IDSCIPUB
Indonesian Scientific Publication

Politeia
Journal of Public Administration and
Political Science and International Relations

Check for updates

OPEN ACCESS

*CORRESPONDENCE
Puspo Dewi Dirgantari,
puspodewi@upi.edu

RECEIVED 26 March 2026
ACCEPTED 26 April 2026
PUBLISHED 30 April 2026

CITATION
Prasetia AR, Dirgantari PD (2026) Strategic Capability and Public Value in Online Gambling Enforcement: An Indonesian National Police Case Study. *Politeia : Journal of Public Administration and Political Science and International Relations*. 4 (2), 97-106. doi: 10.61978/politeia.v4i2.1493

TYPE Original Research
PUBLISHED 30 April 2026
DOI 10.61978/politeia.v4i2.1493
VOL 4 Issue 2 April 2026.

Strategic Capability and Public Value in Online Gambling Enforcement: An Indonesian National Police Case Study

Arus Reka Prasetia[1], Puspo Dewi Dirgantari[2*]

[12]Universitas Pendidikan Indonesia, West Java, Indonesia

Abstract

Online gambling has become a major public governance and cyber law enforcement challenge in Indonesia due to its links to social harm, illicit financial flows, and threats to digital order. This article examines how the Indonesian National Police, particularly the Directorate of Cyber Crime within the Criminal Investigation Agency, mobilizes strategic capability in online gambling enforcement and how these enforcement patterns can be interpreted through a public value lens. The study employed a qualitative document-based single-case design using 21 screened public documents selected from 35 sources related to the 2022–2025 enforcement period. The corpus included performance reports, institutional statements, regulatory and policy documents, task-force coordination materials, and public analytical sources. Data were analyzed using thematic document analysis, pattern matching, and explanation building. The findings identify five strategic capabilities: integrated digital intelligence, accredited digital forensics, inter-agency coordination, public participation and reporting reach, and adaptive legal-investigative capability. These capabilities contribute to economic protection, social protection, and digital ecosystem integrity through intelligence-driven enforcement, financial disruption coordination, public reporting and preventive education, and digital ecosystem stewardship. Economic protection emerged as the strongest dimension, while digital ecosystem integrity remained the most interpretive because it relied on proxy indicators rather than standardized measurement. The article concludes that online gambling enforcement in Indonesia becomes strategically meaningful when police capability is directed not only toward case handling but also toward broader public value creation.

KEYWORDS

cyber law enforcement; indonesian national police; online gambling enforcement; public value; strategic capability.

Introduction

Indonesia's rapid digitalization has widened access to communication, finance, and platform-based services, while simultaneously expanding the opportunity structure for cyber-enabled crime. Within this setting, online gambling has emerged as a major public governance problem because it combines illegal content distribution, fast payment channels, algorithmic visibility, and cross-border operations. Recent research also shows that cybercrime and cybersecurity have become increasingly interconnected research domains, indicating that online gambling enforcement now sits within a broader field of digital risk, platform governance, and illicit online markets (Wu et al., 2023).

Online gambling should therefore not be framed as a narrow offence category alone. It also constitutes a public health, social protection, and digital governance issue because its harms extend beyond individual bettors to household finances,

family stability, mental health, and wider community life. Recent scholarship further shows that gambling-related harm has become more substantial as commercial gambling becomes increasingly digital, accessible, and weakly regulated across jurisdictions (Fisher et al., 2025; Wardle et al., 2024).

The Indonesian state has responded through a combination of legal measures, institutional coordination, and intensified cyber law-enforcement efforts. Conventional enforcement indicators such as arrests, blocked sites, frozen accounts, and seized assets remain important because they capture institutional activity and administrative output. Yet, in the present case, these indicators are not analytically sufficient on their own. They show the scale of intervention, but they do not adequately explain how institutional capability is organized, coordinated, and translated into broader forms of public value. A public value lens provides additional explanatory leverage because it makes it possible to examine whether enforcement contributes to economic protection, social protection, and the governance of the digital environment, rather than only counting case-processing outputs.

This analytical limitation is important because existing research on cybercrime policing has largely concentrated on operational and organizational challenges. Collier et al. (2021) show that cybercrime policing increasingly targets infrastructure and enabling systems rather than offenders alone. Curtis and Oxburgh (2023) similarly demonstrate that cybercrime in real-world policing involves organizational, technical, and procedural complexity that is often underestimated in policy debate. Khan (2024) further argues that cybercrime policing should move toward a harm-centric perspective rather than rely solely on conventional offender-centered logics. These studies are highly relevant, yet they say comparatively little about how a public law-enforcement institution translates strategic capability into public value in a concrete online gambling enforcement setting.

At the same time, public administration scholarship increasingly argues that public organizations should be evaluated through the value they create for society, not merely through bureaucratic output. Public value scholarship, beginning with Moore, (1995) and later elaborated by Stoker, 2006, emphasizes that public organizations exist to create socially recognized and institutionally legitimate outcomes. Later work highlights public value co-creation among multiple actors in networked governance arrangements (Bryson et al., 2017). More recent scholarship on strategizing public value and on policing, technology, and public values extends this agenda by treating public value as something that must be deliberately designed, organized, and governed in technology-intensive settings (Feeney & Mughan, 2025; Kitchener & Ashworth, 2025). Even so, this literature has rarely engaged online gambling enforcement as an empirical arena in which public value is actively created, contested, and sustained.

Strategic capability research offers another useful lens. Capability-based and VRIO-oriented studies suggest that digital transformation becomes strategically meaningful when technological assets are combined with organizational alignment, institutional support, and the ability to deliver value. Simamora et al. (2024) demonstrate this through a VRIO-based analysis of digital transformation, while Hasan et al. (2023) show that public-sector digital processes need to be translated into explicit value delivery. Prasetia et al., (2026) further argue that digital transformation strategies increasingly require ethical and axiological grounding, a point that becomes especially salient when public institutions rely on data-intensive tools and inter-agency information flows. However, these studies stop short of explaining how strategic capability operates in public-sector cyber law enforcement against online gambling.

Viewed together, these literatures suggest that online gambling enforcement can be examined as more than a technical policing problem. The public-sector adaptation of the Triple Bottom Line helps explain why enforcement outcomes should be assessed not only in terms of case disposal, but also in terms of economic protection, social protection, and digital ecosystem integrity. At the same time, VRIO and dynamic capability perspectives help explain why some institutional, technological, and collaborative capacities become durable sources of performance in fast-changing cyber environments. This combined perspective is particularly useful for understanding how public-sector cyber law enforcement creates value while sustaining institutional capability over time (O'Flynn, 2007; Winter, 2003; Zollo & Winter, 2002).

In this article, the public-sector adaptation of the Triple Bottom Line is used as a conceptual extension and analytical analogy rather than as a literal transfer of a corporate evaluative framework. Economic protection corresponds to the economic dimension, and social protection corresponds to the people dimension, while the planet dimension is analytically recast as digital ecosystem integrity. This modification is proposed because the present case concerns the protection of lawful digital space, the disruption of harmful online infrastructures, and the maintenance of safer conditions for digital interaction, rather than environmental sustainability in the literal sense. Accordingly, digital ecosystem integrity is used here as an interpretive analytical lens, not as a fully standardized metric.

Taken together, the literature remains fragmented across studies of online gambling harm, cybercrime policing, public value, and collaborative governance. The contribution of the present study is therefore intentionally specific and bounded. Conceptually, the article brings strategic capability and public value into one analytical conversation in online gambling enforcement, an intersection that remains underdeveloped in the literature reviewed above. Empirically, it examines a concrete enforcement setting in Indonesia rather than discussing cyber policing or gambling harm only at a general level. Contextually, it adopts a qualitative document-based single-case design, which means that the article does not claim broad causal verification across settings. Instead, it offers an interpretive explanation of how capability is mobilized and how its public value implications can be understood in a bounded Indonesian case.

This study therefore examines online gambling enforcement in Indonesia as a single case centered on the Indonesian National Police, with the Directorate of Cyber Crime of the Criminal Investigation Agency serving as the focal operational unit within a broader cross-agency enforcement environment. The wider online gambling eradication regime, especially the Online Gambling Eradication Task Force and associated financial, content-governance, and cyber-governance institutions, is treated as the institutional environment of the case rather than as a separate case in its own right. The study asks how the Indonesian National Police mobilizes strategic capability in online gambling enforcement and how the resulting enforcement patterns can be interpreted through a public

value lens.

On that basis, the article contributes by clarifying the capability-to-value relationship in a public-sector cyber law-enforcement setting, by showing how economic protection, social protection, and digital ecosystem integrity can be used as interpretive dimensions of public value, and by bringing a strategic management perspective into public law enforcement without reducing the analysis to a purely corporate model of competition. The remainder of the article presents the method, reports the findings, discusses the theoretical and practical implications, and concludes with the study's principal analytical contribution.

Methods

This study employed a qualitative document-based single-case study to examine online gambling enforcement in Indonesia as a bounded public-sector enforcement case. The case was defined as the Indonesian National Police response to online gambling enforcement at the national level during 2022 to 2025. Within that case, the Directorate of Cyber Crime within the Criminal Investigation Agency served as the focal analytical unit because it functioned as the principal cyber law-enforcement actor in this policy domain. The wider online gambling eradication regime, especially the Online Gambling Eradication Task Force and associated cross-agency arrangements, was treated as the institutional environment of the case rather than as a separate case in its own right. This distinction was adopted to stabilize the case boundary and to keep the analysis methodologically coherent. Strategic capability and public value were treated as the central analytical constructs, while the public-sector adaptation of the Triple Bottom Line and the VRIO logic served as supporting analytical lenses. Accordingly, the following subsections describe the research type, the documentary corpus and selection criteria, the research location, the analytical tools, the data collection procedure, the data analysis process, and the ethical considerations of the study.

Research Type

This study adopted a qualitative document-based single-case study design. Rather than testing statistical causality, the study sought to develop a context-sensitive explanation of how strategic capability was mobilized and how its public value implications can be interpreted in a public-sector cyber law-enforcement setting. A single-case design was appropriate because online gambling enforcement in Indonesia represented a strategically important and institutionally rich case that combined cybercrime investigation, financial disruption, inter-agency coordination, and community protection within one national policy setting. The design allowed close examination of a bounded institutional response while remaining attentive to the wider governance environment in which that response unfolded.

Population and Sample/Informants

Because this study did not employ surveys or interviews, the unit of analysis was a purposively assembled public documentary corpus rather than individual respondents. The initial mapping stage identified 35 publicly accessible documents relevant to online gambling enforcement in Indonesia. After screening for authority, relevance, temporal fit, and triangulation potential, 21 documents were retained as the formal empirical corpus and 14 documents were excluded because they were overly general, duplicative, conceptually supportive rather than empirically central, or insufficiently anchored to the case. The retained corpus was organized into five source families: eight performance and annual reports, three institutionally released public statements or public data releases, four regulatory and policy texts, two task-force or cross-agency coordination materials, and four corroborative public analytical or statistical reports. Supporting scholarly literature was used to contextualize and cross-check interpretation, but it was not counted as part of the formal empirical corpus. No human informants were recruited in this study.

Core public materials were drawn from the Indonesian National Police and the Directorate of Cyber Crime, the Online Gambling Eradication Task Force, the Financial Transaction Reports and Analysis Center, the Ministry of Communication and Digital Affairs, the National Cyber and Crypto Agency, the Financial Services Authority, Bank Indonesia, and a limited number of corroborative public analytical sources relevant to the Indonesian case. A small number of public documents issued in early 2026 were retained only when they retrospectively reported 2025 enforcement outcomes or coordination patterns. These materials were treated as retrospective reporting documents for the 2025 period and did not extend the substantive temporal boundary of the case beyond 2025. (See Table 1).

Research Location

The study was conducted in Indonesia at the national governance level rather than in a single city-based site. Although the institutional focus was placed on the Indonesian National Police, the analysis was situated within the broader policy and enforcement environment of online gambling eradication, especially the coordination architecture involving financial intelligence, content blocking, cyber governance, and cross-agency law enforcement. This national setting was selected because it represented the principal arena in which strategic capability, public value, and cyber law enforcement intersected in the Indonesian case. The temporal scope covered 2022 to 2025, with particular analytical attention to the intensified coordination phase following the establishment of the Online Gambling Eradication Task Force in 2024.

Instrumentation or Tools

The study employed a structured documentary review protocol and an evidence matrix as its principal analytical tools. The review protocol guided document identification, screening, extraction, comparison, and synthesis. The evidence matrix recorded, for each document, the document identity and date, the source institution and document type, reported enforcement indicators, statements relating to strategic capability, statements relating to public value, corroboration status and source ownership, and analytical notes on attribution, proxy status, and interpretive caution. This structure was designed to preserve an auditable link between raw documentary material and higher-order analytical interpretation.

The analytical framework was organized around two primary constructs. Strategic capability referred to recurrent institutional capacities that combined resources, routines, expertise, and coordination in ways that enabled sustained enforcement performance. It did not refer to isolated functions, one-off actions, or raw outputs. Public value was interpreted through three dimensions, namely economic protection, social protection, and digital ecosystem integrity. Within this framework, digital ecosystem integrity was used

as an interpretive analytical dimension for the condition of lawful digital space and digital order rather than as a fully standardized metric. After recurrent capabilities had been identified, they were further examined through the VRIO logic to assess whether they were valuable, rare, difficult to imitate, and organizationally supported. These tools were used as structured analytical guides rather than rigid coding boxes so that the analysis could remain sensitive to case-specific patterns emerging from the documentary evidence.

Data Collection Procedures

Data collection was carried out in several stages. First, the institutional field of online gambling enforcement in Indonesia was mapped to identify the organizations most directly linked to the case. Second, relevant documents were gathered from official institutional outputs, regulatory archives, public reports, and credible supporting publications. Third, the collected materials were screened using the inclusion criteria of authority, relevance, temporal fit, and triangulation potential. Only publicly accessible or institutionally released materials were included, while confidential case files, unpublished internal memoranda, and personal records were excluded.

Fourth, the selected documents were read repeatedly and key evidence was extracted into the evidence matrix. Extracted materials included numerical indicators, descriptions of enforcement actions, institutional roles, collaborative arrangements, legal instruments, and documentary statements related to strategic adaptation and public value outcomes. Fifth, cross-checking was undertaken across documents to reduce over-reliance on single-source claims, especially when institutionally generated performance data formed the basis of an important argument. To prevent official institutional reporting from dominating the interpretation, police and Dittipidsiber documents were compared, where possible, with cross-agency materials, regulatory texts, and corroborative public analytical or statistical sources. When a major claim could not be corroborated through other credible documents, it was retained only with interpretive caution. This procedure was intended to preserve the analytical value of official materials while minimizing the risk of uncritical institutional reporting.

Data Analysis

The analysis combined deductive and inductive reasoning through thematic document analysis, pattern matching, and explanation building. In the first stage, raw documentary statements were coded descriptively. Examples included cyber patrol, platform-based reporting, transaction tracing, accredited forensic laboratory, account freezing, asset seizure, public education, school outreach, and cross-border coordination. In the second stage, these descriptive codes were grouped deductively into provisional analytical categories aligned with the framework, such as integrated digital intelligence, accredited digital forensics, inter-agency coordination, economic protection, and social protection. In the third stage, inductive refinement was used when recurrent patterns were not fully captured by the initial framework, especially in relation to financial disruption, reporting reach, and digital ecosystem stewardship. In the fourth stage, pattern matching was used to examine how identified capabilities were connected to forms of public value, and explanation building was used to clarify the institutional mechanisms and constraints shaping that relationship.

Interpretive consistency was maintained through repeated reading, constant comparison across documents, recursive rechecking of category boundaries, and explicit notation in the evidence matrix of whether a claim was directly evidenced, proxy-based, or interpretive. For example, recurring references to cyber patrol, public reporting inputs, transaction signals, and target prioritization were first coded as intelligence-related practices and were then consolidated into the higher-order category of integrated digital intelligence. Similarly, recurring references to account freezing, asset seizure, and transaction decline were treated as direct evidence of financial disruption and only then interpreted more cautiously as indicators of economic protection rather than as direct measures of prevented losses. The analysis remained primarily qualitative and interpretive. Quantitative indicators contained in official reports were used descriptively to support interpretation and to trace operational patterns across the study period, but they were not subjected to inferential statistical testing because the purpose of the study was analytical explanation rather than statistical generalization. When a claim relied on proxy indicators rather than direct measurement, this inferential status was acknowledged explicitly. This was especially important in relation to reporting reach, reduced financial circulation, and digital ecosystem integrity.

Table 1. Composition of the Formal Public Documentary Corpus

Source Family	Number Retained	Main Analytical Function
Performance and annual reports	8	Institutional performance, operational capability, and enforcement trends
Institutionally released public statements and public data releases	3	Publicly reported outcomes, outreach, and enforcement signals
Regulatory and policy texts	4	Legal authority, institutional mandate, and governance framework
Task-force and cross-agency coordination materials	2	Coordinated intervention, financial disruption, and cross-agency architecture
Corroborative public analytical or statistical reports	4	External balance, contextual corroboration, and interpretive restraint
Total retained	**21**	**Formal empirical corpus**

Source: Constructed by the author from the screened public documentary corpus.

Ethical Approval

Formal ethical approval was not required because the study did not involve human participants, interviews, surveys, or direct intervention. The research relied exclusively on documentary materials obtained from publicly available or institutionally published sources. Even so, the study followed the principles of responsible scholarship by accurately representing source materials, avoiding speculative claims beyond the available evidence, and treating institutionally generated performance data with analytical caution. No confidential personal data were collected, accessed, or disclosed in this study.

Result and Discussion

The documentary analysis generated three interrelated sets of findings regarding online gambling enforcement in the Indonesian case. The first concerned recurrent strategic capabilities documented across the retained public corpus. The second concerned the forms of public value that could be directly evidenced or cautiously inferred from those materials. The third concerned the institutional mechanisms and constraints through which capability was translated into value.

Before presenting the findings, attribution must be clarified. Police and Dittipidsiber documents reported core enforcement indicators such as handled cases, suspects, frozen accounts, seized assets, and, in 2025, requested website blocking actions and pre-emptive education activities. By contrast, PPATK, task-force, and digital-governance documents reported broader transaction, coordination, and digital-environment indicators. These figures do not all derive from identical institutional owners or identical reporting windows. They are therefore used descriptively and comparatively rather than as interchangeable measures within a single performance series.

-

Table 2. Recurrent Strategic Capabilities in Online Gambling Enforcement

Capability	Main Documentary Manifestations	Why Treated As A Strategic Capability
Integrated digital intelligence	Cyber patrol, platform-based reporting, network mapping, transaction intelligence, and target prioritization	Recurrent combination of intelligence routines, information inputs, and case-selection procedures
Accredited digital forensics	ISO/IEC 17025-accredited laboratory, certified personnel, digital evidence extraction, recovery, and analysis	Stable evidentiary capacity supported by personnel, infrastructure, standards, and procedural continuity
Inter-agency coordination	Coordination with PPATK, the Ministry of Communication and Digital Affairs, OJK, Bank Indonesia, BSSN, the Attorney General's Office, and other agencies	Institutionalized collaborative capacity linking investigation, financial disruption, content governance, and prosecution
Public participation and reporting reach	Patrolisiber.id, public reporting channels, community outreach, volunteer networks, and public communication	Recurrent participatory capacity that expands information flows and preventive reach beyond formal organizational boundaries
Adaptive legal-investigative capability	Use of money laundering provisions, follow-the-money investigations, cross-border cooperation, and evolving tactical responses	Institutional capacity to reconfigure enforcement from surface disruption toward deeper financial and legal intervention

Source: Author's synthesis from the retained public documentary corpus.

Table 3. Forms of Public Value and Evidentiary Status

Public Value Dimension	Direct Documentary Evidence	Proxy or Contextual Indicators	Interpretive Status
Economic protection	Asset seizure, frozen accounts, follow-the-money investigations, and cross-agency transaction disruption indicators	Reduced financial circulation and weakened illicit revenue flows	Strongly supported as financial disruption and economic protection, but not as a direct measure of prevented losses
Social protection	Pre-emptive education activities, public reporting channels, outreach to schools and community organizations, and participation figures	Awareness formation, reporting reach, and preventive exposure reduction	Supported as prevention and outreach, but not as a direct measure of institutional trust
Digital ecosystem integrity	Blocking-related actions or proposals, cyber patrol, forensic standardization, infrastructure disruption, and international coordination	Reduced harmful digital presence and support for cyber resilience	Most interpretive dimension, based on proxy indicators rather than a standardized measured outcome

Source: Author's synthesis from the retained public documentary corpus.

Public police-source documents reported 3,975 handled

cases and 5,982 suspects during 2022 to 2024, together with 4,196 frozen accounts and Rp817.4 billion in seized assets (Bareskrim Polri, 2026). A subsequent public police release for 2025 reported 664 handled cases, 744 suspects, 231,517 requested website blocking actions, 1,764 pre-emptive education activities, and Rp286.256 billion in seized assets (Bareskrim Polri, 2026). Read together, these police-source figures indicate 4,639 handled cases, 6,726 suspects, and total police-attributed seized assets exceeding Rp1.1 trillion across 2022 to 2025. When the 2025 requested blocking figure is read alongside the 2022 to 2024 police blocking figure, the cumulative blockingrelated total exceeds 272,000 actions or proposals across the study period. In addition, PPATK and task-force reporting indicated a decline in online gambling transaction volume from Rp90 trillion in the first quarter of 2024 to Rp47 trillion in the first quarter of 2025 (Satgas Pemberantasan Perjudian Daring, 2025). In this article, the transaction decline is treated as a cross-agency contextual indicator rather than as a police-only output.

Strategic Capabilities

In this article, a strategic capability refers to a recurrent and institutionalized capacity that combines resources, routines, expertise, and coordination in ways that enable sustained enforcement performance. It does not refer to a single output, a one-off action, or a generic administrative function. On that basis, the analysis identified five strategic capabilities. (See table 2).

The first strategic capability was integrated digital intelligence. Across the retained corpus, cyber patrol, public reporting, transaction-based signals, and inter-agency intelligence were repeatedly linked to case prioritization, target selection, and network mapping. This pattern suggests that enforcement was increasingly organized around information integration rather than around isolated offender detection alone. Intelligence therefore functioned as the first strategic filter through which cases, actors, and digital infrastructures were identified and escalated.

The second strategic capability was accredited digital forensics. The documents consistently described an accredited digital forensics laboratory, certified personnel, and forensic procedures capable of extracting, recovering, and analyzing digital evidence from devices, accounts, and network traces. This was more than a technical tool. It was a stable institutional capacity that supported investigative depth, evidentiary continuity, and the legal usability of digital traces.

The third strategic capability was inter-agency coordination. The retained corpus repeatedly showed that online gambling enforcement depended on coordinated action among policing, financial intelligence, payment supervision, content governance, and prosecutorial actors. In this sense, coordination was not treated as a supplementary administrative function. It operated as a recurrent capacity that linked case handling with account freezing, asset tracing, payment supervision, and blocking-related intervention.

The fourth strategic capability was public participation and reporting reach. The documents directly evidenced public reporting channels, community-based digital literacy programs, volunteer networks, and recurring public communication. Publicly released materials reported 2.4 million Patrolisiber.id users, more than 1.2 million direct education participants, more than 450 million social media impressions, more than 24,000 volunteers, and more than 680 supported communities (Bareskrim Polri, 2024; Satgas Pemberantasan Perjudian Daring, 2025). In this article, these figures are interpreted as participation and reporting-reach indicators. They do not, on their own, constitute a direct measurement of institutional trust, legitimacy, or public confidence.

The fifth strategic capability was adaptive legal-investigative capability. The case showed a repeated movement beyond surface-level blocking toward deeper financial and legal intervention through account freezing, asset seizure, money laundering provisions, and cross-border coordination. This pattern suggests that enforcement tactics adapted to the financialized and transnational character of online gambling. The capability was therefore not simply legal compliance. It was a recurring institutional capacity to reconfigure investigative emphasis as the threat environment evolved.

Forms of Public Value

The second set of findings concerned the forms of public value that could be identified from the retained public corpus. To keep the evidentiary basis explicit, the analysis distinguishes among direct documentary evidence, proxy indicators, and interpretive inference. (See Table 3).

The strongest direct documentary evidence concerned economic protection. The corpus consistently portrayed online gambling enforcement as a process of disrupting illicit financial extraction through asset seizure, account freezing, follow-the-money investigation, and coordination with financial intelligence and supervisory agencies. The documents also indicated a qualitative shift from content-based disruption toward financially oriented intervention. In practical terms, this meant that enforcement increasingly targeted the economic foundations of the gambling ecosystem rather than only its visible online content. The public value supported most directly by the corpus is therefore reduced financial circulation, disrupted illicit revenue flows, and the protection of the broader digital-financial environment. By contrast, prevented losses cannot be treated as a directly measured finding because the retained documents do not provide a sufficiently explicit counterfactual measurement strategy.

The second form of public value was social protection. The retained corpus showed that online gambling enforcement addressed not only offenders, but also vulnerable populations and communities exposed to social harm. Public education, digital literacy, community outreach, and platform-based reporting operated as preventive interventions aimed at reducing exposure to

online gambling and increasing public awareness of its risks. The breadth of outreach was notable, including more than 1,200 educational institutions, more than 380,000 students, more than 320 religious communities, and more than 180 women's organizations in police and task-force materials (Bareskrim Polri, 2024; Satgas Pemberantasan Perjudian Daring, 2025). These findings support an interpretation of social protection through prevention, awareness formation, and reporting reach. However, the documents do not directly measure institutional trust, legitimacy, or public confidence, and those claims are therefore not treated here as directly evidenced outcomes.

The third form of public value was digital ecosystem integrity. This was the most interpretive of the three dimensions. The direct documentary evidence consisted of blocking-related actions or proposals, cyber patrol, forensic standardization, infrastructure disruption, and international coordination. Taken together, these materials support the analytical inference that enforcement contributed to reducing the harmful digital presence of online gambling and to maintaining a more orderly digital environment for lawful activity. Even so, the corpus does not provide a direct quantitative measure of digital trust or cyber resilience. Accordingly, digital ecosystem integrity is used here as an interpretive public-value dimension based on proxy indicators rather than as a standardized measured outcome.

Institutional Mechanisms and Constraints

The third set of findings concerned the mechanisms through which strategic capability was translated into public value, and the constraints that limited that translation.

The first mechanism was intelligence to enforcement. Cyber patrol, public reporting, transaction signals, and inter-agency information were converted into investigative leads, case prioritization, target selection, and network mapping. In the Indonesian case, intelligence did not remain descriptive. It fed directly into investigation and operational decision-making.

The second mechanism was coordination to financial disruption. The retained corpus showed that the Indonesian National Police relied on coordination with PPATK, the Ministry of Communication and Digital Affairs, OJK, Bank Indonesia, and other agencies to move from case handling to broader disruption. Through this mechanism, criminal investigation was linked to account freezing, payment supervision, content intervention, and asset tracing. Financial disruption therefore emerged from the institutional combination of police authority, financial intelligence, and digital-governance intervention rather than from police action alone.

The third mechanism was public reporting and preventive education. Patrolisiber.id, community outreach, public campaigns, and volunteer networks converted social participation into enforcement support and preventive capacity. This mechanism linked societal cooperation with institutional reach. The direct documentary evidence supports widened informational reach, early detection support, and preventive exposure reduction. It does not directly demonstrate the level of institutional trust produced by those activities.

The fourth mechanism was digital ecosystem stewardship. Blocking-related actions, infrastructure disruption, forensic standardization, and international coordination can be interpreted as supporting the maintenance of digital order beyond case disposal alone. In this article, this mechanism is treated as an interpretive extension grounded in proxy indicators rather than as a directly measured ecosystem outcome.

At the same time, the retained corpus revealed several persistent constraints. The first was digital anonymity, including the use of VPNs, IP masking, spoofing, encrypted communications, TOR, and dark-web infrastructures. The second was cryptocurrency-related complexity, including mixers, decentralized exchanges, and privacy coins that complicated tracing. The third was dispersed banking and cross-border regulatory fragmentation, which limited the speed and reach of financial and legal intervention. The fourth was internal capability pressure, including uneven personnel development, technology dependence, and the need for continual capability renewal in a rapidly evolving threat environment.

Taken together, these findings portray online gambling enforcement in the Indonesian case as a capability-driven public-sector process in which criminal investigation, financial disruption, preventive outreach, and digital-order stewardship were linked within one institutional response. However, not all public-value claims rest on the same evidentiary strength. Economic protection is the most directly supported dimension, social protection is supported strongly at the level of prevention and reporting reach, and digital ecosystem integrity remains the most interpretive dimension of the analysis.

This section interprets the findings within the evidentiary limits of a qualitative document-based single-case study. Three levels of claim are distinguished. First, the retained public corpus directly evidenced a recurrent configuration of intelligence, forensic, coordinating, participatory, and adaptive investigative capacities. Second, the study interprets these capacities through a public value lens to explain their significance beyond case-processing outputs. Third, the article offers a bounded theoretical extension concerning public participation as an operational enabler and digital ecosystem integrity as an interpretive dimension of value, while acknowledging that some claims rest on proxy indicators rather than direct measurement.

Interpretation of Key Findings

The most directly evidenced contribution of the case is that online gambling enforcement in Indonesia was organized around a layered capability architecture rather than a single operational instrument. Integrated digital intelligence, accredited digital forensics, inter-agency coordination, public participation and reporting reach, and adaptive legal-investigative capability appeared recurrently

across the retained corpus as stable combinations of routines, expertise, institutional support, and coordinated action. This suggests that strategic capability in the case was system-based and relational rather than purely technological.

A second interpretive conclusion is that this capability configuration can be understood through a public value lens. The documentary evidence is strongest for economic protection because the retained corpus reports seizures, frozen accounts, follow-the-money intervention, and cross-agency indicators of reduced financial circulation. The evidence for social protection is also substantial because the corpus records preventive education, reporting channels, and outreach to schools and community organizations. By contrast, the evidence for digital ecosystem integrity is more indirect because it rests on proxy indicators such as blocking-related action, cyber patrol, forensic standardization, infrastructure disruption, and international coordination. The public value lens therefore adds explanatory leverage by showing how enforcement can be interpreted in terms of protection, prevention, and digital-order stewardship rather than only administrative outputs.

The case also clarifies the distinction between public participation and trust. The retained documents directly show that public reporting channels, volunteer networks, and outreach programs widened informational reach and preventive capacity. What they do not directly show is the magnitude of institutional trust, legitimacy, or public confidence among the population. A cautious reading is therefore that participation functioned as an operational enabler in the case, while any effect on trust remains plausible but unmeasured. This distinction is important because it keeps the discussion grounded in the evidentiary limits stated in the method.

A further interpretive lesson concerns technology. The case does not support a technology-determinist reading of enforcement. Digital intelligence systems, forensic infrastructure, and blocking-related intervention became strategically meaningful only when embedded in organizational routines, legal authority, professional competence, and inter-agency coordination. In this sense, the Indonesian case suggests that technological assets by themselves did not produce public value. Public value became possible only when those assets were organizationally supported and linked to broader institutional arrangements. This interpretation is consistent with studies emphasizing that digital transformation becomes strategically effective only when technological tools are supported by organizational alignment and capability configuration (Hasan et al., 2023; Simamora et al., 2024).

The findings also support a disruption-oriented understanding of cybercrime policing, but in a bounded and case-specific sense. The retained corpus shows a movement beyond surface-level disruption such as blocking toward deeper financial intervention through asset seizure, account freezing, and coordinated cross-agency action. This supports prior arguments that cybercrime enforcement increasingly targets infrastructure, money flows, and enabling systems rather than visible offenders alone (Collier et al., 2021; Curtis & Oxburgh, 2023; Khan, 2024). At the same time, the present study adds an interpretive layer by suggesting that such disruption can be read not only as a policing tactic but also as a public-sector mechanism of economic protection and preventive governance.

Finally, the reframing of the planet dimension as digital ecosystem integrity should be understood as a cautious conceptual extension rather than a settled measurement framework. In the Indonesian case, the idea is analytically useful because online gambling was associated with harmful digital presence, predatory infrastructures, and repeated pressure on digital order. Even so, the retained documents do not directly measure digital trust or ecosystem health in a standardized way. The discussion therefore treats digital ecosystem integrity as a bounded interpretive dimension supported by the logic of the case, not as a universally validated evaluative metric.

Comparison with Previous Studies

These findings are consistent with prior public-sector strategy research showing that public organizations can develop distinctive capacities when mandate, expertise, and institutional arrangements are aligned (Bryson et al., 2007). The case also fits collaborative-governance scholarship, especially the view that complex public problems require linked intervention among multiple actors rather than isolated action by a single agency (Bryson et al., 2006; Emerson et al., 2012). In the Indonesian case, online gambling enforcement appears to have become more effective when investigation, financial intelligence, payment oversight, content intervention, and cyber governance were connected within a coordinated architecture.

The findings also resonate with cybercrime-policing research that emphasizes expertise integration, adaptive enforcement, and disruption strategies in digital-crime settings(Whelan et al., 2024, 2025). However, the present study differs from much of that literature in one important respect. Previous studies often focus on operational challenges, investigative tactics, or institutional constraints. This study instead interprets those same processes through the relationship between strategic capability and public value. That move is not a direct test of public value theory. It is a bounded analytical extension based on a document-based single case.

Compared with digital-forensics literature, the present study reinforces the importance of standardization, accredited procedures, and laboratory credibility in supporting evidentiary quality (Tully et al., 2020). At the same time, the Indonesian case suggests a further interpretive implication. Accredited digital forensics may also contribute to public value because it strengthens institutional reliability within cyber investigation. That interpretation is plausible and consistent with the case materials, but its broader validation would require

comparative research and direct stakeholder evidence.

Theoretical and Practical Implications

Theoretically, the study contributes in three ways. First, it brings strategic capability and public value into one analytical conversation in a cyber law-enforcement setting. Second, it shows how a police-centered enforcement case can be read as a capability-to-value relationship rather than only as a sequence of legal outputs. Third, it proposes digital ecosystem integrity as a cautious public-sector extension of the planet dimension in the Triple Bottom Line. This last contribution remains provisional and requires further conceptual and empirical refinement.

Practically, the evidence supports a distinction between short-term institutional actions and longer-term strategic reforms. In the short term, the strongest evidence supports strengthening integrated digital intelligence, preserving accredited digital-forensic capacity, maintaining structured financial-disruption routines across agencies, and consolidating public reporting and preventive education channels. These actions follow directly from capabilities that already recur across the retained corpus and that appear central to the present enforcement architecture.

In the longer term, the case points toward deeper reforms in specialist career pathways, structured knowledge management, cross-border financial tracing, and capability renewal for rapidly evolving technologies. These reforms are strategically important because they respond to the constraints identified in the findings. However, they are more aspirational in evidentiary terms, because they extend beyond what the documents directly demonstrate and instead represent forward-looking institutional responses to documented pressures.

More broadly, the case suggests that the durability of strategic capability in public-sector cyber law enforcement depends on continual renewal, coordinated institutional support, and stable channels of public participation. The Indonesian case therefore supports a view of capability as something that must be maintained through learning, alignment, and adaptive reconfiguration rather than treated as a fixed stock of technical assets.

Limitations and Cautions

Several limitations remain important for interpreting the discussion. First, the study employed a qualitative document-based single-case design. The findings are therefore analytically transferable rather than statistically generalizable. Second, the study relied heavily on publicly released institutional documents. Even with cross-document corroboration and interpretive caution, institutional reporting bias cannot be fully excluded. Third, some claims, especially those related to reduced financial circulation, participation effects, and digital ecosystem integrity, necessarily rely on proxy indicators and interpretive inference rather than direct measurement. Fourth, the study did not incorporate interviews or public-perception data, which means that subjective experiences, organizational tensions, and the public's own assessment of trust or legitimacy remain outside the present evidence base.

Recommendations for Future Research

Future research should extend the present analysis through comparative multi-case work, longitudinal designs, and mixed-method approaches. Comparative studies across cybercrime units or jurisdictions would help distinguish context-specific from more transferable patterns. Longitudinal work would be especially valuable for tracking how strategic capability is renewed, weakened, or reconfigured over time. Mixed-method research that combines documentary analysis with investigator interviews, regulator perspectives, and public-perception data would also be essential for testing the presently unmeasured claims concerning trust, legitimacy, and ecosystem-level outcomes. In addition, future work should develop more robust indicators for digital ecosystem integrity so that the concept can move from interpretive usefulness toward stronger evaluative precision.

Conclusion

This study examined online gambling enforcement in Indonesia as a qualitative document-based single case centered on the Indonesian National Police, with the Directorate of Cyber Crime of the Criminal Investigation Agency serving as the focal operational unit. The documentary evidence suggests that enforcement in this setting was organized around a recurrent capability configuration comprising integrated digital intelligence, accredited digital forensics, inter-agency coordination, public participation and reporting reach, and adaptive legal-investigative capability. Read through a public value lens, this capability configuration can be interpreted as contributing to economic protection, social protection, and, more cautiously, digital ecosystem integrity.

The principal analytical contribution of the article lies in clarifying the relationship between strategic capability and public value in a public-sector cyber law-enforcement setting. In the Indonesian case, online gambling enforcement can be understood not only as criminal suppression, but also as a coordinated institutional process linking investigation, financial disruption, preventive outreach, and digital-order stewardship. Within the limits of the present evidence base, economic protection is the most directly supported dimension, social protection is supported strongly at the level of prevention and reporting reach, and digital ecosystem integrity remains the most interpretive dimension because it rests on proxy indicators rather than direct standardized measurement.

These conclusions should not be read as broad causal verification beyond the present case. Rather, they offer a bounded explanation of how police capability may be organized around public value considerations in online

gambling enforcement. In practical terms, the evidence most directly supports continued strengthening of integrated digital intelligence, accredited digital forensics, structured cross-agency financial disruption, and public reporting and preventive education channels. Longer-term reforms in specialist career pathways, knowledge management, and capability renewal also remain important, although they should be understood as forward-looking strategic implications rather than directly measured outcomes of the study. Future research can build on this explanation through comparative, longitudinal, and mixed-method designs that test these interpretations more directly.

Author contributions

Arus Reka Prasetia conceived the study, conducted the literature review, curated and analyzed the documentary data, developed the analytical framework, prepared the original draft, and revised the manuscript throughout the writing process. Puspo Dewi Dirgantari contributed to conceptual refinement, methodological direction, analytical validation, substantive supervision, and critical review and editing of the manuscript. Both authors discussed the findings, approved the final version of the manuscript, and agreed to be accountable for all aspects of the work.

Acknowledgements

The authors gratefully acknowledge the Doctoral Program in Management Science, Faculty of Economics and Business Education, Universitas Pendidikan Indonesia, Bandung, Indonesia, for its academic environment and institutional support. The authors also acknowledge publicly accessible institutional materials released by the Directorate of Cyber Crime (Dittipidsiber) of the Criminal Investigation Agency (Bareskrim), Indonesian National Police, that were relevant to this study. All interpretations and conclusions presented in this article remain those of the authors.

References

Bareskrim Polri. (2026). *Capaian Kinerja Dittipidsiber dalam Pemberantasan Judi Online 2022–2024*.

Bryson, J. M., Ackermann, F., & Eden, C. (2007). Putting the Resource-Based View of Strategy and Distinctive Competencies to Work in Public Organizations. *Public Administration Review*, *67*(4), 702–717. https://doi.org/10.1111/j.1540-6210.2007.00754.x

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2006). The Design and Implementation of Cross-Sector Collaborations: Propositions from the Literature. *Public Administration Review*, *66*(s1), 44–55. https://doi.org/10.1111/j.1540-6210.2006.00665.x

Bryson, J. M., Sancino, A., Benington, J., & Sørensen, E. (2017). Towards a Multi-Actor Theory of Public Value Co-Creation. *Public Management Review*, *19*(5), 640–654. https://doi.org/10.1080/14719037.2016.1192164

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2021). Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement through a Market for Cybercrime Services. *Policing and Society*, *32*(1), 103–124. https://doi.org/10.1080/10439463.2021.1883608

Curtis, J., & Oxburgh, G. (2023). Understanding Cybercrime in "Real World" Policing and Law Enforcement. *The Police Journal*, *96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Emerson, K., Nabatchi, T., & Balogh, S. (2012). An Integrative Framework for Collaborative Governance. *Journal of Public Administration Research and Theory*, *22*(1), 1–29. https://doi.org/10.1093/jopart/mur011

Feeney, M. K., & Mughan, S. (2025). Policing, Technology, and Public Values: A Public Administration Research Agenda. *Perspectives on Public Management and Governance*, *8*(1), 12–26. https://doi.org/10.1093/ppmgov/gvae011

Fisher, M. L., Piper, T., Fitzpatrick, M., Mavi, S., Retzer, A., Bradbury-Jones, C., Montgomery, P., Melendez-Torres, G. J., Kirby, J., Chandan, J. S., & Bedford, K. (2025). Legal and Regulatory Responses to Online Gambling Harms: A Scoping Review of Evidence. *Harm Reduction Journal*, *22*, 163. https://doi.org/10.1186/s12954-025-01292-y

Hasan, P. P., Hurriyati, R., & Dirgantari, P. D. (2023). Strategi Value Delivery Process pada Pemasaran Digital di Sektor Publik. *Jurnal Wacana Kinerja: Kajian Praktis-Akademis Kinerja Dan Administrasi Pelayanan Publik*, *26*(1), 113–128. https://doi.org/10.31845/jwk.v26i1.787

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, *13*(4), 44. https://doi.org/10.3390/laws13040044

Kitchener, M., & Ashworth, R. (2025). Strategizing Public Value. *Public Management Review*. https://doi.org/10.1080/14719037.2025.2538067

Moore, M. H. (1995). *Creating Public Value: Strategic Management in Government*. Harvard University Press.

O'Flynn, J. (2007). From New Public Management to Public Value: Paradigmatic Change and Managerial Implications. *Australian Journal of Public Administration*, *66*(3), 353–366. https://doi.org/10.1111/j.1467-8500.2007.00545.x

Prasetia, A. R., Muchamad, W., Noraga, G. B., Suryadi, E., & Rasto. (2026). A Systematic Literature Review on Integrating Ethics and Axiology into Organizational Digital Transformation Strategies. *Novatio: Journal of Management Technology and Innovation*, *4*(1), 1–21. https://doi.org/10.61978/novatio.v4i1.1259

Satgas Pemberantasan Perjudian Daring. (2025). *Laporan Kinerja Satgas Pemberantasan Perjudian Daring Periode Juni 2024–Januari 2026*.

Simamora, S. C., Rahayu, A., & Dirgantari, P. D. (2024). Driving Digital Transformation in Small Banks with VRIO Analysis. *Jurnal Aplikasi Bisnis Dan Manajemen*, *10*(1), 99–109. https://doi.org/10.17358/jabm.10.1.99

Stoker, G. (2006). Public Value Management: A New Narrative for Networked Governance? *The American Review of Public Administration*, *36*(1), 41–57. https://doi.org/10.1177/0275074005282583

Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., & Watson, T. (2020). Quality Standards for Digital Forensics: Learning from Experience in England & Wales. *Forensic Science International: Digital Investigation*, *32*, 200905. https://doi.org/10.1016/j.fsidi.2020.200905

Wardle, H., Degenhardt, L., Marionneau, V., Reith, G., Livingstone, C., Sparrow, M., Tran, L. T., Biggar, B., Bunn, C., Farrell, M., Kesaite, V., Poznyak, V., Quan, J., Rehm, J., Rintoul, A., Sharma, M., Shiffman, J., Siste, K., Ukhova, D., … Saxena, S. (2024). The Lancet Public Health Commission on Gambling. *The Lancet Public Health*, *9*(11), e950–e994. https://doi.org/10.1016/S2468-2667(24)00167-1

Whelan, C., Dupont, B., Harkin, D., Martin, J., Miccelli, M., & Villeneuve-Dubuc, M.-P. (2024). Expertise Integration in Cybercrime Policing: Exploring Civilian Career Lifecycles. *Deviant Behavior*. https://doi.org/10.1080/01639625.2024.2357810

Whelan, C., Martin, J., Dupont, B., & Harkin, D. (2025). "The Name of the Game": Policing Perspectives on Cybercrime Disruption. *Police Practice and Research*. https://doi.org/10.1080/15614263.2025.2523522

Winter, S. G. (2003). Understanding Dynamic Capabilities. *Strategic Management Journal*, *24*(10), 991–995. https://doi.org/10.1002/smj.318

Wu, L., Peng, Q., & Lemke, M. (2023). Research Trends in Cybercrime and Cybersecurity: A Review Based on Web of Science Core Collection Database. *International Journal of Cybersecurity Intelligence and Cybercrime*, *6*(1), 5–28. https://doi.org/10.52306/OZMB2721

Zollo, M., & Winter, S. G. (2002). Deliberate Learning and the Evolution of Dynamic Capabilities. *Organization Science*, *13*(3), 339–351. https://doi.org/10.1287/orsc.13.3.339.2780