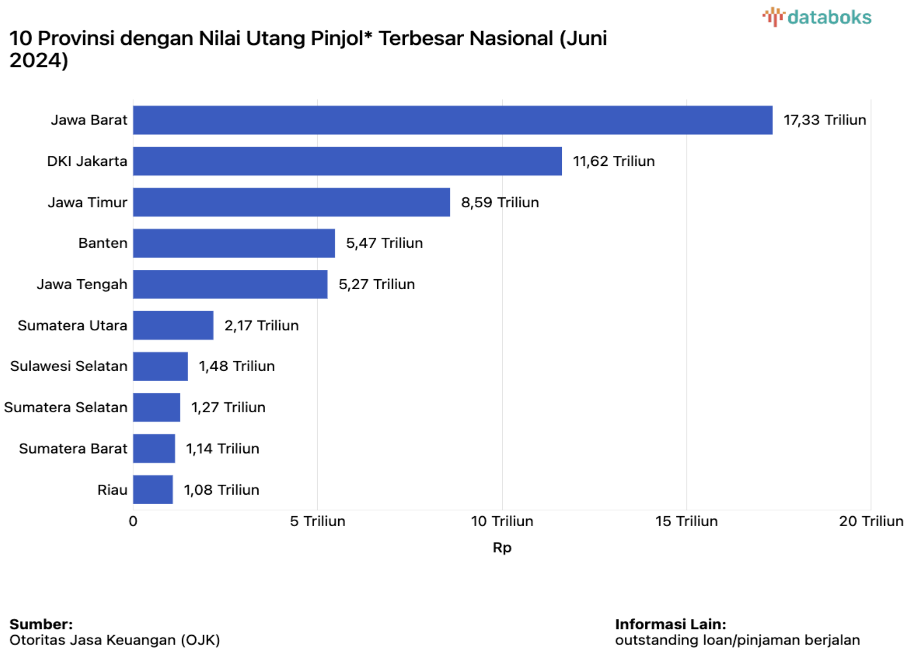

Figure 1. Demographic Mapping of the Population Related to Value Levels

The Largest Online Credit Debt is Spread Across 10 Provinces in Indonesia

Based on the geographical distribution report by Katadata Insight Center (2024), Illegal online loan cases also show a striking pattern in certain regions. In mid-2024, West Java recorded the highest online loan debt value in Indonesia, reaching IDR 17.33 trillion or around 26% of the total national outstanding loan of IDR 66.99 trillion. The next position was occupied by DKI Jakarta with IDR 11.62 trillion and East Java with IDR 8.59 trillion. Other provinces in the top ten include Banten (IDR 5.47 trillion), Central Java (IDR 5.27 trillion), North Sumatra (IDR 2.17 trillion), South Sulawesi (IDR 1.48 trillion), South Sumatra (IDR 1.27 trillion), West Sumatra (IDR 1.14 trillion), and Riau (IDR 1.08 trillion). This debt distribution shows a high concentration in the Java Island region, reflecting the high penetration of digital services and the financial needs of urban communities. Meanwhile, West Papua recorded the lowest online loan debt value, at IDR 74 billion, followed by North Kalimantan with IDR 83 billion and North Maluku with IDR 105 billion. This data highlights the importance of strengthening financial literacy and monitoring illegal online lending practices, especially in provinces with high debt levels.

From a demographic perspective throughout 2018-2023, the victims were the productive age group, namely the 37-46 year old age group being the largest category of online loan victims, while the 17-26 year old and 27-36 year old age groups showed almost the same level of involvement (Ngafifah et al., 2024:71). Data from the Financial Services Authority (OJK) through the PASTI Task Force shows that of the total 15,162 complaints about illegal online loans in 2024, certain age groups contributed 6,348 complaints, while the 17-25 age group was the third largest group with 3,476 complaints (Antara News, 2025). The trend of bad credit for online loans does fluctuate, but the 19-34 age group still dominates with around 301 thousand accounts experiencing TWP90 since the beginning of 2024 and a total outstanding balance reaching IDR 729.6 billion (CNN Indonesia, 2024). These findings indicate that the burden and risk of online loans are mostly borne by the productive age group, so policy interventions are needed that not only focus on financial aspects but also pay attention to integrated digital protection strategies.

This phenomenon indicates that the younger generation, who should be in a productive phase and building financial stability, is vulnerable to the trap of illegal online loans. The dominant factors are financial literacy and economic pressure (Putri & Rinaldi, 2022:102-103), along with easy access to digital loan services without a deep understanding of legality and risk, which are the main causes of this vulnerability. Therefore, more intensive financial education and literacy efforts are needed for the productive age group to prevent the negative impacts of using illegal online loans.

In examining the propaganda strategy of illegal online loans, it is necessary to understand how online loans utilize marketing techniques that resemble propaganda. This can determine how the process of forming the perception that they are a quick and easy solution to financial problems. The following researchers conduct an analysis of propaganda with a literature review of rhetorical strategies in digital advertising, especially those used by illegal online loan providers.

Table 1. Techniques and Strategies of Illegal Online Loan Propaganda in Indonesia

Propaganda Techniques	Definition of Propaganda Techniques	Propaganda Strategy Illegal Online Loans	Implications of Propaganda Strategy	Critical Analysis of Researchers
Glittering Generalities	**Hyperbolic method:** Products with cunning and attractive phrases to exploit the gap between problems and solutions to fulfill needs (McClintock, 2005:664)	Use of the terms "easy", "fast", "safe" without a detailed explanation of the financial consequences or interest structure of the loan.	Trapping people in the illusion of financial security, which weakens the economic resilience of the poor and vulnerable.	Public financial literacy defense system: Symbolic representations controlled by financial corporations to cover up power relations and market domination through sterilized language.
Emotional Appeal	**Methods of persuasion:** Using emotional content to trigger emotional responses, covering entertainment and a range of emotions, including pleasure (Lee & Hong, 2016:364)	Narratives of emotional experiences, such as poverty, urgent need, or family suffering, encourage quick action to access loans.	Emotional exploitation weakens citizens' psychological control and massively increases the economic burden on households.	Psychosocial defense: Strategies to instrumentalize individual emotions in the digital capitalist system for the sake of click conversions and loan applications.
Repetition	**Content repetition method:** Increase the strength of belief in the brand attitude associations communicated in the content (Donnellan, 2016:32)	Repeated display of advertisements on various digital platforms, especially social media, applications, and streaming services, creates high exposure and normalization of online lending practices.	Forming a mass perception that debt is a normal part of everyday life, which threatens the sustainability of the household economy.	Information Defense: This practice demonstrates the control of media structures by fintech financiers, where capitalist algorithms are utilized to disseminate a single narrative systematically.

Influencers	**Persuasive figure method:** A true advertiser who promotes brands persuasively, while developing creative and quality content in strategic collaboration at every stage of message production (Pereira, 2023:4)	The use of public figures or influencers as brand ambassadors, who relate positive experiences (often fictitious or sponsored) using online lending services.	The commodification of public trust through curated narratives strengthens market control over public opinion and digital consumption.	Cultural Protection: A form of commodification of public identity in the market of trust, where celebrities become tools of legitimation of corporate narratives.
Bandwagon	**Mainstream methods:** Following popularity as a form of aspiration to be associated with a particular single product or group (Kang & Ma, 2020:3-4)	Mass claims such as "millions of people have been helped" that are not verified, to create implicit social pressure to participate, so as not to be left behind	Pushing economic decisions without critical consideration risks creating a collective debt crisis in poor or rural communities.	local community defense: An instrument to normalize high-risk financial products within the framework of digital neoliberalism, by exploiting mass market logic.
Fraud	**Consumer confidence methods:** A deliberate trick to create false confidence about product information (Russo et al., 1981:120)	Omission of important information such as compound interest rates, hidden fees, or potential repressive billing in the ad narrative and initial user interaction	Causing information asymmetry that is detrimental to the public, as well as exacerbating structural inequality in access to digital economic justice.	Legal defense of the digital financial sector: Capitalist strategy data to hide the inequality and structural risks of the debt-based economic system, in order to maintain the accumulation of value in the fintech sector.

(Data Processed from Russo et al., 1981:120;McClintock, 2005:664; Lee & Hong, 2016:364; Donnellan, 2016:32; Kang & Ma, 2020:3-4; Pereira, 2023:4 By Researchers)

Based on the mapping of propaganda strategies in online loan marketing as presented in the table, it can be concluded that these practices are not just part of conventional marketing strategies but have become a form of structured communication crime that operates in Indonesia's digital space. The use of manipulative techniques such as glittering generalities, emotional appeal, influencers, bandwagon, and fraud shows the intention to mislead public perception and create dependency on instant financial access that is full of traps. This crime is systemic because it involves controlling the public narrative through the media, forming a culture of debt consumption, and exploiting the socio-economic vulnerabilities of society. This phenomenon leads to a real threat to the cyber communication system being used to cover up risks and facilitate exploitation, so the state needs to view this practice as part of a non-military crime that disrupts national stability. A strategic response is needed through strengthening digital literacy, strict regulation of the digital lending industry, and building a consumer protection system based on social defense management that is adaptive to changes in technology and media dynamics.

In the framework of defense management, illegal online lending crimes have the potential to become a serious cyber threat with a broad impact on community-based national security. With inhumane offering and collection practices, such as repeated telephone intimidation, threats to spread personal data, and psychological harassment, it further exacerbates the mental stress of victims. In the context of national cyber defense, this propaganda shows how individual defenses against digital manipulation and financial exploitation are still weak, and illegal online loans have become an instrument of social pressure that can threaten social stability. At the same time, it has the potential to damage public trust in the digital ecosystem and state institutions. This crime weakens the foundation of social stability and security, which are the main pillars of national defense. Therefore, overcoming this phenomenon must be placed as a strategic priority, through synergy between the government, security forces, and the community to strengthen the cyber defense system. By increasing digital literacy and adaptive protection policies, the state can build a strong defense against all forms of cybercrime threats that have the potential to disrupt national security as a whole.

Implications for the Psychological and Moral Defense of the Nation

Illegal online loan crimes in Indonesia have a direct impact on the psychological aspect, not a few experience emotional crises to prolonged trauma. This problem shows that illegal online loan propaganda is not just a financial crime, but has disrupted social cohesion in society. Psychological problems are rooted in the accumulation of unsettled debts and collection agents who tend to use an intimidating approach, causing psychological pressure and increasing individual stress levels (Fitch et al., 2007:130). In the framework of non-military defense, attacks on the moral and psychological aspects of civilians constitute a disruption to national resilience that requires a cross-sector response, especially if it occurs systematically and is organized. This condition weakens the individual's psychological defense in facing the pressures of life. If left unchecked, this can erode the nation's morale collectively.

The phenomenon of illegal online loans in Indonesia not only targets the economic aspect, but also shows a systematic pattern in targeting certain community groups. Identification of victims based on profession, gender, and age shows that vulnerable groups such as teachers, women, and young people of productive age are the main targets of this practice. According to the Financial Services Authority (OJK), in 2021, 42% of the total victims of illegal online loans were teachers. Apart from teachers, other professions that were caught in illegal online loans included victims of layoffs at 21%, housewives at 18%, employees at 9%, traders at 4%, students at 3%, barbers at 2%, and online motorcycle taxis at 1% (Kompas.id, 2022). The causal factors include low financial literacy and access to digital financial services that have not been balanced with adequate understanding of the legality of loan entities.

How sad, Women are the most vulnerable group to the trap of illegal online loans. Data from the Jakarta Legal Aid Institute (LBH) complaint report shows that out of 1,944 reports received from 2018 to 2024, there were 1,208 victims, and the largest number of reports was 62.14%, the majority of whom were women (Kompas.id, 2025). Women who are victims of online loans experience various forms of violence, from physical, psychological to and sexual violence, carried out by debt collectors. The methods used include sexual harassment, distribution of personal data, to threats that damage the victim's reputation in their social environment. This condition is exacerbated by the lack of digital and financial literacy among women, which makes them more easily trapped in illegal online lending practices. According to the investigative report Watchdoc Documentary (2024), the pressure of illegal online loan debt has caused several victims to suffer mental disorders, even 25 cases of suicide. This phenomenon shows that illegal online loans not only cause financial losses but also threaten the mental health and safety of the victims. The chain of debt that is difficult to break, coupled with intimidation and harassment from debt collectors, creates a heavy mental burden for the victims. This crime has broad psychological and social impacts. Therefore, preventive and educational measures are needed to protect the public from the dangers of illegal online loans.

Weakening Institutional Synergy Prevents Illegal Online Loan Crimes

The rampant practice of illegal online lending in Indonesia is a reflection of institutional dysfunction in responding to organized and adaptive digital crime. The existence of illegal online loans that misuse personal data, charge exorbitant interest rates, and psychologically terrorize victims requires a firm and systematic state presence. However, synergy between state institutions such as the Financial Services Authority (OJK), the Ministry of Communication and Information (Komdigi), the Indonesian National Police (Polri), Bank Indonesia (BI), and the Ministry of Law and Human Rights (Kemenkumham) has not been optimally built. Fragmented coordination and weak response to public reports have increased the room for digital criminals to maneuver in the financial sector. The Financial Services Authority (OJK), as a financial sector regulator, faces limitations in prosecuting illegal online loans because it does not yet have judicial authority. OJK's focus on the administrative side, such as publishing a list of legal fintech providers and closing access, has not been accompanied by a rapid response mechanism to reports from the public who have suffered losses. On the other hand, Komdigi only blocks sites and applications based on requests or passive findings, so that illegal online loan applications often reappear with new identities. The absence of an artificial intelligence-based prevention system or early detection means that handling is always reactive and not solution-oriented. The handling of public reports by the National Police has also not met public expectations. Victims of illegal online loans who report intimidation or the spread of personal data often face a long bureaucracy and slow responses, especially because online loan cases are often categorized as civil disputes. At the Polres and Polda levels, limited human resources in the field of digital forensics hamper investigations. As a result, many reports end without a clear legal resolution. Moreover, the lack of data integration and tracking systems between institutions has caused many perpetrators to escape the law, even though they have been reported many times by the public.

The Ministry of Law and Human Rights also plays a role in the weak handling of illegal online loans. As an institution authorized to ratify legal entities, supervision of entities that abuse their legal status to carry out illegal practices is still minimal. Online loan perpetrators often use the names of fake savings and loan cooperatives or Limited Liability Companies (PT) with fictitious addresses that escape detection by the monitoring system. When public reports mention the name of a particular company or legal entity, there is no quick mechanism for freezing permits or cross-agency administrative investigations, so that perpetrators continue to operate under new names without significant obstacles.

In dealing with public reports effectively, an integrated technology-based reporting and resolution system reform is needed. The establishment of a National Integrated Complaints Center integrated with the OJK, Komdigi, Polri, Bank Indonesia, and Kemenkumham systems is an important step to ensure that every public report can be immediately followed up across sectors. Each report must be followed by a tracking ID, status update mechanism, and clear estimated handling time. In addition, the establishment of a National Task Force for Illegal Online Loans with the authority to intervene quickly against entities reported by the public will increase the responsiveness of the state. Only by building a fast, transparent, and institutional synergy-based report handling system can the state restore public trust and create a safer and fairer digital environment for all citizens.

Digital Protection Strategy for Strengthening National Defense

Illegal online lending crimes have developed into a real threat in the digital era that not only harms individuals economically but also damages the social and psychological structure of society. The modes used are increasingly sophisticated, ranging from theft of personal data, intimidation, to the spread of false information to embarrass victims. This phenomenon shows that weak digital protection can be exploited by malicious actors to disrupt social order and reduce public trust in the national digital system. As a result, social defense as part of national defense is threatened by instability that arises due to trauma, fear, and loss of security in cyberspace. Therefore, digital protection strategies must be reformulated to respond to digital crimes such as illegal online lending as part of a systemic threat to the state.

Reformulation of digital protection needs to start with strengthening the monitoring system and taking action against illegal digital activities that are destructive, such as unauthorized online lending operations. This includes the integration of artificial intelligence-based monitoring technology to detect suspicious activity patterns on the internet, as well as the development of a centralized database containing a list of illegal digital services. Digital regulations also need to be updated to be more responsive to developments in cybercrime, including giving authority to service providers to block access to illegal online lending applications quickly and effectively. Personal data protection must be placed as a strategic priority to prevent data misuse by irresponsible parties. With this approach, digital protection functions not only as a protection tool but also as a control instrument against potential national instability.

In addition to technological and regulatory aspects, community empowerment through digital literacy is key to creating a collective defense against the threat of illegal online loans. The public must be equipped with the ability to recognize the characteristics of illegal loan services, understand the risks of data misuse, and know the reporting procedures if they become victims. Educational campaigns must be designed massively, structured, and inclusively to reach the most vulnerable groups, such as students, housewives, and informal workers. This increased awareness will form a “social filter” where individuals and communities can detect and defend against digital fraud attempts. A digital protection strategy that makes the community the main actor not only strengthens the layer of protection but also builds a culture of security in the cyber era. This is very important to maintain social cohesion and trust in the national digital system.

Table 2. Approaches Integrated Digital Protection as a Pillar of National Defense

No	Strategic Dimension	Digital Defense Policy Approach	Related Institutions	Recommendation Update	Strategic Objectives
1.	**Institutional Capacity to Build Government Defense**	**1. Decentralization of responsibility:** Government defense requires the division of responsibilities to each government function in a decentralized manner. **2. Top-down coordination:** To prevent systemic failures that have mutual impacts, a top-down, coordinated approach is needed. **3. The role of central institutions:** It is recommended that there be a central agency specifically designated to oversee and ensure the implementation of defense policies and continuity at all levels of government.	Financial Services Authority	1. Building an AI-based automated monitoring system 2. Expanding digital financial literacy 3. Establish an initial investigation unit against perpetrators of the illegal financial sector	Increasing the effectiveness of prevention and early action against illegal financial activities and strengthening public understanding of a safe digital financial ecosystem.
			Ministry of Communication and the Digital Republic of Indonesia	1. Establishing partnerships with global digital platforms 2. Establishing a 24/7 digital financial cyber unit 3. Integration of the public complaint system into the automatic blocking system	Accelerate the response to the systemic spread of illegal online loans and optimize digital protection based on technology and public participation.
			Republic of Indonesia Police	1. Formation of Cyber Task Force for Illegal Online Loans 2. Increasing the capacity of regional cyber investigators 3. Integration of victim data with OJK and Komdigi reports	Ensuring that law enforcement touches the root of the problem through a systemic approach to cybercrime syndicates, not just individual perpetrators.
			Ministry of Law and Human Rights of the Republic of Indonesia	1. Legal entity verification system based on digital transparency 2. Tracking changes in legal entity structure 3. Freezing of problematic legal entities	Increasing transparency and accountability of legal entities and minimizing the misuse of legal entities in illegal digital activities.

			House of Representatives of the Republic of Indonesia	1. Deregulate the Cyber Security Law, the Personal Data Protection Law, and Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure (IIV)	Providing a strong legal basis to guarantee the protection of digital space and citizens' digital rights.
			Bank Indonesia	1. Establish a village bank with supportive products and regulations with easy requirements.	Progressive and sustainable financial inclusion as a defense of the community's economy in a fair and equitable manner
2.	**Securing the State's Digital Infrastructure and Services**	**1. Mandatory safety standards:** Countries need to set minimum security standards that all digital public service and infrastructure providers must meet. **2. Protect against internal and external threats:** Cyber defense must include protection from *cyber attack* due to negligence or sabotage from within **3. Protection of critical data and services:** Unauthorized access or manipulation of key digital data and services must be effectively prevented.	National Digital Protection Cross-Agency Coalition	1. National Data Integration: Cross-institutional digital dashboard system for real-time information exchange	Structuring and improving the speed and accuracy of response to digital threats through collaboration and shared data
				2. Permanent National Task Force: Formation of a cross-institutional task force (OJK, Komdigi, Polri, Kemenkumham, BI)	
				3. Special Law on Illegal Fintech: Special regulations for the protection and prosecution of illegal fintech	
				4. Multilevel Approach: Public education, strict law enforcement, international cooperation (blocking foreign servers)	

3.	**Manage Third-Party Risk For Technology Innovation**	**1. The need for risk mitigation:** Countries need to establish procedures to reduce these risks to reasonable levels. **2. Avoid over-regulation:** Mitigation efforts must continue to encourage innovation and avoid overly restrictive policies.	All Pillars of Digital Government	1. Strengthening the coordinating role in one national platform 2. Harmonization of regulations between sectors 3. National digital defense system design	Produce a sustainable and nationally coordinated digital protection system to maintain national stability and defense in the face of cross-sector cyber threats.

(Data Processed From Raieste et al., 2024 by Researchers)

Reformulating digital protection against illegal online lending crimes is a strategic step to address the escalation of cyber threats that can weaken the joints of national defense. A cross-dimensional approach involving financial institutions, communications, law enforcement, and regulators is key to building a resilient and adaptive digital defense system. These efforts include policy updates, the formation of special operational units, cross-sector data integration, and the preparation of regulations that are responsive to the complexity of technology-based digital crimes.

Furthermore, a joint national strategy and strengthening of the coordinating structure are the foundations to ensure that all actors move within a synergistic policy framework. Through technology integration, regulatory harmonization, and inclusive public literacy, Indonesia can form a digital ecosystem that is not only reactive to attacks but also proactive in maintaining information sovereignty and socio-economic stability. Thus, digital protection is not just a defense tool, but a main pillar in realizing sustainable national defense in the cyber era.

The success of this strategy depends on synergy between stakeholders, willingness to share data and authority efficiently, and a shared commitment to upholding Indonesia's digital sovereignty. Therefore, the steps in this integrated table are not only technocratic recommendations but also a roadmap for building a safe, fair, and inclusive digital ecosystem for all citizens. In this way, Indonesia's digital space will not only become a rapidly developing economic and social field but also a strong fortress in maintaining the integrity and stability of the nation in the cyber era.

CONCLUSION AND RECOMMENDATION

Illegal online loan propaganda is a form of digital crime that exploits people's financial needs through promises of ease and speed of disbursement of funds without collateral. With massive distribution through social media, short messages, and unofficial applications, illegal online loans target vulnerable groups with minimal digital financial literacy. This propaganda is not only misleading, but also becomes a gateway into debt traps and misuse of personal data. The impact is very real on individuals' psychological defenses, with mental pressure that can lead to disinformation and social polarization. More broadly, this propaganda is also a threat to national morals because it encourages people to rely on instant solutions that violate the law, weaken integrity values, and foster an irresponsible consumer culture.

The weak synergy between institutions in cracking down on illegal online loans indicates a structural dysfunction that hinders effective law enforcement. The lack of integration between financial institutions, law enforcement officers, and related government agencies weakens public trust in the state. When the state is unable to protect its people from increasingly complex digital threats, the integrity of the government is at stake. This situation creates a gray area that can be exploited by irresponsible individuals to expand their influence. Not only that, the nation's moral values , such as honesty, responsibility, and social solidarity, are also eroded by the normalization of illegal practices that appear easy and profitable on the surface.

As a concrete step, an integrated and multi-layered national digital strategy is needed, starting from increasing technological capacity to law enforcement that touches the roots of the syndicate. The formation of a Joint Task Force, a cross-institutional digital dashboard, and special regulations on illegal fintech must be a top priority. In addition, a multi-level approach needs to be implemented: broad public education, strengthening the monitoring and enforcement system, and international cooperation to disable foreign server networks. Threats to national morals must be faced by strengthening character values through education and digital literacy campaigns that instill ethics in media. Synergy between institutions such as OJK, Komdigi, Polri, BI, Kemenkumham, and community forums is no longer an option, but an absolute necessity to maintain digital sovereignty, psychological defense, and the moral integrity of the nation as a whole.

REFERENCES

Antara News. (2023). Lack of financial literacy is the cause of someone getting trapped in online loans.

Antara News. (2025). OJK: Illegal online loans are the most common cases found by the PASTI Task Force.

CNBC Indonesia. (2024). Sad! Teachers are the most entangled in online loans, this is what OJK says.

CNN Indonesia. (2024). Not mothers, this is the age group with the most loan arrears. https://www.cnnindonesia.com/ekonomi/20241004125940-78-1151498/bukan-emak-emak-ini-kelompok-usia-paling-banyak-tunggak-utang-pinjol(Accessed on 22 May 2025)

Donnellan, J. (2016). Effect of ad repetition and relevance in social media advertising. International Journal of Business and Applied Social Science, 2(3). https://ssrn.com/abstract=2940059

Financial Services Authority. (2024). Task Force PASTI blocks 1001 illegal entities in June–July 2024. Financial Services Authority.

Fitch, C., Simpson, A., Collard, S., & Teasdale, M. (2007). Mental health and debt: Challenges for knowledge, practice and identity. Journal of Psychiatric and Mental Health Nursing, 14(2), 128-133. https://doi.org/10.1111/j.1365-2850.2007.01053.x

Heister, S., & Yuthas, K. (2022). How blockchain and AI enable personal data privacy and support cybersecurity. In T. M. Fernández-Caramés & P. Fraga-Lamas (Eds.), Advances in the convergence of blockchain and artificial intelligence (pp. 33–54). Springer.

Kang, I., & Ma, I. (2020). A study on bandwagon consumption behavior based on fear of missing out and product characteristics. Sustainability, 12(6), 2441. https://doi.org/10.3390/su12062441

Katadata Insight Center. (2024). 10 provinces with the largest online loan debt in mid-2024.

Kompas.id. (2022). The teaching profession is the most common victim of illegal loans. https://www.kompas.id/baca/ekonomi/2022/10/07/profesi-guru-paling-banyak-jadi-korban-pinjol-ilegal(Accessed on 21 May 2025)

Kompas.id. (2025). Why women become victims of online loans. https://www.kompas.id/artikel/mengapa-perempuan-menjadi-korban-pinjol(Accessed on 21 May 2025)

Lee, J., & Hong, I. B. (2016). Predicting positive user responses to social media advertising: The roles of emotional appeal, informativeness, and creativity. International Journal of Information Management, 36(3), 360-373. https://doi.org/10.1016/j.ijinfomgt.2016.01.001

McClintock, A. (2005). Propaganda techniques in today's advertising. College Writing Skills with Readings, 663-667. https://www.lirvin.net/0301bbsite/propaganda.pdf

National Digitalization Commission. (2004). The rise of fraud, Task Force PASTI stops thousands of illegal financial entities.Komdigis.

Ngafifah, I., Widianti, L., Roihana, P. N. A., Makarando, E. M., Nailatul, A. A., & Dewi, R. (2024). Analysis of online loan cases in the CNN Indonesia news

portal in 2018–August 2023.Journal of Sociological Interaction, 3(2). https://jos.unsoed.ac.id/jis/article/download
Pereira, M. J. d. S., Cardoso, A., Canavarro, A., Figueiredo, J., & Garcia, J. E. (2023). Digital influencers' attributes and perceived characterizations and their impact on purchase intentions. Sustainability, 15(17), 12750. https://doi.org/10.3390/su151712750
Putri, P. A., & Rinaldi, K. (2022). The problems of illegal online loans based on the victim's perspective: A case study. International Journal of Advances in Social and Economics, 4(3), 102-106. https://doi.org/10.33122/ijase.v4i3.215
Raieste, A., Rebane, A., Tapupere, M., & McBride, K. (2024). Government resilience in the digital age. Nortal. https://ora.ox.ac.uk/objects/uuid:7af1a0e0-09a2-434b-aa8d-f4997d9fa112/files/skp78gj50h
Russo, J. E., Metcalf, B. L., & Stephens, D. (1981). Identifying misleading advertising. Journal of Consumer Research, 8(2), 119-131. https://doi.org/10.1086/208848
Sherman, J. (2021). Digital authoritarianism and implications for US national security. The Cyber Defense Review, 6(1), 107–118. https://www.jstor.org/stable/26994115
Tate, D., Pirini, J., & Lofgren, K. (2023). Towards a multi-stakeholder framework for evaluating digital government success [Conference contribution]. Open Access Te Herenga Waka–Victoria University of Wellington. https://doi.org/10.25455/wgtn.24540100
Tempo.co. (2021). OJK: Beware of illegal online loan offers via SMS or WhatsApp. https://www.tempo.co/ekonomi/ojk-waspada-tawaran-pinjaman-online-ilegal-via-sms-atau-whatsapp-484068(Accessed on 22 May 2025)
Victor-Mgbachi, T. O. Y. I. N. (2024). Navigating cybersecurity beyond compliance: Understanding your threat landscape and vulnerabilities. Iconic Research and Engineering Journals, 7.
Watchdoc Image. (2024). LOAN TRAP: Rules, interest, individuals and low knowledge [Video]. YouTube. https://www.youtube.com/watch?v=SpzQ3ab9Yjc(Accessed on 21 May 2025)
Women, risks, and consumer protection in online lending platforms in Indonesia: A study on the multiple vulnerabilities of women as users and its impact to gender-based violence (Criminology report). (2023). Faculty of Social and Political Sciences, University of Indonesia.