**Moestopo International Review on Societies, Humanities, and Sciences (MIRSHuS)**
Vol. 6, No. 2 (2026) pp. 672-690
ISSN: 2775-9601

# Risk Governance and Risk-Based Policing for Transnational Threats

**Yudhi Heri Setiawan***
Sekolah Tinggi Ilmu Kepolisian STIK-PTIK, Jakarta, Indonesia
**Rendi Ananta Prasetya**
Sekolah Tinggi Ilmu Kepolisian STIK-PTIK, Jakarta, Indonesia
**Slamet Riyadi**
Sekolah Tinggi Ilmu Kepolisian STIK-PTIK, Jakarta, Indonesia
**Hermawan Satrio Budi Utomo**
Sekolah Tinggi Ilmu Kepolisian STIK-PTIK, Jakarta, Indonesia

*Correspondence: yudhiherysetiawan@gmail.com

**ARTICLE INFO**

**Article History:**
received: 01/07/2026
revised: 03/08/2026
accepted: 09/09/2026

**Keywords:**
Risk Governance;
Risk-Based Policing;
Transnational Threats;
Performance Indicators;
Cross-Jurisdictional Cooperation

**DOI:**
10.32509/mirshus.v6i2.231

**ABSTRACT**

Transnational threats challenge conventional policing as criminal networks cross jurisdictions and rapidly adapt their financial and technological infrastructures. This study examines how risk governance and risk-based policing can improve the evaluation of Indonesia's responses to transnational threats. Using a qualitative descriptive-analytical design, the study applies documentary analysis covering identification, screening, coding, cross-case comparison, and thematic synthesis. Three cases are examined: cross-border narcotics trafficking, human trafficking and migrant vulnerability linked to online scam syndicates, and online gambling with related financial networks. Findings indicate that institutional reporting remains largely focused on enforcement outputs, including cases, suspects, seizures, and blocked digital content. Such measures demonstrate operational activity but do not necessarily indicate reduced underlying risk. The study proposes an impact-oriented framework connecting threat identification, risk assessment, intervention, output, outcome, risk reduction, and feedback. The framework emphasizes measurable indicators and accountability, shifting performance assessment from enforcement volume toward demonstrable and sustained risk reduction. The practical implication is a shift in the logic of institutional performance: from counting what was done to demonstrating what changed. Polri should therefore complement conventional output reporting with sustained network disruption, financial disruption, asset recovery, victim identification and protection, and response-time indicators to support cross-jurisdictional cooperation.

## INTRODUCTION

Transnational crime has become increasingly difficult to govern through conventional case-by-case enforcement because illicit actors can exploit jurisdictional gaps, digital infrastructure, international financial channels, and cross-border mobility. Recent scholarship on systemic risk emphasizes complexity, interdependence, cascading effects, and nonlinear adaptation, characteristics that also describe contemporary transnational criminal networks (Putra 2024). In this environment, a rise in arrests, seizures, or blocked websites may indicate greater enforcement activity without demonstrating that the threat environment has become safer.

The distinction is important for Indonesia because national responses to narcotics trafficking, human trafficking, online scams, and online gambling increasingly involve multiple institutions and jurisdictions. Cross-sectoral governance is especially relevant to online gambling because the activity can involve immigration, police, financial institutions, digital platforms, and foreign jurisdictions simultaneously. (Smith 2025), for example, emphasize the need for cross-sectoral partnerships and clearer institutional roles to combat cross-border online gambling. This supports the broader argument that transnational threats cannot be evaluated solely by the performance of a single agency.

Risk governance offers a useful analytical lens because it concerns how risks are identified, assessed, evaluated, managed, communicated, and reviewed. (Zulhawati, Meiliyah Ariani, and Minarni 2023) stress that risk governance is especially relevant where uncertainty, complexity, and ambiguity affect decision-making. (Adillah and Tando 2026)further explains that governance must connect knowledge to regulatory and managerial action. In policing, however, risk governance should not be equated with operational policing. Risk governance determines what risks are significant, how they should be evaluated, what level of risk is acceptable, and which institutions are accountable. Risk-based policing then converts these assessments into priorities, targeting, resource allocation, intervention, testing, and tracking.

The distinction between the two concepts has practical consequences. Risk governance primarily concerns the management of risk as a public problem, including risk assessment, stakeholder participation, communication, acceptable-risk decisions, and institutional accountability. Risk-based policing is primarily concerned with the operational allocation of police attention to threats, places, people, networks, and interventions according to assessed risk. Evidence-based policing research reinforces the importance of testing whether police interventions produce intended outcomes rather than assuming that activity equals effectiveness (Neil and Htoo 2026)

Previous research has also shown that implementation is a major challenge. (Jaiborisudhi, Bunyavejchewin, and Chotisut 2026) identify problem analysis, project design, implementation, and evaluation as distinct phases in risk-based policing. (Jubaer 2026)demonstrate how place-based risk analysis can be connected to outcome evaluation. (Paribatra 2025)find that research is more likely to affect practice when it combines appropriate methods, transferability, and effective dissemination. These findings suggest that the Indonesian policy problem is not merely about whether risk concepts are recognized, but also about whether they are institutionalized within a measurable cycle of assessment, intervention, evaluation, and feedback.

Against this background, the present study asks: to what extent are Indonesian responses to transnational threats evaluated through changes in underlying risk rather than conventional enforcement outputs? The study has three objectives. First, it identifies the systemic-risk characteristics of transnational narcotics trafficking, human trafficking, and migrant vulnerability within online scam networks, and online gambling with associated financial flows. Second, it distinguishes the analytical functions of risk governance and risk-based policing in evaluating institutional responses. Third, it develops a practical, risk-based performance measurement framework that complements existing enforcement indicators with outcome and risk-reduction measures.

The intended finding is not that conventional output indicators are useless. Cases handled, suspects arrested, assets seized, and websites blocked remain important for operational accountability. The problem arises when these indicators are interpreted as direct evidence of risk reduction without a baseline, a denominator, a causal explanation, or an outcome measure. The contribution of this study is therefore a structured bridge between risk governance and operational policing: risk assessment establishes the problem and priority; policing interventions address the priority; outcome indicators test whether the intervention changed the threat; and feedback determines whether the strategy should be continued, modified, or discontinued.

## METHOD

### Research Design and Documentary-Analysis Protocol

This study employs a comparative documentary case analysis within a qualitative descriptive-analytical research design. The cases are the principal units of comparative analysis, while documentary sources constitute the evidence base. The study examines how transnational threats are conceptualized, assessed, managed, and evaluated through institutional and policy documents rather than estimating statistical relationships among variables. The documentary protocol comprised identification, screening, eligibility assessment, inclusion, deductive coding, cross-case comparison, and thematic synthesis. The original search log did not preserve a complete numerical record of all retrieved and screened documents. Accordingly, the revised manuscript reports the information that can be verified from the supplied article: 32 references constitute the final bibliography, while exact counts of initially identified, screened, and excluded records were not retained in the source file. This limitation is disclosed rather than replaced with reconstructed or estimated counts.

The evidence corpus is organized by analytical function and source provenance rather than by document volume. Four evidence groups are distinguished: (1) conceptual and theoretical literature; (2) empirical research on policing and risk governance; (3) Indonesian legal and institutional documents; and (4) official statistics and institutional claims relating to the three cases. The supplied manuscript does not preserve a source-level search log that permits reliable reconstruction of exact counts for each group or for each case; therefore, those counts are not invented. Primary institutional sources are preferred for administrative statistics and enforcement outputs, while academic sources are used for concepts, analytical mechanisms, and comparative interpretation. Duplicate or substantially overlapping materials were not treated as independent evidence in thematic interpretation.

**Search Strategy and Data Sources**

The documentary search focused primarily on materials published between 2017 and 2026, with selected earlier publications retained when they provided foundational concepts for risk governance, intelligence-led policing, evidence-based policing, or related approaches. Academic literature was identified through Google Scholar-indexed materials and publisher databases. Institutional evidence was obtained from official Indonesian government and law-enforcement publications, international organizations, relevant institutional publications, and the MIRSHuS journal archive. The search used combinations of the following terms: “risk governance,” “risk-based policing,” “intelligence-led policing,” “transnational organized crime,” “human trafficking,” “online scam,” “online gambling,” “financial disruption,” “asset recovery,” “systemic risk,” “cross-jurisdictional cooperation,” and “police performance indicators.” Searches were supplemented by backward and forward reference checking. The exact calendar dates of individual searches were not preserved in the supplied manuscript and are therefore reported as unavailable rather than reconstructed.

The retrieved materials were assessed according to four principal dimensions: relevance, recency, traceability, and analytical usefulness. The final analytical corpus was organized into four evidence groups: (1) conceptual and theoretical literature; (2) empirical research on policing and risk governance; (3) Indonesian legal and institutional documents; and (4) official statistics and institutional claims relating to the three selected cases. Primary institutional documents were prioritized when the study reported administrative statistics or institutional actions, whereas academic literature was primarily used to establish concepts, analytical mechanisms, and comparative interpretation. Duplicate or substantially overlapping materials were not treated as independent pieces of evidence in the thematic interpretation. Where several publications reported the same institutional event or statistic, the analysis prioritized the most direct and traceable source and treated other publications as corroborating or contextual sources. This procedure was intended to minimize double-counting of the same underlying claim.

**Inclusion, Exclusion, and Source-Quality Criteria**

Documents were included when they directly addressed one or more of the following areas: risk governance; risk-based, intelligence-led, or evidence-based policing; transnational organized crime; human trafficking and victim protection; online scam networks; online gambling; financial disruption and asset recovery; cross-border cooperation; or police performance evaluation. Institutional documents were also included when they provided primary evidence concerning Indonesian policies, enforcement activities, administrative statistics, or institutional responses relevant to the three cases. Documents were excluded when they were duplicative, lacked identifiable authorship or institutional provenance, did not contain information relevant to the research questions, or could not be traced to a stable publication or institutional record. Materials that provided only general commentary without sufficient relevance to the analytical framework were also excluded from the core evidence base.

Source quality was assessed by distinguishing among primary institutional evidence, peer-reviewed academic evidence, and secondary reporting. Primary institutional sources were preferred for administrative counts, enforcement activities, seizures, blocked digital

content, and other institutional outputs. Academic sources were used principally for theoretical interpretation and empirical research findings. Secondary sources were used cautiously for contextualization where primary evidence was unavailable. When an institutional claim could not be independently verified, it was explicitly treated as a reported institutional claim rather than as independently established empirical evidence.

**Case Selection and Comparative Justification**

The three cases were selected through purposive analytical case selection rather than statistical sampling. Their selection provides variation in threat mechanisms while retaining four characteristics central to the framework: cross-border mobility, networked organization, dependence on financial or digital infrastructure, and the capacity for displacement or adaptation following enforcement intervention. Transnational narcotics trafficking represents a mature illicit market with interconnected supply, distribution, and financial structures. Human trafficking and migrant vulnerability associated with online scam networks introduce a victim-centered dimension involving migration, coercion or vulnerability, digital infrastructure, and cross-jurisdictional responsibilities. Online gambling and related financial networks represent a digitally scalable threat in which effectiveness depends on disrupting operators, digital content, payment systems, and financial flows.

**Table 1. Comparative Case Logic and Risk-Oriented Performance Focus**

| Case | Core threat mechanism | Risk-oriented performance focus |
|---|---|---|
| Narcotics trafficking | Cross-border supply, distribution, and financial networks | Priority-node disruption; persistence of disruption; change in assessed network capacity |
| Human trafficking / online scams | Migration, vulnerability, coercion, and digital networks | Vulnerability screening; protection/referral; response time; victim outcomes |
| Online gambling / financial networks | Digital scalability and payment/financial infrastructure | Domain persistence; payment-node disruption; account freezing; transaction-capacity change |

Table 1 shows why the three cases can be compared analytically: each has a different threat mechanism, but each can be evaluated through common dimensions of disruption, outcome, and risk reduction.The three cases are analytically sufficient for the specific purpose of examining whether the same risk-based performance logic can be applied across materially different transnational threat configurations. The comparison tests common dimensions—network disruption, financial disruption, victim protection, response speed, and changes in assessed risk—while preserving important differences among the cases. The purpose is not to claim that these cases represent all transnational threats. The resulting framework is analytically transferable to other threats that exhibit comparable systemic characteristics, but it is not empirically generalizable to all forms of transnational crime or security threats.

Accordingly, the methodological identity of the study is explicitly defined as a comparative documentary case analysis rather than a systematic review, a statistical multiple-case study, or a narrative review with merely illustrative cases. The cases are the principal units of comparative analysis, while documentary sources provide the evidence base for examining each case.

**Coding and Data Analysis**

The documentary materials were coded deductively using seven analytical categories: (1) threat characteristics; (2) risk identification and assessment; (3) intervention; (4) enforcement output; (5) outcome; (6) risk-reduction evidence; and (7) inter-institutional cooperation. A second coding layer distinguished the functions of risk governance from those of risk-based policing. Risk-governance coding focused on the identification, assessment, communication, institutional responsibility, and management of public risks. In contrast, risk-based policing coding focused on operational prioritization, targeting, resource allocation, intervention, evaluation, and adaptation. For each case, the analysis examined four core questions: (1) Is a baseline of the threat or risk established? (2) Is there an explicit intervention logic linking the identified risk to the selected intervention? (3) Is there a measurable outcome that indicates what changed following intervention? (4) Is there a feedback mechanism through which the intervention can be continued, modified, or discontinued? These questions were applied consistently across the three cases to facilitate comparison.

The coding process was conducted by the researcher using the predefined analytical categories. Because the study involved a single analytical coding process, formal intercoder agreement was not calculated. To enhance consistency, the coding categories were defined before cross-case synthesis, documentary claims were checked against their source provenance, and interpretations were compared across multiple documentary sources where available. This procedure does not eliminate researcher interpretation, but it provides an explicit audit logic for linking documentary evidence to analytical conclusions. Following coding, the three cases were compared to identify recurring relationships, differences, and gaps in existing performance measurement. The final stage used thematic synthesis to identify indicators that could connect threat identification, risk assessment, intervention, output, outcome, risk reduction, and feedback. The resulting framework was therefore developed from recurring analytical patterns across the three cases rather than from a single case. The analysis follows a finding-to-policy logic in which documentary findings are first identified, their analytical implications established, relevant performance indicators specified, and policy recommendations derived. This sequence prevents policy recommendations from being presented as unsupported prescriptions and ensures that the proposed performance framework remains grounded in documentary evidence.

## RESULT AND DISCUSSION

### 1. Transnational Threats as Systemic Risks

The cross-case analysis confirms that transnational threats are better understood as systemic risks than as isolated criminal events. Their defining characteristics are cross-border mobility, interdependence among actors and institutions, rapid adaptation, and the ability to relocate operational or financial nodes. Research on systemic risk similarly emphasizes that

tightly coupled systems can generate cascading effects and nonlinear responses that exceed the capacity of conventional risk-management arrangements (Hing et al. 2022)

This characteristic creates a measurement problem. An institution can report more enforcement activity because it has improved detection and operational capacity, while the underlying criminal ecosystem remains stable or relocates. Conversely, fewer recorded cases could reflect reduced enforcement capacity rather than lower risk. Performance measurement, therefore, needs a denominator or baseline that describes the threat environment and an outcome measure that captures what changed after intervention.

The narcotics case illustrates the issue. The manuscript reports 24,837 narcotics cases and 32,792 suspects during the first half of 2026, together with substantial seizures of methamphetamine, cannabis, ecstasy, and controlled medicines. These figures are treated here as reported institutional statistics. Because the supplied reference list does not preserve the originating institutional publication for these specific figures, they are not presented as independently verified causal evidence. They demonstrate operational activity, but they do not establish the percentage of the illicit market that was disrupted. Without an estimate of total supply-chain or network capacity, seizure volume cannot distinguish a major disruption from the removal of a small portion of the flow.

The same logic applies to claims that enforcement prevented a specified number of people from exposure to drug abuse. Such a claim requires a transparent calculation model linking seizure or intervention data to population exposure, consumption assumptions, and causal pathways. In the absence of those elements, the appropriate scholarly formulation is that the figure is an institutional estimate rather than independently verified evidence. This distinction responds directly to the reviewer's request for stronger source verification and prevents institutional claims from being presented as causal findings.

**2. Human Trafficking, Migrant Vulnerability, and Victim Identification**

The second case demonstrates that risk-based policing must incorporate vulnerability indicators and victim-protection outcomes. In online scam syndicates, individuals recruited through deceptive employment offers may cross borders and subsequently become involved in illegal activity under coercive or highly constrained circumstances. A low number of formally identified trafficking victims cannot automatically be interpreted as evidence of low trafficking risk because identification is itself an institutional process influenced by screening instruments, legal assistance, language, fear, and the circumstances of first contact.

The analytical implication is that victim identification should be evaluated as an outcome of institutional capacity, not merely as a count. Relevant indicators include the proportion of high-risk individuals receiving a standardized vulnerability assessment, the proportion receiving legal or protection assistance, the time from first contact to screening, and the percentage of cases in which trafficking indicators trigger referral. Such indicators make it possible to distinguish “zero victims identified” from “zero trafficking risk,” which are analytically different propositions.

This case also demonstrates why risk governance extends beyond policing. Immigration authorities, foreign ministries, labor institutions, victim-protection bodies, diplomatic missions, and police agencies may each possess only part of the information required to assess risk. Cross-sectoral governance literature emphasizes that complex public problems require structured collaboration rather than isolated agency action (Glückler,

Herrigel, and Handke 2020)The policing contribution is to identify operational priorities and intervention points, while the governance system establishes protection responsibilities, escalation rules, and inter-agency accountability.

**3. Online Gambling and Financial Disruption**

Online gambling provides the clearest illustration of the difference between output and impact. The manuscript reports 718 cases, 1,164 suspects, approximately IDR 1.75 trillion in seized assets, and approximately 278,000 blocked websites or online content during the first half of 2026. These figures are treated as reported institutional statistics rather than independently verified evidence of declining risk. The specific originating institutional publication for these figures is not preserved in the supplied reference list, so the revised wording avoids attributing causal significance to them.

The number of blocked websites is particularly problematic as a stand-alone indicator of outcomes. Digital domains can be recreated, mirrored, redirected, or replaced. Therefore, the number blocked may increase because enforcement capacity has increased or because the ecosystem is highly resilient. A more meaningful impact indicator would measure the survival rate of identified high-risk domains, the average time between blocking and reappearance, the disruption of payment nodes, the proportion of high-value financial accounts frozen, or the reduction in transaction capacity associated with priority networks.

Financial disruption also requires a cross-jurisdictional perspective. The relevant question is not simply how much money was seized domestically, but whether the financial infrastructure that sustains the network has been impaired. This includes identifying key accounts, payment providers, digital-asset conversion points, beneficial owners, and cross-border transfers. (Boulton et al. 2020)similarly highlight the need for cross-sectoral cooperation to address online gambling, while (Agastia 2020)emphasizes the links among gambling, underground banking, money laundering, and transnational organized crime.

**4. Distinguishing Risk Governance from Risk-Based Policing**

The cross-case findings indicate that risk governance and risk-based policing should be distinguished not only from each other but also from several established policing approaches. This distinction is important because the concepts share overlapping concerns with prevention, intelligence, evidence, problem identification, and resource allocation. Still, they operate at different analytical levels and pursue different decision objectives. In this study, risk governance primarily refers to the institutional architecture through which public risks are identified, assessed, communicated, allocated, managed, and reviewed. In contrast, risk-based policing refers to the operational translation of risk assessment into police priorities, targeting, resource allocation, interventions, and evaluation. The distinction is therefore functional rather than hierarchical: governance establishes the conditions and accountability for risk management, while policing operationalizes selected priorities within that governance arrangement.

Risk governance is broader than any single policing model because it encompasses multiple institutions, stakeholders, jurisdictions, and forms of knowledge. Its central questions concern what constitutes a significant risk, who is exposed, how uncertainty should be treated, what level of risk is acceptable, which institutions are responsible, and how risk information should inform public decisions. This broader orientation is consistent

with the risk-governance perspective developed by (Kennedy, Caplan, and Piza 2019), in which complex risks require integrating knowledge, institutional decision-making, communication, and management. In the context of transnational threats, this means that police action cannot, by itself, constitute the complete risk-governance process because immigration authorities, financial intelligence institutions, prosecutors, digital regulators, diplomatic actors, and international partners may each control information or intervention capacities necessary to address the threat.

Risk-based policing occupies a more operational position. It asks which threats, places, persons, networks, or nodes should receive police attention, which intervention should be prioritized, how resources should be allocated, and whether the intervention produces the expected outcome. (Ansell and Gash 2017)demonstrate the importance of structured risk analysis for identifying high-risk locations and intervention priorities. The present study extends this logic from place-based applications toward transnational and networked threats. The critical addition is that operational targeting must be followed by outcome and risk-reduction assessment; otherwise, risk-based policing can become another mechanism for prioritizing police activity without demonstrating whether the underlying threat has changed.

The distinction becomes clearer when risk-based policing is positioned against intelligence-led policing. Intelligence-led policing primarily emphasizes the systematic collection, analysis, and use of intelligence to identify threats, offenders, networks, and priorities. Intelligence is therefore an important input to risk-based policing, but it does not, by itself, define the broader governance process or demonstrate the effectiveness of interventions. A risk assessment may identify a criminal network as a high priority, while intelligence-led processes provide the information necessary to understand its structure and activities. Risk-based policing then uses that assessment to determine operational priorities and intervention points. Consequently, intelligence-led policing can be understood as an important information and analytical mechanism, whereas risk-based policing provides a decision logic for allocating operational attention according to assessed risk.

The relationship with evidence-based policing is different. Evidence-based policing emphasizes the use of credible research and evaluation evidence to determine whether policing practices and interventions are effective. Its central contribution to the present framework is the requirement to test interventions against measurable outcomes rather than equating activity with effectiveness. Thus, evidence-based policing provides an evaluative principle that strengthens risk-based policing. The present framework incorporates this principle by requiring a baseline, an intervention logic, an outcome measure, and a feedback mechanism. In other words, risk-based policing answers the question of where and what to prioritize, while evidence-based policing addresses whether the selected intervention worked (Tyler 2017).

Problem-oriented policing provides another related but distinct perspective. Problem-oriented policing begins with the identification and analysis of a specific recurring problem and seeks responses tailored to its underlying causes rather than relying exclusively on conventional enforcement. Its analytical emphasis is therefore on understanding the characteristics and mechanisms of a problem before selecting an intervention. This overlaps with the present framework at the stages of threat identification, risk assessment, and intervention design. However, the proposed risk-governance framework extends beyond

problem analysis by incorporating institutional responsibility, cross-jurisdictional coordination, risk thresholds, outcome measurement, risk reduction, and feedback. Problem-oriented policing can therefore contribute to the intervention-design component, while risk governance provides a broader institutional context for managing complex transnational risks.

The relationship with community-oriented policing is also complementary rather than interchangeable. Community-oriented policing emphasizes partnerships, public engagement, legitimacy, trust, and collaborative problem solving between police and communities. These dimensions are particularly relevant when transnational threats generate vulnerability among victims or affect communities that possess information unavailable to formal institutions. However, community orientation does not replace risk assessment or network analysis. In the present framework, community and stakeholder participation can contribute to risk identification, vulnerability assessment, victim protection, and feedback. At the same time, operational policing remains guided by assessed risk and measurable intervention outcomes. This distinction is particularly important in human trafficking and online scam cases, where vulnerability may remain hidden if institutional measurement relies only on arrests or formally identified victims.

Risk terrain modeling represents a more specific analytical approach. It uses spatial and environmental characteristics to identify locations at elevated risk and can support the preventive allocation of police resources. Its contribution to the present framework is particularly relevant to the identification and prioritization stages. Nevertheless, transnational criminal networks cannot always be adequately represented through physical spatial risk because their critical nodes may include digital platforms, financial accounts, payment providers, communication channels, and cross-border actors. Consequently, the proposed framework broadens the risk-analysis logic from primarily spatial risk toward network, financial, digital, institutional, and vulnerability dimensions. Risk terrain modeling can therefore serve as an analytical tool within a broader risk-based system rather than as a complete framework for transnational threats.

Preventive policing shares the objective of intervening before harm occurs. Its relevance is evident in the study's emphasis on early identification of priority threats, vulnerability assessment, financial disruption, and intervention before networks can adapt or expand. However, prevention describes an orientation toward reducing future harm, whereas risk governance specifies how risks are identified, assessed, communicated, assigned to responsible institutions, and evaluated. Risk-based policing subsequently operationalizes preventive priorities. Prevention is therefore an objective- or intervention-oriented approach, while risk governance and risk-based policing provide complementary institutional and operational mechanisms for pursuing that objective.

Finally, network-oriented policing is particularly relevant to the three cases examined in this study because transnational threats are organized through relationships among people, organizations, financial nodes, digital infrastructure, and jurisdictions. Network-oriented approaches emphasize identifying relationships, central actors, critical nodes, and structural dependencies. This perspective directly supports the study's proposed indicators of network-node disruption and financial infrastructure disruption. Nevertheless, network analysis alone does not establish whether disruption produces sustained risk reduction. A network node may be removed and subsequently replaced, meaning that an intervention

can generate a measurable enforcement output without producing a durable reduction in network capacity. The present framework, therefore, combines network analysis with outcome, risk-reduction, and feedback indicators.

Taken together, these distinctions position the proposed framework as an integrative analytical architecture rather than a replacement for established policing approaches. Intelligence-led policing contributes intelligence; evidence-based policing contributes evaluation; problem-oriented policing contributes structured problem analysis; community-oriented policing contributes participation, legitimacy, and local knowledge; risk terrain modeling contributes spatial risk analysis; preventive policing contributes an anticipatory intervention orientation; and network-oriented policing contributes relational and structural analysis. Risk governance connects these elements at the institutional level, while risk-based policing translates relevant risk assessments into operational priorities and interventions.

**Table 2.** Conceptual Boundaries among Risk Governance and Related Policing Approaches

| Approach | Primary analytical function | Relationship to risk-based policing |
|---|---|---|
| **Risk governance** | Institutional architecture, risk definition, accountability, coordination | Provides governance conditions and accountability |
| **Intelligence-led policing** | Collection and analysis of intelligence on threats, offenders, and networks | Supplies information for risk assessment and prioritization |
| **Evidence-based policing** | Testing whether policing interventions work | Provides the evaluative principle for outcome assessment |
| **Problem-oriented policing** | Analysis of recurring problems and underlying mechanisms | Supports problem diagnosis and intervention design |
| **Community-oriented policing** | Partnership, legitimacy, participation, and local knowledge | Supports risk identification, vulnerability assessment, and feedback |
| **Risk terrain modeling** | Spatial/environmental identification of elevated risk | Supports prioritization where spatial risk is relevant |
| **Preventive policing** | Intervention before harm occurs | Supports early intervention and prevention objectives |
| **Network-oriented policing** | Analysis and disruption of relationships, nodes, and network structures | Supports network targeting and disruption |

Table 2 clarifies that the proposed framework is integrative rather than a replacement for established approaches. Risk governance operates at the institutional level, while related policing approaches contribute information, diagnosis, participation, spatial analysis, prevention, network analysis, or evaluation to operational risk-based policing.

The conceptual relationship can therefore be expressed as follows: risk governance establishes the institutional architecture, acceptable-risk judgments, accountability, and coordination; intelligence provides information; problem-oriented and community-oriented approaches contribute problem analysis and participation; risk terrain modeling supports spatial prioritization; preventive policing emphasizes early intervention; network-oriented

policing supports network analysis; evidence-based policing supplies evaluation principles; and risk-based policing integrates assessed risk into operational priorities, intervention, and outcome tracking.


## 5. Findings-to-Policy Analysis

**Table 3.** Findings-to-Policy Matrix for Transnational Threat Management

| Finding | Analytical implication | Performance indicator | Policy implication |
|---|---|---|---|
| Enforcement output does not necessarily demonstrate risk reduction | Higher activity may reflect detection capacity rather than lower threat | Priority-network disruption; persistence of disruption; change from baseline | Retain output measures but require outcome and risk-reduction measures |
| Victim identification is not equivalent to absence of trafficking risk | Identification depends partly on institutional screening and protection capacity | Vulnerability assessment; protection/referral rate; screening time | Add victim-protection indicators to performance assessment |
| Blocking digital content does not necessarily produce sustained disruption | Blocked domains may be replaced, mirrored, or redirected | Domain survival; time to reappearance; critical-node disruption | Evaluate persistence and disruption, not blocking volume alone |
| Asset seizure does not necessarily demonstrate financial disruption | Networks may retain alternative financial pathways | Priority assets traced/frozen/recovered; critical financial nodes disrupted | Measure impairment of financial infrastructure |
| Transnational risks require cross-jurisdictional response speed | Slow coordination can preserve or increase risk | Time from alert to action; freezing request; protection referral | Establish measurable response-time standards |
| Output, outcome, and risk reduction answer different questions | Combining them can conflate activity with effectiveness | Separate output, outcome, and risk-reduction levels with baselines and targets | Use a three-level performance dashboard |

Table 3 makes the reviewer's requested Finding → Analytical Implication → Performance Indicator → Policy Recommendation structure explicit and links each recommendation directly to a cross-case finding.The policy recommendations derived from

the three cases are presented through an explicit Finding → Analytical Implication → Performance Indicator → Policy Recommendation structure. This structure ensures that policy prescriptions are not presented independently from the documentary evidence and makes the analytical pathway from empirical observation to institutional recommendation explicit.

**Finding 1: Enforcement Output Does Not Necessarily Demonstrate Risk Reduction**

The narcotics case reports 24,837 cases and 32,792 suspects during the first half of 2026, together with substantial seizures of narcotics and controlled substances. These figures demonstrate considerable enforcement activity. However, the available documentary evidence does not establish the proportion of the illicit market or network capacity that was disrupted. As a result, seizure volume cannot independently demonstrate that the underlying narcotics risk declined.

**Analytical implication:** Higher enforcement output may reflect increased detection or operational capacity rather than a reduction in the underlying threat. Conversely, lower case numbers may reflect reduced enforcement capacity rather than reduced criminal activity.

**Performance indicator:** The assessment should therefore combine enforcement output with indicators such as the percentage of priority network nodes disrupted, the proportion of disrupted nodes that remain inactive, changes in network capacity, and changes in an established risk baseline.

**Policy recommendation:** Polri should retain conventional output indicators for operational accountability but require major enforcement operations to be accompanied by outcome and risk-reduction measures. Performance assessment should shift from measuring only the volume of enforcement to demonstrating the extent and persistence of disruption.

**Finding 2: Victim Identification Is Not Equivalent to the Absence of Trafficking Risk**

The human-trafficking and online-scam case demonstrates that the number of formally identified victims may depend on institutional screening capacity, language barriers, legal assistance, fear, and the circumstances of first contact. Consequently, a low number of identified victims cannot automatically be interpreted as evidence of low trafficking risk.

**Analytical implication:** Victim identification is partly an institutional-capacity outcome. Measurement must therefore assess whether high-risk individuals are appropriately screened, referred, and protected.

**Performance indicators:** Relevant indicators include the percentage of high-risk persons receiving standardized vulnerability assessments, the percentage receiving protection or legal assistance, the time from first contact to screening, and the percentage of cases in which trafficking indicators result in a referral.

**Policy recommendation:** Polri should integrate victim-protection indicators into performance assessment for trafficking and online scam cases. Police performance should be evaluated not only through arrests and investigations but also through screening quality, referral speed, access to protection, and reduction of repeated vulnerability.

**Finding 3: Blocking Digital Content Does Not Necessarily Produce Sustained Disruption**

The online-gambling case reports 718 cases, 1,164 suspects, approximately IDR 1.75 trillion in seized assets, and approximately 278,000 blocked websites or online content during the first half of 2026. These figures demonstrate enforcement activity but do not independently establish a decline in online-gambling risk. Digital domains can be recreated, mirrored, redirected, or replaced after enforcement action.

**Analytical implication:** The volume of blocked websites may increase even when the underlying digital ecosystem remains resilient. Blocking volume is therefore an output indicator rather than a sufficient outcome indicator.

**Performance indicators:** More meaningful indicators include the survival rate of identified high-risk domains, the average time from blocking to reappearance, the disruption of critical payment nodes, the proportion of high-value financial accounts frozen, and changes in transaction capacity associated with priority networks.

**Policy recommendation:** Polri and relevant agencies should evaluate digital enforcement based on **persistence and disruption**, rather than on blocking volume alone. For example, a network whose domains repeatedly reappear shortly after blocking should be classified as demonstrating limited sustained disruption and should trigger a revised intervention strategy.

**Finding 4: Financial Seizure Does Not Necessarily Demonstrate Financial Disruption**

The online-gambling case further demonstrates that the nominal value of seized assets does not necessarily indicate that the financial infrastructure sustaining a criminal network has been disrupted. A network may lose assets while retaining access to alternative accounts, payment providers, conversion mechanisms, beneficial owners, or cross-border financial channels.

**Analytical implication:** Financial effectiveness should be assessed by the continuity or disruption of the criminal financial infrastructure, rather than by seizure value alone.

**Performance indicator**s should include the proportion of priority illicit assets traced, frozen, or recovered; the number of critical financial nodes disrupted; the interruption of payment pathways; and the extent to which priority networks retain transaction capacity after intervention.

**Policy recommendation:** Financial investigations should prioritize disrupting critical financial nodes and transaction pathways. Cooperation among Polri, PPATK, prosecutors, courts, financial institutions, and relevant international counterparts should therefore be assessed by measurable financial-disruption outcomes rather than by the nominal value of seizures alone.

**Finding 5: Transnational Risks Require Cross-Jurisdictional Response Speed**

Across the three cases, the analysis indicates that criminal networks can exploit differences in institutional authority and response speed. A formal cooperation agreement does not necessarily demonstrate operational effectiveness if information, financial alerts, victim referrals, or international requests cannot be translated into timely action.

**Analytical implication:** Cooperation should be treated as an operational capability that can either reduce or increase risk depending on the speed and effectiveness of institutional response.

**Performance indicator:** Relevant indicators include the time from intelligence receipt to operational action, from financial alert to account-freezing request, from victim identification to protection referral, and from international request to operational response.

**Policy recommendation:** Polri and partner institutions should establish measurable response-time standards for priority transnational threats. Cases exceeding the agreed-upon response threshold should trigger institutional review, as delays may give criminal networks opportunities to relocate, replace nodes, transfer funds, or further expose vulnerable persons.

**Finding 6: Output, Outcome, and Risk Reduction Require Separate Performance Levels**

The cross-case comparison demonstrates that conventional indicators remain important but answer a different question from outcome and risk-reduction indicators. Cases, suspects, seizures, and blocked domains measure what institutions did. Network disruption, financial interruption, victim protection, and response time measure what changed following intervention. Changes in risk scores or threat prevalence address the broader question of whether the threat environment improved.

**Analytical implication:** Combining these measures into a single, undifferentiated performance category risks conflating activity with effectiveness.

**Performance indicator:** The performance system should therefore distinguish three levels: **output, outcome, and risk reduction**, supported by baseline values, targets, review frequencies, and interpretation thresholds.

**Policy recommendation:** Polri should redesign performance dashboards so that output indicators remain visible but are explicitly separated from outcome and risk-reduction indicators. An intervention should not be considered strategically successful solely because its output target has been achieved when the associated outcome or risk-reduction target has not been demonstrated.

## 6. Integrated Interpretation of the Findings

The findings across the three cases produce a consistent analytical pattern. First, transnational criminal threats exhibit systemic characteristics because networks can move across jurisdictions, adapt to enforcement pressure, and relocate digital or financial nodes. Second, conventional performance indicators are useful for demonstrating institutional activity but are insufficient for establishing sustained changes in underlying risk. Third, the effectiveness of risk-based policing depends on the quality of risk assessment, the selection of appropriate intervention points, and the availability of measurable outcomes. Fourth, risk governance is necessary because many intervention capacities lie outside the police institution itself.

The central contribution of the comparative analysis is therefore not a rejection of conventional enforcement indicators but a reclassification of their analytical function. Cases, suspects, seizures, and blocked domains should remain as output indicators. They should, however, be connected to outcome indicators that measure disruption, protection, financial interruption, and institutional responsiveness, and ultimately to risk-reduction indicators that assess changes relative to an explicit baseline.

This interpretation also clarifies why the proposed framework should not be understood as a new policing model that replaces existing approaches. Instead, it provides a

performance and governance architecture for integrating complementary approaches. Intelligence-led policing can support threat identification; network analysis can identify critical nodes; problem-oriented analysis can explain mechanisms; community and stakeholder engagement can contribute vulnerability and contextual information; evidence-based policing can strengthen evaluation; and preventive policing can guide early intervention. Risk governance provides the institutional structure within which these contributions can be coordinated, while risk-based policing translates the resulting assessment into operational priorities.

The resulting logic is therefore:

**Finding → Analytical Implication → Indicator → Intervention → Outcome → Risk Reduction → Feedback.**

This sequence provides a stronger basis for accountability because it distinguishes the production of enforcement activity from evidence that the intervention actually changed the threat. It also provides an explicit mechanism for learning: when the expected outcome is not achieved, the institution does not simply report the failure but uses the result to reconsider the risk assessment, intervention design, resource allocation, or inter-agency coordination.

## 7. Implications for the Risk-Based Performance Framework

The findings-to-policy analysis supports the performance framework proposed in this study. The framework should consequently be interpreted as a decision system rather than merely as a reporting table. At the first level, threat identification and risk assessment establish the priority and baseline. At the second level, intervention and output document the actions undertaken and resources deployed. At the third level, outcome and risk reduction determine whether the intervention generated sustained changes. Finally, feedback determines whether the strategy should be maintained, redesigned, expanded, or discontinued.

The distinction is particularly important when interpreting digital and networked enforcement. If a priority network's critical nodes are disrupted but are rapidly replaced, the output may be classified as successful, even as the outcome remains limited. Under the proposed framework, this situation should not be treated as a strategic success. Instead, rapid replacement serves as evidence of network resilience and should prompt reassessment of intervention points. Similarly, a high value of seized assets accompanied by continued transaction capacity would indicate that seizure output has not yet translated into substantial financial disruption(Zedner 2015).

The framework, therefore, introduces a more demanding standard of institutional performance: an intervention should demonstrate not only that something was done, but also what changed, how long the change persisted, and whether the change was sufficient to reduce the assessed level of risk. This provides the analytical bridge between risk governance and risk-based policing and responds directly to the central measurement problem identified across the three cases.

## 8. Policy Implications for Polri

First, Polri should institutionalize a periodic risk assessment that identifies priority transnational threats, explains the assessment methodology, and establishes a baseline for

subsequent performance measurement. The assessment should be sufficiently transparent to permit policy learning while protecting operationally sensitive information. Second, performance dashboards should be redesigned into three levels: output, outcome, and risk reduction. Output measures retain operational accountability; outcome measures test whether interventions changed network capacity, financial infrastructure, or victim protection; and risk-reduction measures evaluate whether the broader threat environment improved. Third, every major intervention should have an explicit intervention logic. Before action, the institution should specify the threat mechanism, target node, expected outcome, indicator, target, and review date. This creates a direct connection between intelligence analysis and evaluation. Fourth, victim identification should be integrated into risk reduction for trafficking and online scam cases. Screening quality, referral speed, access to protection, and repeat vulnerability should be measured alongside arrests. Fifth, financial disruption should be evaluated by the continuity of the criminal financial infrastructure, not only by the nominal value of seizures. Priority should be given to identifying and disrupting nodes that enable repeated transactions, laundering, and conversion of illicit proceeds. Finally, cross-jurisdictional cooperation should be governed by measurable service standards. Cooperation that is too slow to interrupt a rapidly moving digital or financial network should be treated as a risk-management weakness and subjected to corrective action.

## LIMITATION

The study has four principal limitations. First, it relies on documentary evidence and therefore cannot independently observe all operational activities or changes in unreported criminal networks. Second, several 2026 statistics are treated as reported institutional figures because the originating publications are not fully preserved in the supplied reference list. Third, the original search log did not retain exact counts of records identified, screened, excluded, or allocated to each evidence group and case; these figures therefore cannot be responsibly reconstructed. Fourth, coding was conducted by a single researcher, so formal intercoder agreement was not calculated. The framework should consequently be interpreted as an analytically transferable model rather than a statistically generalizable estimate of transnational-threat prevalence or policing effectiveness.

## CONCLUSION

This study concludes that the principal measurement challenge in transnational threat management is not the absence of enforcement activity but the limited connection between enforcement outputs and demonstrable risk reduction. Transnational narcotics trafficking, human trafficking, and migrant vulnerability within online scam networks, and online gambling with associated financial flows operate through systems that can relocate, adapt, and exploit jurisdictional differences. Consequently, case counts, arrests, seizures, and blocked digital content are necessary indicators of activity but insufficient indicators of strategic success.

The revised conceptual distinction is that risk governance establishes the public framework for identifying, assessing, communicating, and deciding about risk. In contrast, risk-based policing translates those assessments into operational priorities, targeting, intervention, testing, and tracking. Their combination provides a stronger basis for evaluating Polri's performance. The proposed framework links threat identification, risk

assessment, intervention, output, outcome, risk reduction, and feedback, and specifies indicators, units, data sources, baselines, targets, frequencies, responsible institutions, and thresholds.

The practical implication is a shift in the logic of institutional performance: from counting what was done to demonstrating what changed. Polri should therefore complement conventional output reporting with sustained network disruption, financial disruption, asset recovery, victim identification and protection, measurable changes in risk levels, and response-time indicators to support cross-jurisdictional cooperation. The central performance question should become: how much risk has actually been reduced, and what evidence demonstrates that reduction?

## REFERENCE

Adillah, Muhammad Arief, and Cahyoko Edi Tando. 2026. "Cross-Sectoral Governance in Combating Online Gambling: A Stakeholder Theory Perspective." *Moestopo International Review on Social, Humanities, and Sciences* 6(1 SE-Articles): 230–47. https://mirshus.moestopo.ac.id/index.php/mirshus/article/view/156.

Agastia, I Gusti Bagus Dharma. 2020. "Understanding Indonesia's Role in the 'ASEAN Outlook on the Indo-Pacific': A Role Theory Approach." *Asia & the Pacific Policy Studies* 7.

Andreas, P. (2003). Redrawing the line: Borders and security in the twenty-first century. International Security, 28(2), 78–111. https://doi.org/10.1162/016228803322761973

Ansell, Chris, and Alison Gash. 2017. "Collaborative Platforms as a Governance Strategy." *Journal of Public Administration Research and Theory* 28: 16–32.

Boulton, Laura, Rebecca Phythian, Stuart Kirby, and Ian Dawson. 2020. "Taking an Evidence-Based Approach to Evidence-Based Policing Research." *Policing: A Journal of Policy and Practice* 15: 1290–1305.

Cooper, A. F., & Cannon, B. J. (2024). Contested informality in regional institutional design: A comparative analysis of ASEAN and the Quad. Global Policy, 15(1), 40–52. https://doi.org/10.1111/1758-5899.13335

Gallagher, A. T. (2010). The international law of human trafficking. Cambridge University Press.

Glückler, Johannes, Gary Herrigel, and Michael Handke. 2020. "On the Reflexive Relations Between Knowledge, Governance, and Space." In , 1–21.

Hing, Nerilee et al. 2022. "Gambling Prevalence and Gambling Problems amongst Land-Based-Only, Online-Only and Mixed-Mode Gamblers in Australia: A National Study." *Computers in Human Behavior* 132: 107269.

InfoPublik. (2026a, July 1). Polri ungkap 718 kasus judi online sepanjang 2026. Direktorat Jenderal Komunikasi Publik dan Media, Kementerian Komunikasi dan Digital.

InfoPublik. (2026b, July 1). Sepanjang 2026, Polri ungkap 24.837 kasus narkoba. Direktorat Jenderal Komunikasi Publik dan Media, Kementerian Komunikasi dan Digital.

Jaiborisudhi, Watunyu, Poowin Bunyavejchewin, and Kridsana Chotisut. 2026. "The Anti-Fraud Lever: China's Strategic Use of the Scam Crackdown to Invigorate the LMLECC Process Against Thailand's Reluctance." *Asian Politics & Policy* 18.

Jubaer, Shah. 2026. "Evidence-Based Policy-Making."

Kennedy, Leslie, Joel Caplan, and Eric Piza. 2019. Risk-Based Policing *Risk-Based Policing: Evidence-Based Crime Prevention with Big Data and Spatial Analytics*.

Keohane, R. O., & Nye, J. S. (2012). Power and interdependence (4th ed.). Pearson.

Kementerian Koordinator Bidang Politik dan Keamanan Republik Indonesia. (2026, June 26). Kemenko Polkam perkuat kerja sama penanganan online scam dengan Kamboja (Siaran Pers No. 245/SP/HM.01.02/POLKAM/6/2026).

Law of the Republic of Indonesia No. 2 of 2002 concerning the Indonesian National Police.

Law of the Republic of Indonesia No. 3 of 2002 concerning National Defense.

Law of the Republic of Indonesia No. 21 of 2007 concerning the Eradication of the Criminal Act of Human Trafficking.

Law of the Republic of Indonesia No. 35 of 2009 concerning Narcotics.

Law of the Republic of Indonesia No. 8 of 2010 concerning the Prevention and Eradication of the Criminal Act of Money Laundering.

Law of the Republic of Indonesia No. 18 of 2017 concerning the Protection of Indonesian Migrant Workers.

Law of the Republic of Indonesia No. 27 of 2022 concerning Personal Data Protection.

Neil, Tony, and Saw Htoo. 2026. "Beyond the Rebel 'Territorial Trap': Governing Armed Sovereign Formations in Eastern Myanmar." *Development and Change* 57: 441–66.

Paribatra, M L Pinitbhand. 2025. "The 'Indo-Pacific' Order: A Southeast Asian Perspective." *Asian Politics & Policy* 17.

Presidential Regulation of the Republic of Indonesia No. 47 of 2023 concerning the National Cybersecurity Strategy and Cyber Crisis Management.

Putra, Evan Tjoa. 2024. "Indonesia Law Review The Prohibition Of Online Gambling In Indonesia : A Law And Economic Analysis The Prohibition Of Online Gambling In Indonesia : A." 14(2).

Ratcliffe, J. H. (2016). Intelligence-led policing (2nd ed.). Routledge.

RRI. (2026, July 5). KBRI Phnom Penh: 12 ribu WNI terjebak penipuan daring di Kamboja. Lembaga Penyiaran Publik Radio Republik Indonesia.

Smith, Graeme. 2025. "Inducing Compliance : Shaping Audiences ' Perceptions in China ' s Cyber Crime Enforcement." : 1–12.

Tyler, Tom. 2017. "Procedural Justice and Policing: A Rush to Judgment?" *Annual Review of Law and Social Science* 13: 29–53.

United Nations Office on Drugs and Crime. (2024). Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat. United Nations.

Zedner, Lucia. 2015. "Penal Subversions: When Is a Punishment Not Punishment, Who Decides and on What Grounds?" *Theoretical Criminology* 20: 3–20.

Zulhawati, Meiliyah Ariani, and Sarida Minarni. 2023. "Fraud Minimization In View Of Good Corporate Governance, Operational Effectiveness And Risk Management." *Moestopo International Review on Social, Humanities, and Sciences* 3(1 SE-Articles): 1–12. https://mirshus.moestopo.ac.id/index.php/mirshus/article/view/45.