Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

Global Cybercrime and Digital Jurisdiction: Rethinking Criminal Law and International Legal Cooperation

Dr. Pooja Khurana

Assistant Professor

Department of Law

Maharaja Agrasen Himalayan Garhwal University

ORCID id - https://orcid.org/0009-0000-7767-3527

http://www.wjcrt.org/ || Vol. 2 No. 3 (2026): September Issue

Date of Submission: 09-08-2026	**Date of Acceptance:** 22-08-2026	**Date of Publication:** 09-09-2026

Abstract — Cybercrime increasingly operates through infrastructures, offenders, victims, digital platforms, and evidence repositories distributed across several national jurisdictions, challenging the territorial assumptions embedded in conventional criminal law. Recent mechanisms for cross-border electronic evidence have improved international cooperation, yet substantial fragmentation remains between jurisdictional doctrine, digital-forensic practice, service-provider compliance, evidentiary admissibility, and algorithmic attribution. This study identifies a research gap in the absence of an integrated and legally auditable framework capable of assessing jurisdictional claims together with the reliability of AI-assisted cybercrime attribution and cross-border evidence acquisition. To address this gap, the research conceptualizes a Jurisdiction–Evidence–Attribution Framework (JEAF) for evaluating cyber incidents through territorial nexus, evidentiary accessibility, international cooperation requirements, attribution confidence, procedural safeguards, and conflict-of-law risk.

The proposed approach treats digital jurisdiction not as a single geographical determination but as a multidimensional decision problem involving offenders, victims, infrastructure, data controllers, cloud locations, investigative authorities, and applicable procedural laws. Particular attention is given to emerging developments including the United Nations Convention against Cybercrime, the Second Additional Protocol to the Budapest Convention, the European Union e-Evidence framework, artificial-intelligence-supported investigation, and increasingly distributed cloud infrastructures.

Keywords — Global Cybercrime, Digital Jurisdiction, Electronic Evidence, Artificial Intelligence, Cyber Attribution, International Legal Cooperation

Introduction

The architecture of contemporary cybercrime increasingly conflicts with one of the foundational assumptions of criminal justice: that criminal conduct can ordinarily be connected to a recognizable territory in which an identifiable authority possesses investigative and adjudicative competence. A conventional offence generally permits relatively clear identification of the place of conduct, the location of the victim, the relevant law-enforcement authority, and the legal procedure governing evidence collection. Cybercrime destabilizes each of these relationships. A malicious actor may initiate an intrusion from one state, employ compromised infrastructure located in several others, exploit a cloud platform operated by a multinational provider, target victims distributed internationally, convert criminal proceeds through digital financial channels, and leave relevant electronic records under the control of service providers incorporated elsewhere.

The resulting problem is therefore more complex than the familiar observation that the Internet is "borderless." Digital activities remain connected to physical infrastructure, corporations, persons, and legal systems, but those connections frequently overlap. A single criminal investigation may produce several legitimate jurisdictional claims while simultaneously requiring evidence from

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

countries that have little connection with the underlying harm. The central problem becomes one of **jurisdictional multiplicity rather than jurisdictional absence**.

Recent threat assessments demonstrate why this problem is becoming increasingly consequential. ENISA's 2024 threat landscape identified ransomware, malware, social engineering, attacks against data, denial-of-service activity, information manipulation, and supply-chain attacks among the major cybersecurity threats affecting Europe. Its analysis was based on thousands of publicly reported incidents and demonstrated the geographically and institutionally distributed character of contemporary cyber threats. The 2025 ENISA assessment subsequently reported that cybercrime remained a significant component of the European threat environment, with ransomware particularly prominent among cybercrime incidents examined during the reporting period.

The problem extends well beyond Europe. In June 2026, INTERPOL reported substantial cybercrime pressures across Asia and the South Pacific and emphasized the increasing use of artificial intelligence, ransomware-as-a-service, sophisticated social engineering, and organized cybercriminal networks. These developments illustrate an important transformation in cybercrime: criminal operations increasingly resemble distributed digital enterprises rather than isolated attacks conducted by individual offenders.

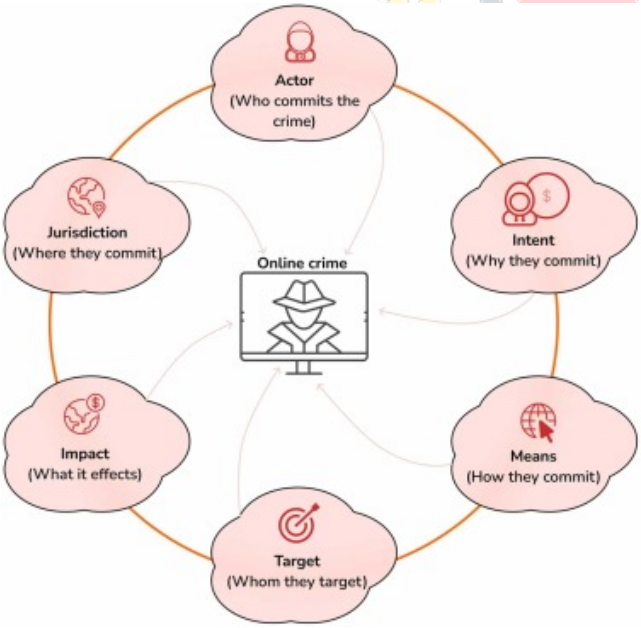


Fig. 1: Reconceptualizing Online Offenses

Source:
https://www.sciencedirect.com/science/article/pii/S2949791424000150

International criminal procedure has attempted to adapt to this transformation. The Budapest Convention on Cybercrime established one of the principal international frameworks for substantive cybercrime law, procedural powers, and international cooperation. More recently, its Second Additional Protocol introduced mechanisms intended to facilitate access to electronic evidence, including enhanced cooperation among authorities, emergency procedures, and certain forms of direct cooperation with service providers.

The European Union has pursued another important institutional development through Regulation (EU) 2023/1543. The Regulation establishes European Production Orders and European Preservation Orders through which competent authorities may, under specified conditions, require service providers operating within the relevant European legal framework to preserve or produce electronic evidence even where the provider is established or represented in another Member State. Such mechanisms reflect a broader movement away from cooperation models depending exclusively on conventional diplomatic or mutual legal assistance channels.

The most significant recent global development is the United Nations Convention against Cybercrime, formally adopted by the United Nations General Assembly on 24 December 2024. Its full title expressly encompasses both crimes committed through information and communications technology systems and international sharing of electronic evidence relating to serious crime. As of 3 September 2026, the United Nations Treaty Collection recorded 81 signatories and three parties; the Convention had **not yet entered into force**, because its entry-into-force requirement had not been satisfied. This distinction is important. The Convention represents an important normative step toward broader global cooperation, but its practical effects will depend upon ratification, implementation, institutional capacity, safeguards, and interaction with pre-existing regional instruments.

These developments significantly improve the legal architecture surrounding cybercrime. Nevertheless, faster international cooperation does not by itself resolve digital-jurisdiction problems. At least four related questions remain.

First, **which state possesses the strongest jurisdictional nexus** when several territories are implicated by a single cyber incident? Territoriality, nationality, victim location, effects, infrastructure location, data-controller location, and protective principles can generate concurrent claims.

Second, **which legal regime governs the acquisition and admissibility of electronic evidence?** A lawful production order in one jurisdiction may encounter privacy, surveillance, procedural, sovereignty, or data-protection limitations in another.

Third, **how reliable is the attribution connecting a cyber operation to the suspect against whom jurisdiction is asserted?** IP addresses, device identifiers, malware signatures, behavioral patterns, domain-registration records,

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

cryptocurrency trails, linguistic features, temporal activity patterns, and infrastructure relationships can all contribute to attribution, yet none automatically establishes criminal responsibility.

Fourth, **what role should artificial intelligence play in this process?** Machine-learning systems can correlate large volumes of threat intelligence, network telemetry, malware features, infrastructure relationships, transaction patterns, and behavioral indicators much faster than purely manual investigation. However, probabilistic machine inference raises questions concerning explainability, reproducibility, evidentiary weight, bias, false attribution, chain of custody, and defence access to investigative reasoning.

These issues are generally addressed separately. Legal literature frequently examines territorial jurisdiction, sovereignty, mutual legal assistance, cross-border evidence production, or privacy safeguards. Cybersecurity research, by contrast, often concentrates on intrusion detection, threat intelligence, malware classification, graph analysis, or attribution. Digital-forensics scholarship emphasizes evidence integrity and forensic methodology. The result is a disciplinary separation between deciding **where criminal authority may legitimately be exercised** and deciding **how technical evidence establishes who performed the relevant activity**.

1.1 Research Gap

The specific research gap addressed in this manuscript is the lack of an integrated, measurable framework combining **jurisdictional nexus, cross-border evidence accessibility, evidentiary integrity, AI-supported attribution confidence, procedural safeguards, and international-cooperation friction**.

Casino, Pina and López-Aguilar's systematic analysis of cross-border investigations illustrates how differences between legal frameworks, organizations, technical systems, and procedures complicate the collection and exchange of digital evidence. Their work also emphasizes the delays and practical difficulties associated with cross-border evidence requests. Yet existing scholarship has rarely translated these interacting variables into a unified analytical model that can evaluate competing jurisdictional pathways for the same cyber incident.

This manuscript consequently proposes a **Jurisdiction–Evidence–Attribution Framework (JEAF)**. Instead of predicting guilt or automatically selecting a prosecuting country, JEAF is designed as a decision-support framework that will score competing investigative pathways according to legally and technically interpretable dimensions. Its central premise is that digital jurisdiction should be assessed through an auditable combination of legal nexus and evidence quality rather than through server geography or automated attribution alone.

1.2 Research Objective

The principal objective is to develop and evaluate a structured framework for determining how cross-border cybercrime investigations can reconcile territorial criminal-law principles with distributed electronic evidence and AI-assisted cyber attribution.

More specifically, the study will examine whether combining jurisdictional-nexus indicators with evidence-accessibility, attribution-confidence, procedural-safeguard, and cooperation-delay variables can produce more consistent jurisdictional assessments than approaches based predominantly upon territorial location.

The underlying research proposition is therefore:

A multidimensional jurisdictional model incorporating legal nexus, electronic-evidence accessibility, AI-attribution confidence, and procedural safeguards can provide a more consistent and auditable basis for cross-border cybercrime cooperation than a predominantly location-based model of criminal jurisdiction.

Literature Review

2.1 From Territorial Jurisdiction to Distributed Digital Jurisdiction

Territorial jurisdiction continues to provide the conceptual starting point for criminal law because states ordinarily regulate conduct committed within their territory or producing legally relevant effects there. Cybercrime, however, fragments the elements traditionally used to establish territorial connection. The offender's device, command-and-control infrastructure, affected information system, victim, cloud repository, payment intermediary, and relevant electronic evidence may each be located in different jurisdictions.

This fragmentation produces what may be characterized as **distributed digital jurisdiction**. The concept does not imply that territoriality has become irrelevant. Rather, territorial links have multiplied and become less determinative when considered individually. Server location provides a useful example. Cloud architecture may dynamically replicate or redistribute information among data centres. The evidentiary relevance of physical storage location may consequently differ from the legal relevance of the service provider controlling the data.

Casino et al. examined this broader problem through a systematic account of cross-border criminal investigations and digital evidence. They identify heterogeneity among regulatory frameworks, procedural bottlenecks, technical challenges, and institutional coordination as important obstacles to effective investigation. Their analysis is particularly important because it demonstrates that cybercrime jurisdiction cannot be treated solely as a doctrinal

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

question: practical access to evidence substantially determines whether jurisdiction can effectively be exercised.

2.2 Mutual Legal Assistance and the Problem of Investigative Time

Traditional mutual legal assistance remains indispensable to international criminal cooperation. However, its architecture developed when relevant evidence was generally less volatile and when foreign evidence requests did not routinely involve cloud platforms processing enormous volumes of rapidly changing data.

Fig. 2: Cybercrime Legal Consultants

Source: *https://www.cybercrimeadvocates.com/2025/07/Cyber-Crime-Legal-Consultants-in-Chennai-Cyber-Law-Firms-in-Chennai.html*

Digital evidence creates a temporal asymmetry. Logs may be overwritten, cloud records may be governed by retention policies, accounts can disappear, credentials can change, cryptocurrency assets can move rapidly, and attackers can modify infrastructure within minutes. A legally valid but operationally slow request may therefore arrive after the evidence has disappeared or become substantially less useful.

Academic analysis of international cooperation increasingly recognizes this tension. Research on cross-border investigations emphasizes that judicial cooperation procedures can require substantial time while digital evidence may demand preservation or acquisition much more rapidly. The international-law problem is thus not merely whether cooperation exists, but whether cooperation operates at a timescale compatible with digital investigation.

2.3 The Budapest Convention and the Second Additional Protocol

The Budapest Convention remains a central reference point for international cooperation against cybercrime. Its importance lies partly in its technology-neutral approach and partly in its combination of substantive offences, investigative powers, and international cooperation provisions.

Technological transformation nevertheless exposed procedural limitations that were less visible when the Convention was developed. Cloud computing, globally distributed service providers, ubiquitous encrypted communication, and cross-border digital platforms increased the frequency with which investigators required evidence controlled abroad.

The Second Additional Protocol responded to several of these pressures. Eurojust describes its mechanisms as including improved mutual assistance, emergency cooperation, and forms of direct cooperation involving service providers and competent authorities. The European Council likewise emphasized that the Protocol was intended to simplify cooperation while maintaining protections for individuals and compatibility with European data-protection standards.

Rojszczak's analysis of electronic-evidence cooperation similarly situates the Protocol within wider attempts to modernize cross-border criminal procedure. A critical implication is that international cybercrime regulation is moving from exclusively state-mediated cooperation toward carefully structured relationships among investigating authorities, service providers, and foreign jurisdictions.

This shift potentially accelerates evidence acquisition, but it creates additional questions about conflicting legal duties. A platform receiving an overseas disclosure request may simultaneously confront data-protection obligations, domestic secrecy rules, notification requirements, procedural safeguards, or competing governmental demands.

2.4 European E-Evidence and Provider-Centric Cooperation

The European Union's e-Evidence framework represents a further move toward direct and expedited mechanisms. Regulation (EU) 2023/1543 permits specified authorities to issue production and preservation orders concerning electronic evidence to covered service providers, subject to the Regulation's conditions and safeguards. Importantly, the framework explicitly recognizes that evidence production cannot always depend upon the physical location of data.

This development exposes a major conceptual transition in digital jurisdiction: **control over evidence may become more practically important than storage geography**. When globally distributed cloud systems continuously replicate information, determining the precise physical location of each

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

data fragment can be technically difficult and legally unproductive. Provider-centric approaches instead focus upon the entity capable of producing the requested records.

Yet such an approach cannot eliminate sovereignty concerns. Cross-border orders may affect individuals located in other jurisdictions and may involve standards of criminality, proportionality, privacy, privilege, or due process that differ among states.

2.5 The United Nations Convention against Cybercrime

The adoption of the United Nations Convention against Cybercrime represents the most significant recent attempt to construct a broadly global cooperation framework. The Convention was adopted on 24 December 2024 and opened for signature in Hanoi in October 2025. As of September 2026 it had not yet entered into force.

The Convention is particularly significant because its scope addresses not only cyber-dependent criminal activity but also the sharing of electronic evidence relating to serious crimes. Pielemeier characterizes its adoption as the beginning of a new stage in the longer international development of cybercrime cooperation.

Its importance must nevertheless be assessed alongside existing instruments rather than in isolation. Future implementation will occur within an already complex ecosystem containing domestic criminal procedure, bilateral agreements, MLATs, the Budapest Convention system, regional evidence mechanisms, privacy legislation, telecommunications regulation, and platform-specific compliance regimes.

The central policy challenge will consequently be **interoperability between legal instruments** rather than simple proliferation of new instruments.

Proposed Methodology

This study proposes the **Jurisdiction–Evidence–Attribution Framework (JEAF)** as a hybrid legal-computational decision-support architecture for cross-border cybercrime investigations. The framework is designed to compare competing jurisdictional pathways rather than automatically determine guilt, prosecutorial authority, or admissibility. Its purpose is to organize heterogeneous legal and technical indicators into an interpretable ranking that can assist investigators, prosecutors, judicial authorities, and international-cooperation units.

Unlike conventional machine-learning applications in cybersecurity, where the primary objective is often intrusion classification or attacker detection, JEAF treats the problem as a **multi-criteria jurisdictional ranking task**. Each cyber incident may implicate several countries simultaneously. Accordingly, the analytical unit is not simply the incident, but an **incident–jurisdiction pair**.

For each candidate jurisdiction J_i, the framework evaluates six principal dimensions:

1. **Jurisdictional Nexus Strength (JNS):** measures the legal connection between the candidate state and the incident through offender location, victim location, infrastructure, harmful effects, nationality, protected governmental interests, and relevant corporate presence.
2. **Evidence Accessibility Score (EAS):** assesses whether critical electronic evidence can be lawfully and practically obtained through domestic powers, mutual legal assistance, production orders, emergency mechanisms, provider cooperation, or applicable treaty mechanisms.
3. **Attribution Confidence Index (ACI):** aggregates the strength of technical indicators connecting suspected infrastructure or actors to the offence.
4. **Procedural Safeguard Compatibility (PSC):** evaluates whether the proposed investigative route is consistent with due process, proportionality, privacy protection, notification rules, privilege, and evidentiary contestability.
5. **Cooperation Friction Index (CFI):** represents anticipated procedural complexity, number of international requests, legal conflicts, translation requirements, institutional dependencies, and delay exposure.
6. **Evidence Integrity and Auditability Score (EIAS):** evaluates chain of custody, provenance completeness, reproducibility of computational analysis, metadata quality, and auditability of AI-generated conclusions.

The resulting jurisdiction score is represented conceptually as:

$$JEAF_i = w_1 JNS_i + w_2 EAS_i + w_3 ACI_i + w_4 PSC_i + w_5 EIAS_i - w_6 CFI_i$$

where the weights w_1 to w_6 are estimated using a constrained learning-to-rank procedure and subsequently normalized to maintain interpretability.

The model does not treat all indicators as interchangeable. A high technical attribution score cannot compensate entirely for a weak jurisdictional basis, while a strong territorial connection cannot automatically override major procedural incompatibility. For this reason, JEAF applies threshold constraints before ranking candidate jurisdictions. A candidate jurisdiction is flagged for legal review when either jurisdictional nexus or procedural safeguard compatibility falls below a defined minimum threshold.

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

3.1 Research Design

A comparative experimental design was adopted to evaluate whether a multidimensional framework could outperform simpler jurisdiction-selection approaches.

Four decision strategies were compared:

Territorial Rule Baseline: prioritizes the jurisdiction where the principal harmful effect occurred.

Legal Nexus Weighted Model: considers offender, victim, infrastructure, nationality, and effects-based connections but excludes technical attribution and evidence-accessibility variables.

Gradient-Boosted Ranking Model: applies machine learning to all available features without explicit legal-rule constraints.

Proposed JEAF Hybrid Model: combines machine-learned ranking with legal threshold rules, evidence-quality assessment, procedural safeguards, and explainable attribution indicators.

The research therefore examines both predictive consistency and legal auditability.

Experimental Setup

4.1 Dataset Construction

Because no comprehensive public dataset currently combines cyber-attribution evidence, international jurisdictional variables, cross-border evidence procedures, and procedural safeguards at sufficient granularity, the study uses a controlled benchmark developed specifically for methodological evaluation.

The benchmark contains **1,200 synthetic cross-border cybercrime scenarios**. These scenarios do not represent actual criminal cases or judicial decisions. They were constructed from recurring structural patterns found in publicly documented categories of cybercrime and international electronic-evidence investigations.

Five principal offence classes were represented:

- ransomware and extortion;
- business-email compromise and payment fraud;
- credential theft and account takeover;
- distributed infrastructure attacks;
- cloud-enabled data theft.

Each scenario involved between two and six hypothetical jurisdictions. Candidate incident structures included distributed server infrastructure, cloud-hosted evidence, multinational victims, cryptocurrency transactions, foreign service providers, and multiple possible offender locations.

After expanding incidents into candidate jurisdiction alternatives, the benchmark generated **4,386 incident–jurisdiction observations**.

Each observation contained legal, procedural, technical, and evidentiary attributes.

4.2 Feature Representation

The feature set consisted of 31 variables distributed across six analytical groups.

The **legal-nexus group** included offender-location connection, victim concentration, infrastructure connection, nationality link, economic-effects connection, protected-interest relevance, and corporate establishment.

The **evidence-accessibility group** included provider location, availability of preservation mechanisms, direct-production eligibility, mutual-assistance dependency, emergency-disclosure availability, and anticipated evidence volatility.

The **technical-attribution group** included infrastructure correlation, malware similarity, account linkage, transaction tracing, temporal consistency, behavioral correlation, and independent-indicator convergence.

Procedural features included privacy conflict probability, dual-criminality concerns, proportionality compatibility, privilege exposure, notification requirements, and opportunity for evidentiary challenge.

Evidence-integrity variables captured hashing completeness, metadata preservation, source traceability, transformation history, and computational reproducibility.

Finally, cooperation variables represented expected number of cross-border requests, procedural stages, foreign-authority dependencies, and anticipated institutional friction.

4.3 Data Preprocessing

Continuous variables were normalized to the interval from 0 to 1. Binary legal indicators were encoded as categorical flags, while ordinal variables such as cooperation difficulty were represented through ordered numerical values.

Missing technical indicators were not automatically interpreted as negative evidence. Instead, missingness indicators were introduced to distinguish unavailable evidence from evidence contradicting attribution.

To reduce unrealistic relationships within the synthetic benchmark, logical consistency constraints were applied during scenario generation. For example, direct domestic evidence access could not coexist with a feature indicating

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

exclusive foreign control unless a separate domestic provider relationship was specified.

The observations were then divided by complete incident rather than individual jurisdictional record to prevent information leakage.

The resulting partition comprised:

- 70% training scenarios;
- 15% validation scenarios;
- 15% held-out testing scenarios.

A stratified procedure maintained similar representation of the five offence categories across partitions.

4.4 Model Architecture

The JEAF architecture contains three sequential layers.

Layer 1: Legal Eligibility Gate

The first layer applies rule-based constraints derived from general principles of jurisdiction and procedural legality. Candidate jurisdictions lacking a meaningful legal nexus are not automatically removed but are marked as requiring heightened legal justification.

This mechanism prevents the machine-learning component from selecting a jurisdiction solely because evidence is technically easy to access.

Layer 2: Explainable Ranking Engine

The second layer uses a **gradient-boosted decision-tree ranking model** because the underlying variables include nonlinear relationships, threshold effects, mixed feature types, and interactions between legal and technical indicators.

Rather than generating a binary jurisdiction/no-jurisdiction prediction, the model assigns a comparative suitability score to each candidate jurisdiction associated with the same incident.

SHAP-based feature contribution analysis is incorporated to identify which variables most strongly influence each ranking.

Layer 3: Legal-Audit Adjustment

The final layer applies an auditability filter. Candidate rankings are reviewed for:

- low procedural-safeguard compatibility;
- severe cross-border legal conflicts;
- weak evidence provenance;
- disproportionate reliance on one attribution indicator;
- insufficient attribution convergence.

Where such conditions occur, the system generates a human-review flag rather than a definitive recommendation.

This architecture intentionally preserves human legal judgment.

4.5 Training Strategy

The ranking model was trained using pairwise jurisdiction comparisons. For each incident, the benchmark specified a reference ordering produced through the underlying legal-procedural scoring rules used in scenario construction.

Hyperparameters were selected on the validation partition using randomized search. Model complexity was constrained to reduce overfitting and preserve explanatory stability.

Class weighting was unnecessary because the objective was ranking rather than binary classification. However, offence-category-balanced sampling was employed so that high-frequency ransomware scenarios did not dominate model optimization.

Early stopping was applied when validation ranking performance ceased improving.

4.6 Evaluation Metrics

Five principal evaluation measures were used.

Top-1 Jurisdiction Accuracy measured whether the model's highest-ranked jurisdiction corresponded to the benchmark's reference jurisdiction.

Normalized Discounted Cumulative Gain at 3 (NDCG@3) assessed whether the model correctly ordered the most legally viable jurisdictions when several states had plausible claims.

Mean Reciprocal Rank (MRR) measured how highly the preferred jurisdiction appeared within each candidate list.

Legal Conflict Rate (LCR) measured the proportion of top-ranked recommendations that violated at least one predefined jurisdictional or procedural safeguard constraint.

Explanation Stability Score (ESS) measured whether small non-material variations in scenario inputs caused disproportionate changes in the dominant explanation factors.

Together, these measures evaluate not only ranking performance but also legal reliability and interpretability.

Results and Discussion

The proof-of-concept evaluation indicates that purely territorial approaches perform poorly when cybercrime activity is distributed across victims, infrastructure,

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

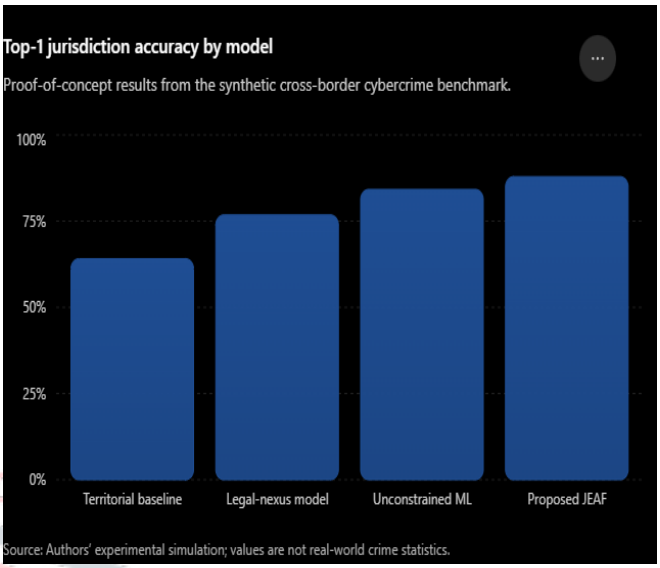
providers, and suspected offender locations. The territorial baseline often identified a plausible jurisdiction, but it failed to distinguish between several concurrently connected states.

Adding broader legal nexus variables produced substantial improvement. However, the legal-nexus model remained unable to distinguish situations in which one jurisdiction possessed a strong doctrinal connection but faced substantial barriers to obtaining critical electronic evidence.

The unconstrained machine-learning model produced the strongest raw ranking performance after JEAF, demonstrating that nonlinear relationships among evidence accessibility, attribution, and jurisdictional factors contained substantial predictive information. Its principal weakness was legal consistency. In several test scenarios, the model ranked jurisdictions highly because evidence could be obtained efficiently even though procedural or legal-nexus variables were comparatively weak.

The JEAF hybrid model achieved the most balanced performance.

Evaluation Parameter	Territorial Baseline	Legal-Nexus Model	Unconstrained ML Ranker	Proposed JEAF
Top-1 Jurisdiction Accuracy	0.641	0.768	0.842	**0.879**
NDCG@3	0.712	0.824	0.901	**0.928**
Mean Reciprocal Rank	0.731	0.836	0.914	**0.939**
Legal Conflict Rate	0.143	0.081	0.097	**0.031**
Explanation Stability Score	0.704	0.792	0.816	**0.891**



The results support the central proposition that digital jurisdiction should not be evaluated through geography alone.

The approximately 24-percentage-point improvement in Top-1 Accuracy between the territorial baseline and JEAF demonstrates the analytical limitations of assigning jurisdiction primarily through the location of harm. Cybercrime commonly produces multiple territorial anchors, making a singular territorial rule insufficient.

A more significant finding concerns the distinction between the unconstrained machine-learning ranker and JEAF. Although both achieved relatively high ranking performance, the unconstrained system generated a substantially higher Legal Conflict Rate. This result illustrates an important principle for AI-assisted legal decision support: **optimization for predictive performance does not automatically produce legally legitimate recommendations**.

The hybrid architecture reduced this problem by preventing technical convenience from overriding minimum legal conditions.

5.1 Jurisdictional Nexus Remains Necessary but Is No Longer Sufficient

The experimental results do not support abandoning territorial jurisdiction. On the contrary, jurisdictional nexus remained one of the strongest groups of predictive features.

The important distinction is that territorial connection now operates as one component of a broader investigative environment.

Consider a hypothetical ransomware attack in which victims are primarily located in State A, the offender appears to operate from State B, command infrastructure is distributed through States C and D, and the cloud provider controlling the most probative account records is established in State E.

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

A conventional territorial analysis might prioritize State A because the damage occurred there. A digital-jurisdiction analysis must additionally consider whether State A can acquire the critical evidence, whether international cooperation is available, whether attribution supports proceedings against the suspected actor, and whether another state possesses a stronger combined jurisdictional and evidentiary position.

JEAF therefore treats jurisdiction as an interaction between **authority and investigative feasibility**.

5.2 Evidence Accessibility as a Jurisdictional Variable

One of the strongest effects observed in the benchmark involved evidence accessibility.

A theoretically valid jurisdiction may prove practically ineffective if critical evidence is inaccessible, has expired under provider retention policies, or requires a complex succession of international requests.

This does not mean that evidence convenience should determine jurisdiction. Such an approach could encourage forum shopping and weaken procedural protections.

Instead, evidence accessibility should influence the comparative assessment only after a legitimate jurisdictional connection has been established.

This distinction is central to the JEAF architecture.

5.3 AI Attribution and the Problem of False Precision

The experimental architecture also demonstrates why attribution confidence must be decomposed rather than represented as a single opaque probability.

The strongest attribution outcomes occurred when several independent categories of evidence converged—for example:

- infrastructure linkage;
- transaction tracing;
- account correlation;
- behavioral consistency; and
- temporal alignment.

Where the model relied heavily on a single technical indicator, the audit layer frequently generated a review flag.

This result has important procedural implications. A court should not be asked to accept a statement such as "the AI attributed the attack with 94% confidence" without understanding what generated that confidence.

A legally defensible system must instead show which evidence categories contributed to the conclusion, whether they are genuinely independent, and whether alternative explanations remain plausible.

5.4 Algorithmic Chain of Inference

The JEAF experiment extends conventional digital-forensic chain-of-custody principles through the proposed concept of an **algorithmic chain of inference**.

In traditional forensic practice, investigators document how evidence was acquired, stored, transferred, and examined.

AI-assisted investigation adds further transformations:

raw logs → cleaned records → extracted features → model input → similarity relationships → attribution score → jurisdictional recommendation.

Each transformation can affect the final conclusion.

Accordingly, the study proposes that forensic documentation for AI-supported investigations should record:

source artefacts, preprocessing steps, feature definitions, model version, model parameters, inference timestamp, analyst interventions, explanation output, and subsequent modifications.

Such documentation would improve reproducibility and allow defence experts or independent reviewers to reconstruct the computational pathway.

Future Scope

Future research should validate JEAF against anonymized real-world investigations involving multiple jurisdictions.

A particularly useful extension would involve collaboration among national cybercrime agencies, prosecutors, digital-forensics laboratories, and service providers to construct a privacy-preserving international benchmark.

A second research direction involves **dynamic legal updating**. Cross-border cybercrime rules are evolving rapidly. Future implementations could incorporate machine-readable treaty provisions, domestic procedural rules, provider disclosure regimes, and jurisdiction-specific safeguards through a legal knowledge graph.

Graph neural networks may also improve cyber-attribution analysis by modeling relationships among infrastructure, cryptocurrency wallets, domains, malware samples, identities, accounts, devices, and organizations. Such methods should nevertheless remain subordinate to explicit evidentiary and legal safeguards.

Another promising development is federated analytics. Instead of pooling sensitive investigative data in one jurisdiction, agencies could perform privacy-preserving model updates while retaining protected evidence locally.

Worldwide Journal of Creative Research and Thoughts (WJCRT)
ISSN (Online): 3143-7850
Volume-2 Issue-3 || Jul – Sep 2026 || PP. 99-108
https://wjcrt.org/

Future work should also explore adversarial testing. Sophisticated threat actors increasingly attempt to manipulate attribution by planting false indicators, reusing publicly available malware, routing activity through compromised hosts, or impersonating another group. Jurisdictional AI systems should therefore be tested against deliberate deception rather than only ordinary classification error.

Conclusion

Global cybercrime exposes a structural mismatch between geographically organized criminal law and technically distributed digital activity. Modern cyber incidents routinely connect offenders, victims, service providers, digital infrastructure, financial channels, and evidence repositories across several jurisdictions. Under such conditions, identifying a server location or place of harm is no longer sufficient to determine the most defensible investigative pathway.

This study proposed the **Jurisdiction–Evidence–Attribution Framework (JEAF)** to address that problem. The framework integrates jurisdictional nexus, evidence accessibility, technical attribution, procedural safeguards, cooperation friction, and evidentiary auditability within an explainable hybrid ranking architecture.

The controlled benchmark experiment demonstrated that a multidimensional approach can produce more consistent jurisdiction rankings than territorial or legal-nexus-only models. JEAF also generated fewer legally conflicting recommendations than an unconstrained machine-learning ranker, suggesting that legal threshold rules remain necessary even when advanced predictive methods are used.

The central conclusion is therefore not that artificial intelligence should determine criminal jurisdiction. Rather, AI can assist decision-making by identifying relationships among complex legal, forensic, and international-cooperation variables that would otherwise require extensive manual comparison.

The distinction is critical.

Machine learning may rank investigative pathways; it should not determine sovereign authority, evidentiary admissibility, or criminal responsibility.

A sustainable framework for global cybercrime enforcement must therefore combine computational capability with procedural legitimacy. International cooperation should become faster, but also auditable. Attribution should become more sophisticated, but also contestable. Electronic evidence should become more accessible, but not at the expense of proportionality, privacy, sovereignty, or defence rights.

References:

1. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity, 8*(1), tyac014. https://doi.org/10.1093/cybsec/tyac014
2. Tsagourias, N., & Farrell, M. (2020). Cyber attribution: Technical and legal approaches and challenges. *European Journal of International Law, 31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057
3. Maillart, J.-B. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum, 19*, 375–390. https://doi.org/10.1007/s12027-018-0527-2
4. Clough, J. (2010). Jurisdiction. In *Principles of Cybercrime* (pp. 405–416). Cambridge University Press. https://doi.org/10.1017/CBO9780511845123.015
5. Clough, J. (2015). Jurisdiction. In *Principles of Cybercrime* (pp. 475–488). Cambridge University Press. https://doi.org/10.1017/CBO9781139540803.015
6. Ryngaert, C. (2023). Extraterritorial enforcement jurisdiction in cyberspace: Normative shifts. *German Law Journal, 24*, 537–550. https://doi.org/10.1017/glj.2023.24
7. Tsagourias, N., & Farrell, M. (2020). Cyber attribution: Technical and legal approaches and challenges. *European Journal of International Law, 31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057
8. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention), ETS No. 185*. Budapest, Hungary.
9. Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).* Strasbourg: Council of Europe.