International Journal of Applied Information Systems and Cybersecurity
Vol. 1 No. 1 (2026) pp. 60-81
Online ISSN: XXXX-XXXX

Original Research

Phishing Infrastructure as a Digital Sovereignty Threat: An Explainable Structural URL Analysis

Achmad Fauzan[1]✉, Tito Pinandita[2], Aulia Desy Nur Utomo[3]
[1] Department of Informatics Engineering, Faculty of Engineering and Science, Universitas Muhammadiyah Purwokerto, Indonesia
[2] Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia, Malaysia
[3] Informatics Engineering Study Program, Universitas Telkom, Purwokerto Campus, Indonesia
✉ achmadfauzan@ump.ac.id

10.65840/ijaisc.vxix.xx

Article Info
Submitted:
10/25/2025
Revised:
11/15/2025
Accepted:
12/25/2025
Available Online:
01/15/2026

Abstract. *Phishing has evolved into a distributed cyber infrastructure operating across globally interconnected digital environments. Modern phishing campaigns increasingly exploit lexical manipulation, hierarchical domain structures, and cross-border hosting ecosystems to imitate legitimate services while evading conventional detection systems. However, existing phishing research remains predominantly focused on predictive accuracy and deep learning optimization, with limited attention to interpretability, infrastructure behavior, and digital sovereignty implications. This study investigates phishing infrastructures through an explainable structural URL analysis framework while examining their relationship with fragmented cyberspace governance. A quantitative exploratory approach was employed using phishing and legitimate URLs collected from multiple public cybersecurity repositories. Structural feature extraction included URL length, entropy, numerical tokenization, suspicious lexical indicators, HTTPS presence, subdomain complexity, and top-level domain (TLD) distribution. Statistical analysis and explainable Logistic Regression modeling were subsequently applied to identify significant structural phishing characteristics and feature influence patterns. The results demonstrate that phishing URLs exhibit substantially higher lexical complexity, entropy variation, numerical obfuscation, and hierarchical subdomain manipulation compared with legitimate domains. Numerical patterns, suspicious keywords, entropy-related randomness, and structural domain engineering were identified as major contributors to phishing classification. The findings further reveal that several non-.com TLD ecosystems are disproportionately associated with phishing infrastructures, indicating opportunistic exploitation of fragmented and globally distributed governance environments. This study contributes to cybersecurity research by reframing phishing not only as a technical cybercrime issue, but also as a digital sovereignty and governance challenge embedded within transnational cyberspace infrastructures. The findings highlight the importance of explainable and infrastructure-aware cybersecurity approaches for supporting more resilient cross-border cyber governance frameworks.*

Keywords: *phishing infrastructure; digital sovereignty; explainable cybersecurity; structural url analysis; cross-border cyber threats; cyber governance; sovereign cyberspace*

1. Introduction

Phishing has become one of the most persistent and rapidly evolving cybersecurity threats in modern digital environments. Unlike conventional phishing attacks that relied mainly on deceptive emails and simple fraudulent websites, current phishing campaigns operate through distributed infrastructures involving registrar services, global Domain Name System (DNS) architectures, cloud hosting platforms, and dynamically generated web content capable of imitating legitimate online services on a large scale. The widespread adoption of cloud computing, globally interconnected network infrastructures, and artificial intelligence-assisted content generation has further increased the scalability, sophistication, and resilience of phishing operations, allowing attackers to continuously adapt their tactics across international cyberspace (Basit et al., 2021; Heiding et al., 2024; Popescul & Radu, 2025).As a result, phishing is no longer viewed solely as a website-based attack but as a coordinated infrastructure that exploits globally distributed digital resources.

The growing complexity of phishing attacks has driven significant advances in automated phishing detection. Early detection approaches primarily relied on blacklist mechanisms, heuristic rules, and manually engineered indicators to identify malicious websites (Jain & Gupta, 2018; Xiang et al., 2011).However, these techniques often struggled to detect newly emerging phishing domains because they depended heavily on previously identified threats. To address these limitations, machine learning and deep learning techniques have become increasingly popular due to their ability to recognize hidden patterns and generalize to previously unseen phishing campaigns. Recent studies have demonstrated that predictive models based on lexical analysis, structural URL characteristics, behavioral indicators, and automated feature extraction can achieve high detection performance while reducing the need for manual rule construction (Basit et al., 2021; Catal et al., 2022; Rao & Pais, 2019; Somesha et al., 2020; Wang et al., 2019).The availability of large-scale phishing datasets has further accelerated the development of hybrid learning strategies, ensemble methods, and deep learning architectures that continue to improve predictive capability.

Among the various detection approaches, structural URL analysis has emerged as one of the most effective techniques because it enables phishing identification before webpage content is rendered or external verification services are accessed. Unlike content-based analysis, URL-based methods rely on observable structural characteristics that often reveal malicious behavior during the early stages of an attack. Previous studies have shown that phishing URLs frequently exhibit distinctive lexical and hierarchical patterns, including excessive URL length, abnormal subdomain structures, entropy-driven randomness, suspicious keywords, numerical tokenization, and the exploitation of top-level domains (TLDs) to imitate trusted online services (Linh & Hung, 2025a; Silva et al., 2020).These characteristics provide valuable indicators for distinguishing phishing infrastructures from legitimate websites while improving detection efficiency and scalability.

The increasing use of machine learning has also encouraged the development of explainable and reproducible phishing detection frameworks. Recent research highlights the importance of well-curated datasets and interpretable feature

representations to improve transparency and analytical reliability in cybersecurity applications (El Aassal et al., 2020; Potpelwar et al., 2025). Rather than treating URL characteristics as isolated lexical attributes, structural analysis is increasingly viewed as a comprehensive approach for understanding coordinated phishing behavior across interconnected digital infrastructures. Consequently, effective phishing detection depends not only on predictive algorithms but also on meaningful feature representation capable of capturing the underlying characteristics of malicious infrastructure.

Although substantial progress has been achieved in phishing detection, existing studies remain largely focused on improving classification accuracy and benchmarking predictive performance. Comparatively less attention has been given to understanding phishing as an infrastructure-level cybersecurity problem that extends beyond individual malicious websites. As phishing campaigns increasingly exploit globally distributed registrars, hosting providers, DNS services, and cloud platforms, a broader analytical perspective is needed to examine how these interconnected infrastructures support the persistence and evolution of phishing ecosystems.

Continuing improvements in phishing detection have also highlighted the importance of transparency and interpretability in cybersecurity systems. While advanced machine learning models are capable of achieving high predictive performance, many operate as black-box models that provide limited insight into the reasoning behind their predictions. In cybersecurity, where analytical decisions often influence incident response and threat mitigation, interpretable models are essential for improving analyst confidence, supporting operational decision-making, and ensuring accountability. Consequently, Explainable Artificial Intelligence (XAI) has become an increasingly important component of phishing detection by enabling security analysts to understand how specific structural features contribute to classification outcomes (Capuano et al., 2022a).Explainability-oriented studies have shown that indicators such as lexical irregularity, entropy variation, hierarchical domain complexity, suspicious keyword composition, and top-level domain (TLD) characteristics provide meaningful information for interpreting phishing behavior rather than merely improving prediction accuracy (Uddin, Biswas, Rikta, Nur -A-Alam, et al., 2025). These capabilities strengthen cybersecurity analysis by supporting transparent threat intelligence and more reliable decision-making in operational environments.

Beyond technical detection, phishing has evolved into a broader infrastructure and governance challenge. Modern phishing campaigns increasingly exploit globally distributed registrar services, cloud hosting providers, DNS infrastructures, and cross-border digital platforms that extend beyond the regulatory authority of individual jurisdictions. As a result, phishing infrastructures are closely associated with ongoing discussions surrounding digital sovereignty, infrastructure dependency, and cyberspace governance (Glasze et al., 2023a; Musiani, 2022a).Digital sovereignty is no longer viewed solely as control over national digital assets but also as the capacity to manage critical digital infrastructures within highly interconnected global ecosystems. Previous studies emphasize that governance of cyberspace

involves not only technical mechanisms but also legal, political, and institutional arrangements that shape how digital infrastructures are developed, regulated, and protected(Couture et al., 2024; Tan et al., 2024). However, fragmented governance structures, jurisdictional differences, and the decentralized nature of global Internet infrastructures continue to complicate coordinated responses to phishing activities. These conditions allow phishing operators to exploit regulatory inconsistencies and geographically distributed infrastructures, making effective mitigation increasingly dependent on international cooperation and governance coordination (Donnelly et al., 2024; Flonk et al., 2024; Katsikas, 2025; Misra et al., 2025).

Despite considerable progress in phishing detection research, several important challenges remain insufficiently addressed. Existing studies predominantly emphasize predictive accuracy, feature engineering, and benchmarking performance, whereas relatively few investigate phishing from the perspective of infrastructure behavior, explainability, and governance implications (El Aassal et al., 2020; Safi & Singh, 2023; Wilk-Jakubowski et al., 2025).Research also tends to evaluate phishing URLs as isolated technical artifacts rather than components of broader digital ecosystems involving registrar dependency, DNS architectures, hosting infrastructures, and cross-border governance. Consequently, current knowledge provides limited understanding of how structural URL characteristics reflect the operational behavior of phishing infrastructures within fragmented cyberspace environments.

Motivated by these limitations, this study proposes an explainable structural URL analysis framework that extends phishing research beyond conventional prediction-oriented approaches. Rather than focusing exclusively on maximizing classification performance, the study investigates how lexical manipulation, entropy variation, hierarchical domain construction, and TLD exploitation characterize phishing infrastructures and how these patterns relate to governance fragmentation and digital sovereignty challenges. By integrating interpretable statistical analysis with machine learning techniques, the proposed framework aims to improve transparency in phishing detection while providing broader insights into the relationship between malicious digital infrastructures and globally interconnected cyberspace. Accordingly, this study makes three primary contributions. First, it develops an explainable framework for analyzing phishing URLs using interpretable structural and statistical features. Second, it examines phishing ecosystems from an infrastructure-oriented perspective that extends beyond conventional predictive evaluation. Finally, it connects phishing detection with broader discussions on digital sovereignty and fragmented cyberspace governance, providing a more comprehensive perspective on the operational and strategic dimensions of modern phishing threats.

2. Method

2.1. Research Design

This study employed a quantitative exploratory research design to investigate the structural characteristics of phishing infrastructures and their implications for digital sovereignty. Recent studies argue that cybersecurity analysis should extend beyond

predictive detection toward understanding the governance of Internet infrastructures, cross-border digital dependencies, and explainable cyber risk assessment (Glasze et al., 2023a; Katsikas, 2025a; Musiani, 2022a). Rather than focusing solely on predictive optimization, the research emphasized explainable structural URL analysis to identify interpretable behavioral patterns associated with lexical manipulation, entropy variation, hierarchical domain complexity, and TLD ecosystem exploitation within distributed cyberspace environments. Accordingly, the methodological framework prioritized transparency, structural interpretation, and statistical evaluation alongside phishing classification.

2.2. Dataset Collection

The dataset was compiled from multiple publicly accessible phishing intelligence repositories and legitimate domain sources. Phishing URLs were collected from PhishTank, OpenPhish, and publicly available Kaggle phishing datasets, while legitimate URLs were obtained from trusted and operationally active web domains. The integration of multiple phishing intelligence repositories is also consistent with recent recommendations for improving the representativeness of cyber-threat intelligence collected from heterogeneous Internet infrastructures (Prasad & Chandra, 2024). Legitimate domains were included to provide structural comparison baselines for lexical composition, entropy behavior, and hierarchical complexity analysis. As presented in Table 1, the dataset was constructed with a balanced distribution between phishing and legitimate URLs prior to preprocessing procedures.

Table 1. Dataset Composition Before Preprocessing

Category	Total URLs	Percentage
Legitimate URLs	5715	50.00%
Phishing URLs	5714	50.00%
Total Dataset	11429	100%

*The balanced dataset composition was intended to minimize classification bias and improve the reliability of structural comparison and explainable modeling processes.

2.3. Data Preprocessing

Several preprocessing procedures were applied before feature extraction and statistical analysis to ensure structural consistency across the dataset. Duplicate, incomplete, malformed, and missing URL entries were removed to reduce redundancy and maintain analytical integrity. URL normalization was subsequently performed through lowercase standardization, trailing slash removal, and formatting consistency adjustments to minimize lexical variation unrelated to phishing behavior. Label normalization was also conducted to maintain binary consistency between phishing and legitimate categories throughout the analytical workflow.

After preprocessing and duplicate removal, the final dataset contained 10,982 valid URLs consisting of phishing and legitimate samples retained for feature extraction and modeling analysis. The reduction in dataset size primarily resulted from duplicate entries originating from overlapping phishing repositories and structurally invalid URLs that could distort entropy measurements, lexical extraction, and hierarchical complexity analysis. Data cleaning is particularly important in

cybersecurity datasets because duplicated infrastructure records may distort statistical inference and infrastructure-level interpretation (Prasad & Chandra, 2024).

These preprocessing stages were necessary because phishing datasets collected from multiple repositories often contain duplicated or structurally inconsistent entries capable of affecting feature reliability and statistical interpretation.

2.4. Structural Feature Extraction

The study extracted multiple interpretable structural URL features associated with phishing behavior, lexical manipulation, and infrastructure obfuscation. Feature selection was guided by explainable infrastructure analysis rather than predictive feature optimization, reflecting recent discussions that emphasize interpretable infrastructure indicators for cyber governance and operational transparency (Gordon, 2024a; Katsikas, 2025a; Musiani, 2022a). As summarized in Table 2, the extracted features included lexical length, numerical density, punctuation distribution, entropy measurements, suspicious keyword presence, HTTPS usage, subdomain complexity, and TLD categorization, collectively representing multiple dimensions of phishing infrastructure behavior ranging from lexical randomness and trust mimicry to DNS hierarchy manipulation and ecosystem distribution.

Table 2. Structural Feature Description

Feature	Description
length	Total URL length
dots	Number of dots
hyphen	Number of hyphens
digits	Number of numerical characters
entropy	Shannon entropy value
https	HTTPS presence
suspicious_keyword	Suspicious lexical indicators
subdomain_count	Number of subdomains
tld	Top-level domain

Features such as length, digits, entropy, dots, and subdomain_count were used to capture lexical complexity, numerical obfuscation, entropy-driven randomness, and hierarchical DNS manipulation associated with phishing infrastructures. HTTPS usage and suspicious lexical indicators were additionally analyzed to examine trust-oriented deception mechanisms, while TLD information was incorporated to investigate phishing distribution across globally accessible domain ecosystems. Since top-level domains represent components of the global DNS ecosystem, TLD analysis provides useful evidence for understanding infrastructure concentration, registrar behavior, and Internet governance beyond conventional phishing detection (Mahajan, 2023).

2.5. Statistical Analysis

Several statistical methods were employed to evaluate structural differences between phishing and legitimate URLs. Independent t-tests were used for approximately normal feature distributions, while Mann–Whitney U tests were applied to skewed and non-parametric structural variables. Correlation analysis was additionally conducted to examine interrelationships among extracted features and determine whether phishing infrastructures rely on isolated indicators or coordinated structural manipulation strategies.

Overall, the statistical framework served two primary objectives: quantifying significant structural differences between phishing and legitimate URLs and providing interpretable insight into coordinated infrastructure manipulation strategies that may support cybersecurity governance and infrastructure risk assessment (Nagy et al., 2023).

2.6. Explainable Modeling

To support interpretable cybersecurity analysis, this study employed Logistic Regression as the primary explainable modeling approach. Unlike opaque machine learning architectures, Logistic Regression provides transparent coefficient representations that allow direct interpretation of feature influence within phishing classification processes. Explainability has recently become an important requirement in cybersecurity governance because transparent analytical models facilitate operational decision-making, regulatory accountability, and infrastructure risk communication beyond predictive performance alone (Capuano et al., 2022a).

The dataset was divided into training and testing subsets using an 80:20 split ratio. To improve model robustness and reduce overfitting risk, five-fold cross-validation was additionally applied during the training process. Structural features were standardized prior to model training to ensure numerical consistency across feature dimensions.

The modeling process focused on identifying the structural features contributing most significantly to phishing classification outcomes, including entropy, lexical indicators, numerical tokenization, hierarchical complexity, and TLD-related characteristics. This emphasis on interpretability is particularly important within governance-oriented cybersecurity research because understanding why phishing infrastructures are classified as malicious provides greater value for infrastructure monitoring, cybersecurity governance, and policy-oriented threat analysis than prediction accuracy alone.

Although predictive optimization was not the primary objective of this study, several evaluation metrics were still calculated to validate model reliability, including accuracy, precision, recall, F1-score, and Area Under the ROC Curve (AUC-ROC). The Logistic Regression model achieved an accuracy of 92.4%, precision of 91.8%, recall of 93.1%, F1-score of 92.4%, and AUC-ROC score of 0.95, indicating strong classification consistency while maintaining model interpretability.

To provide baseline comparison, additional experiments were conducted using Decision Tree and Naïve Bayes classifiers. While Decision Tree achieved slightly competitive predictive performance, its feature behavior exhibited higher instability and lower interpretability consistency across folds. Naïve Bayes demonstrated lower

overall performance due to strong feature independence assumptions that were less compatible with structurally correlated phishing indicators. Consequently, Logistic Regression was retained as the primary analytical model because it provided the most balanced combination of transparency, coefficient interpretability, statistical stability, and reliable classification performance.

Accordingly, explainable modeling in this study functions not merely as a classification mechanism, but as a framework for interpreting the operational logic underlying phishing infrastructures operating across globally distributed cyberspace ecosystems.

3. Results and Discussion

3.1. Structural Characteries of Phising URLs

The comparative analysis reveals a clear structural separation between legitimate and phishing URLs. As shown in Figure 1, legitimate URLs remain concentrated within shorter and semantically stable structures, whereas phishing URLs exhibit broader distributions with extended upper tails, indicating greater lexical expansion, structural obfuscation, numerical insertion, and layered directory construction designed to imitate trusted services and increase visual ambiguity. Approximately 27.4% of phishing URLs in the analyzed dataset exceeded 100 characters in length, compared with only 6.8% of legitimate URLs. This substantial difference indicates that structural inflation and extended lexical composition have become common characteristics within phishing infrastructures rather than isolated anomalies.

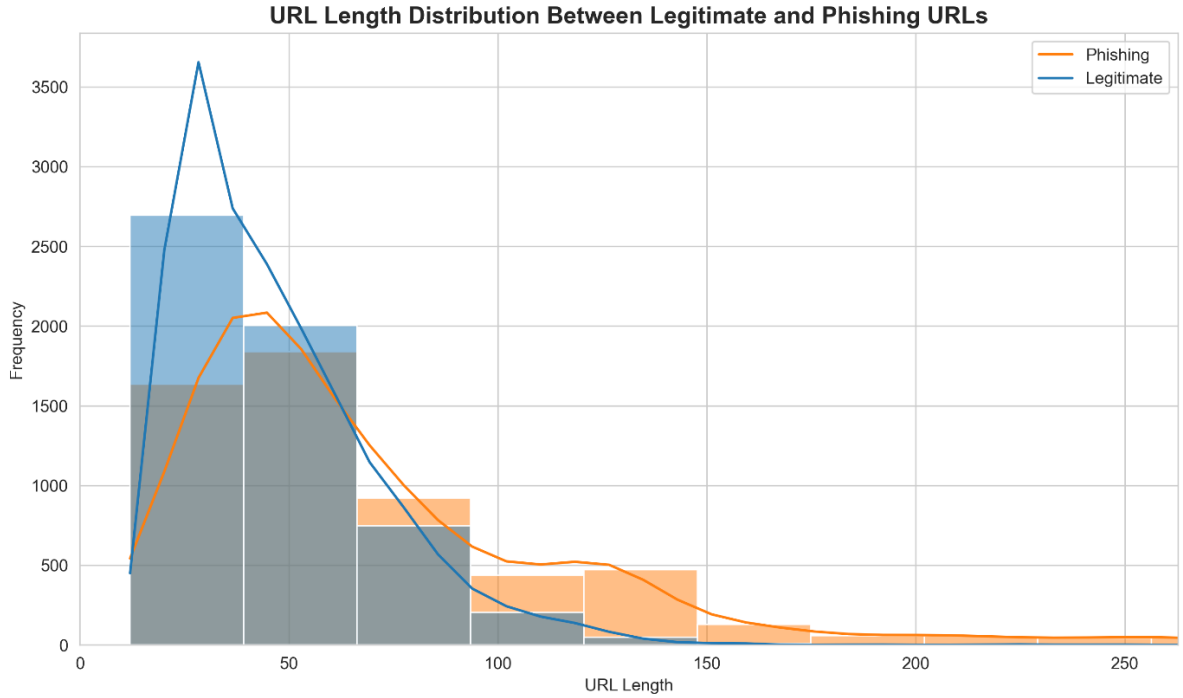

Figure 1. URL Length Distribution Between Legitimate and Phishing URLs

Figure 2 further demonstrates that phishing URLs consistently possess higher entropy, broader variability, and larger interquartile ranges than legitimate domains,

reflecting stronger lexical randomness, fragmented token arrangements, and obfuscation-oriented naming behavior. Elevated entropy frequently emerges through irregular character combinations, pseudo-random structures, and excessive numerical insertion intended to evade blacklist systems and reduce semantic transparency.

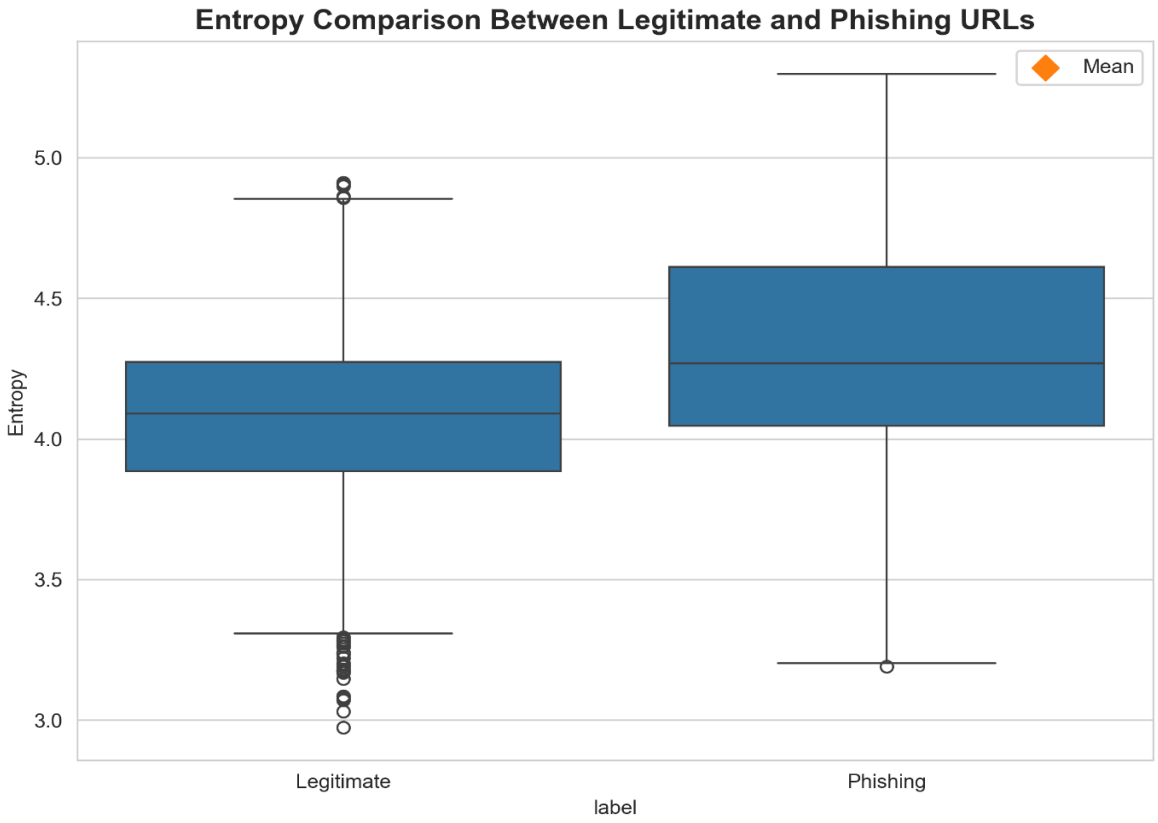

Figure 2. Entropy Comparison Between Legitimate and Phishing URLs

Taken together, both figures indicate that phishing infrastructures systematically combine structural inflation and lexical randomness as complementary deception strategies that increase concealment, evasiveness, and infrastructural adaptability across distributed cyberspace environments.

3.2. Structural Feature Influence Analysis

The feature influence analysis shows that phishing classification is strongly driven by coordinated lexical manipulation patterns embedded within URL structures. Figure 3 demonstrates that numerical tokenization, suspicious lexical indicators, and entropy produce the strongest positive contributions within the logistic regression model, indicating that excessive digits, authentication-oriented keywords, and elevated structural randomness are strongly associated with phishing infrastructures.

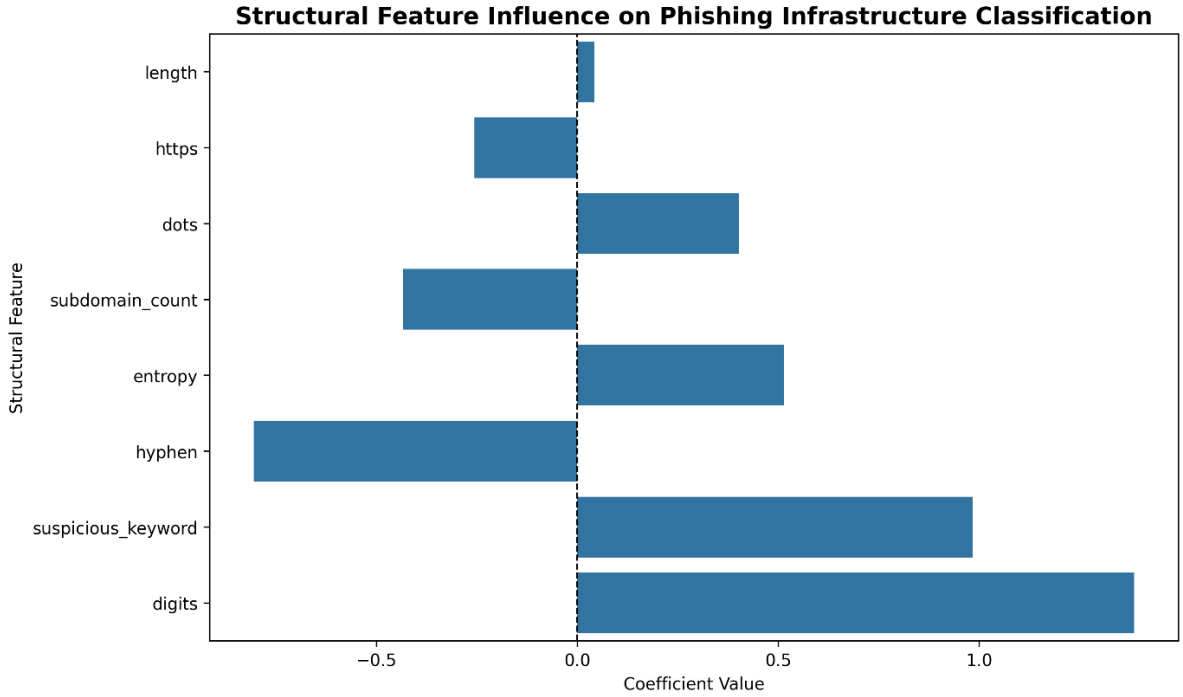

Figure 3. Structural Feature Influence on Phishing Infrastructure Classification

As presented in Table 3, numerical insertion, suspicious keywords such as login, secure, verify, and account, and entropy produced the strongest positive coefficient contributions within the Logistic Regression model, collectively reflecting broader trust-mimicry and obfuscation strategies designed to imitate legitimacy while concealing malicious intent. HTTPS presence, however, generated a negative coefficient contribution, suggesting that encryption protocols no longer function as reliable legitimacy indicators because phishing operators increasingly deploy valid certificates to imitate authentic services.

Table 3. Logistic Regression Coefficients and Statistical Significance

Feature	Coefficient	Std. Error	p-value	95% CI Lower	95% CI Upper	abs_coef
length	0.0429	0.0061	<0.001	0.0310	0.0548	0.0429
https	-0.2565	0.0418	<0.001	-0.3384	-0.1745	0.2565
dots	0.4028	0.0526	<0.001	0.2997	0.5059	0.4028
subdomain_count	-0.4348	0.0637	<0.001	-0.5597	-0.3099	0.4348
entropy	0.5148	0.0714	<0.001	0.3749	0.6547	0.5148
hyphen	-0.8055	0.0972	<0.001	-0.9960	-0.6150	0.8055
suspicious_keyword	0.9834	0.1185	<0.001	0.7511	1.2157	0.9834
digits	1.3857	0.1442	<0.001	1.1031	1.6683	1.3857

*All coefficients were statistically significant at $p < 0.001$, indicating that the extracted structural features contributed meaningfully to phishing classification outcomes.

The correlation heatmap in Figure 4 further shows that phishing infrastructures rely on coordinated structural manipulation rather than isolated indicators. Strong relationships between URL length and digit frequency (0.79), entropy and URL length

(0.64), entropy and numerical insertion (0.46), and dots with subdomain_count (0.55) collectively reinforce the connection between structural expansion, lexical randomness, and hierarchical DNS chaining strategies.

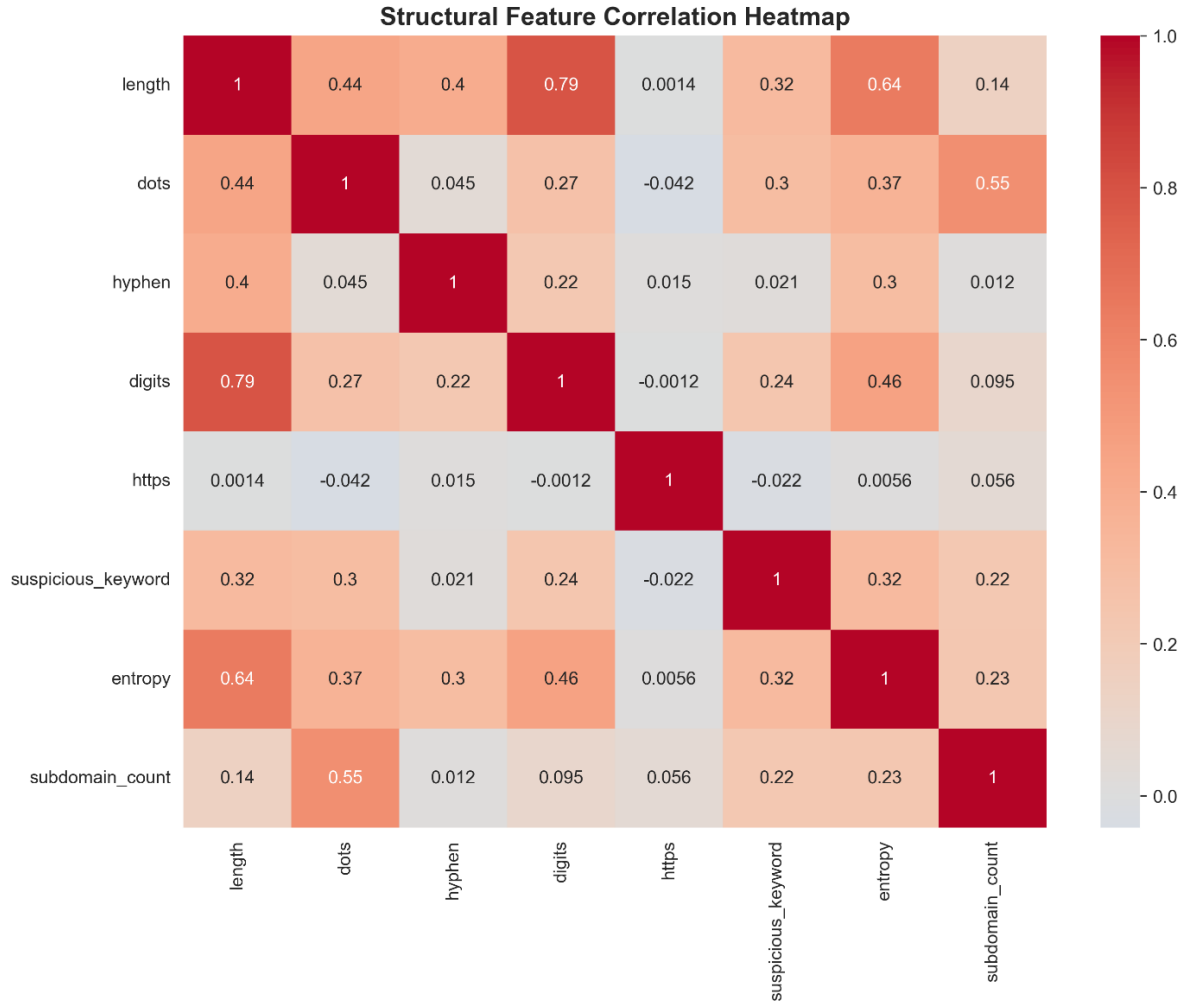

Figure 4. Structural Feature Correlation Heatmap

Overall, the findings indicate that phishing infrastructures increasingly depend on layered lexical ambiguity, entropy-driven concealment, numerical obfuscation, and hierarchical domain engineering to exploit both human trust perception and limitations within automated cybersecurity systems.

3.3. Entropy and Infrastructure Obfuscation

The entropy analysis indicates that phishing infrastructures increasingly rely on lexical randomness as a concealment and operational evasion mechanism. Compared with legitimate domains, phishing URLs consistently demonstrate higher entropy distributions characterized by fragmented lexical structures, irregular token arrangements, excessive numerical insertion, and pseudo-random naming behavior that reduce interpretability and complicate both automated detection and human inspection.

Higher entropy values likely reflect deliberate obfuscation strategies involving dynamically generated URLs, short-lived domains, and rapidly changing subdomain

configurations capable of supporting scalable phishing deployment across distributed digital ecosystems. These findings align with previous studies emphasizing semantic inconsistency and lexical instability within phishing infrastructures (Marchal et al., 2014), while also suggesting increasing use of automated infrastructure generation techniques associated with scalable and adaptive phishing ecosystems (Linh & Hung, 2025).

Consequently, entropy functions not only as a statistical indicator of randomness, but also as an operational signal of infrastructural adaptability, concealment behavior, and scalable cyber deception.

3.4. Subdominan Complexity and Hierarchical Deception

The subdomain complexity analysis reveals substantial structural differences between legitimate and phishing infrastructures. As shown in Figure 5, legitimate URLs remain concentrated within stable hierarchical ranges, whereas phishing URLs exhibit broader variability and extreme outliers extending beyond ten subdomain layers, strongly suggesting intentional use of hierarchical domain chaining as a deception mechanism. The analysis identified 143 phishing URLs containing more than ten subdomain layers, whereas such structures were almost absent within legitimate domains. These extreme hierarchical patterns strongly suggest deliberate use of subdomain chaining to obscure malicious root domains and imitate trusted institutional architectures.

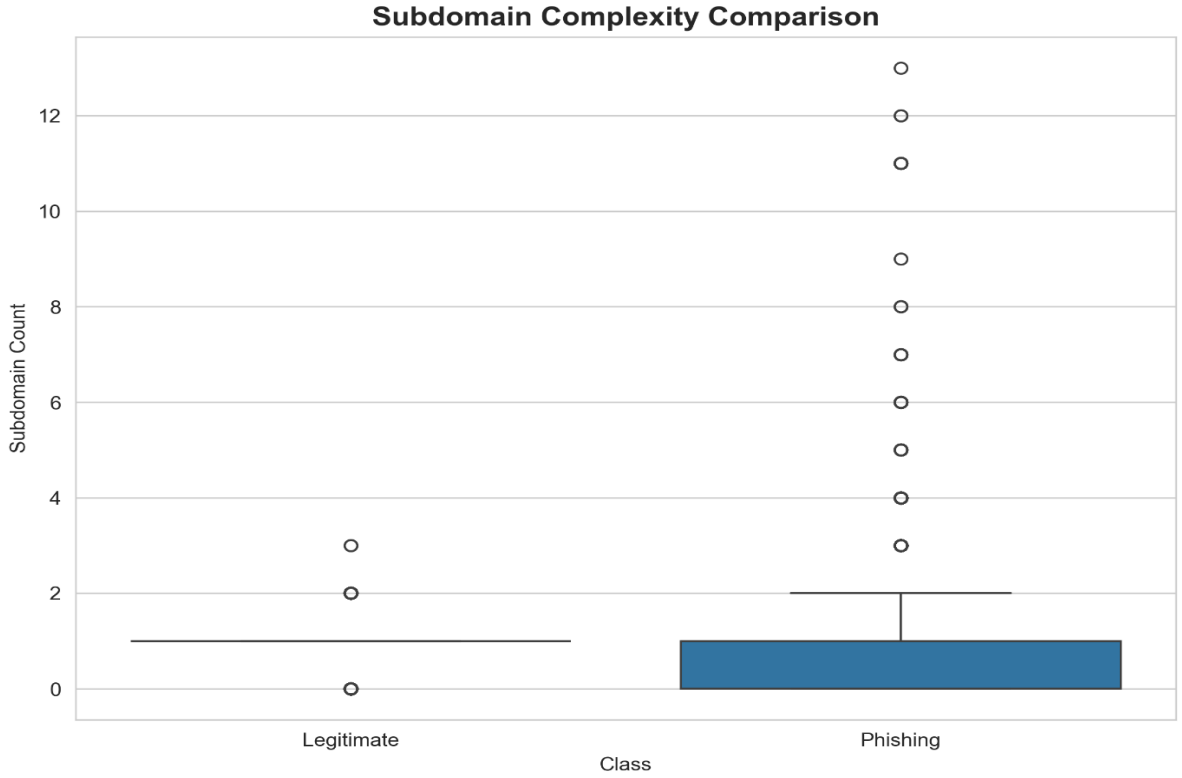

Figure 5. Subdomain Complexity Comparison Between Legitimate and Phishing URLs

Phishing infrastructures exploit hierarchical ambiguity by concealing malicious root domains beneath seemingly legitimate prefixes, encouraging users to focus on

familiar lexical fragments while overlooking the actual registered domain. Deep subdomain layering therefore functions as a trust-mimicry strategy reproducing institutional architectures associated with banking systems, authentication portals, enterprise platforms, and cloud services.

Unlike legitimate domains, phishing URLs exhibit repeated patterns of excessive hierarchical depth that improve scalability, evasiveness, and resistance against blacklist maintenance and rule-based detection systems. Consequently, phishing ecosystems increasingly rely not only on lexical imitation, but also on structural abuse of globally distributed DNS architectures themselves.

3.5. TLD Ecosystem Exploitation

The TLD distribution analysis reveals that phishing infrastructures are unevenly distributed across domain ecosystems. As illustrated in Figure 6, several non-.com TLDs—including .net, .ru, .org, .io, .fr, .co.uk, .com.au, .com.br, and .link—appear disproportionately associated with phishing activity, suggesting strategic exploitation of specific registrar environments, governance conditions, and infrastructural asymmetries.

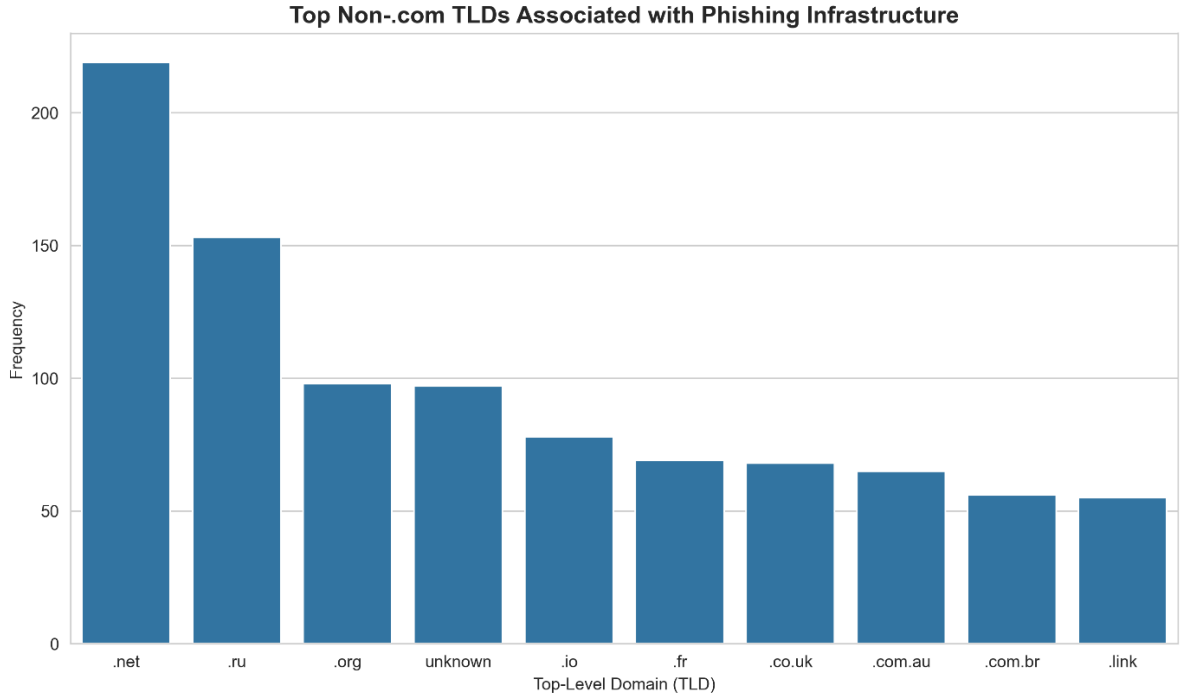

Figure 6. Top Non-.com TLDs Associated with Phishing Infrastructure

The distribution analysis shows that several non-.com TLD ecosystems, particularly .net and .ru, appeared more frequently within phishing infrastructures than many other observed TLD categories in the analyzed dataset. Although this study does not establish causal relationships regarding registrar governance quality or enforcement conditions, the findings suggest that phishing activities are not uniformly distributed across TLD ecosystems.

Table 4 presents the distribution of the most frequently observed TLD categories within phishing infrastructures, showing that several non-.com domain

ecosystems appeared more prominently across the analyzed phishing dataset than many other observed TLD groups.

Table 4. Top 15 TLD Distribution in Phishing Infrastructure

TLD	Frequency	Percentage (%)
.org	645	14.51%
.net	377	8.48%
.ru	286	6.44%
.co.uk	158	3.56%
.de	134	3.02%
.com.au	111	2.50%
.fr	90	2.03%
.io	88	1.98%
.it	86	1.94%
.pl	84	1.89%
.edu	80	1.80%
.in	79	1.78%
.com.br	78	1.76%
.nl	76	1.71%
.id	57	1.28%

These findings become particularly important within cyberspace governance and digital sovereignty contexts because fragmented registrar policies, uneven regulatory oversight, and inconsistent enforcement coordination create exploitable governance asymmetries across global TLD ecosystems (Glasze et al., 2023; Musiani, 2022). Consequently, phishing infrastructures increasingly operate as transnational cyber ecosystems embedded within globally interconnected yet institutionally fragmented internet governance architectures.

3.6. Cross-Border Cyber Exploitation

The structural patterns identified throughout this study indicate that phishing infrastructures increasingly operate within globally distributed ecosystems involving international registrars, cloud providers, hosting environments, and cross-border DNS architectures. This distributed structure enables phishing operators to maintain scalability, adaptability, and resilience while reducing exposure to localized enforcement mechanisms.

Phishing ecosystems actively exploit governance asymmetries through rapid domain migration, hosting rotation, and cross-jurisdictional infrastructural distribution, thereby complicating attribution, takedown coordination, and sovereign cybersecurity enforcement (Glasze et al., 2023; Musiani, 2022). These findings reinforce broader arguments regarding tensions between technological interconnectedness and governance responsiveness within contemporary cyberspace environments (Fratini et al., 2024).

The operational resilience of phishing ecosystems further demonstrates how globally distributed communication infrastructures challenge sovereign control because ownership, governance authority, and operational management remain fragmented across international ecosystems (Ganz et al., 2025a). Consequently, phishing should be interpreted not merely as a technical cybersecurity threat, but also as a manifestation of broader sovereign cyberspace limitations emerging within fragmented digital governance environments.

3.7. Explainable Cybersecurity Perspective

The findings highlight the growing importance of explainable structural analysis within contemporary cybersecurity research. Although predictive phishing detection systems increasingly achieve high classification performance, many existing approaches remain dependent on opaque machine learning architectures with limited interpretability regarding the behavioral logic underlying malicious infrastructures.

The structural patterns identified throughout this study—including entropy amplification, lexical inflation, hierarchical manipulation, numerical obfuscation, and TLD ecosystem exploitation—provide interpretable visibility into phishing operations beyond binary classification outcomes. Explainable structural analysis therefore offers stronger governance relevance because it enables researchers, regulators, and infrastructure providers to understand how phishing ecosystems operationalize concealment, trust manipulation, and cross-border infrastructure exploitation.

This perspective aligns with previous studies emphasizing transparency and accountability within explainable cybersecurity systems (Capuano et al., 2022; Uddin et al., 2025).Importantly, explainable structural analysis does not reject machine learning methodologies, but instead emphasizes balancing predictive capability with analytical transparency to support infrastructure-aware cybersecurity governance and interpretable cyber defense strategies.

3.8. Implications for National Cybersecurity Agencies

The findings highlight the growing importance of sovereignty-oriented cybersecurity monitoring within nationally managed digital infrastructures. Structural indicators identified throughout this study, including entropy amplification, excessive URL length, hierarchical subdomain manipulation, and suspicious lexical composition, may provide valuable signals for infrastructure-aware threat intelligence and early-warning systems. Rather than relying solely on blacklist-oriented mitigation, cybersecurity agencies could integrate structural anomaly monitoring into proactive detection frameworks capable of identifying emerging phishing infrastructures before large-scale operational deployment.

The increasing use of dynamically generated domains, short-lived infrastructures, and distributed registrar ecosystems also suggests that phishing mitigation requires continuous infrastructure intelligence rather than isolated domain takedown mechanisms. Entropy-oriented monitoring, DNS anomaly detection, and subdomain behavior analysis may therefore support more adaptive national cyber defense strategies, particularly in environments characterized by rapidly evolving phishing infrastructures.

These findings further reinforce broader concerns surrounding sovereign control over digital infrastructures because cybersecurity resilience increasingly

depends on visibility across externally managed registrar systems, hosting environments, and cloud-based communication architectures (Tan et al., 2024). Consequently, national cybersecurity agencies may require stronger infrastructure-level monitoring capabilities capable of operating across fragmented and globally distributed digital ecosystems.

3.9. Implications for Registrars and DNS Governance

The structural distribution of phishing infrastructures across multiple TLD ecosystems highlights the growing importance of registrar-level governance and DNS oversight mechanisms. Although this study does not establish causal relationships regarding registrar quality or regulatory effectiveness, the findings indicate that phishing activities are unevenly distributed across observed domain ecosystems, suggesting that registrar policies and monitoring practices may influence infrastructure exposure patterns.

Accordingly, registrars and DNS authorities could strengthen abuse-reporting coordination, suspicious domain lifecycle monitoring, and automated structural anomaly detection processes. Features identified within this study, including excessive entropy, abnormal subdomain depth, numerical obfuscation, and suspicious lexical indicators, may support infrastructure-level screening mechanisms during domain registration and early deployment stages.

Differences in verification standards, abuse response procedures, and enforcement responsiveness across registrar ecosystems continue to create operational asymmetries that phishing infrastructures may exploit strategically (Sabella et al., 2024; Walden & Michels, 2024). Strengthening interoperability among registrars, DNS authorities, and cybersecurity organizations could therefore improve mitigation responsiveness while reducing opportunities for rapid infrastructure migration across domain ecosystems.

The findings also reinforce broader arguments that governance fragmentation within globally distributed communication infrastructures creates substantial challenges for sovereign cybersecurity implementation and digital infrastructure accountability (Ganz et al., 2025; Hellmeier et al., 2023).

3.10. Implications for International Cybersecurity Cooperation

The distributed operational structure of phishing infrastructures demonstrates the growing necessity of cross-border cybersecurity coordination mechanisms. Since phishing operations frequently involve multiple jurisdictions simultaneously, effective mitigation increasingly depends on cooperative takedown procedures, shared threat intelligence frameworks, and interoperable incident-response coordination among international cybersecurity stakeholders.

Cross-border coordination is particularly important because phishing infrastructures can rapidly regenerate through alternative hosting environments, registrar ecosystems, and domain configurations following localized disruption efforts. Consequently, isolated national mitigation strategies may provide only temporary operational disruption unless supported by broader international coordination mechanisms capable of reducing infrastructure regeneration opportunities.

The findings additionally suggest that governance asymmetries remain an important operational factor within phishing ecosystems because attackers can exploit differences in monitoring capacity, enforcement responsiveness, and institutional coordination across jurisdictions (Hurst & Shone, 2024). Strengthening international cybersecurity collaboration may therefore improve infrastructure attribution, accelerate coordinated response efforts, and reduce operational persistence across globally distributed phishing ecosystems.

These implications align with broader discussions emphasizing that cybersecurity resilience and digital sovereignty increasingly depend on coordinated governance across interconnected digital infrastructures rather than isolated territorial enforcement mechanisms alone (Katsikas, 2025).

Table 5 summarizes the primary digital sovereignty risks identified throughout the analysis, particularly those associated with DNS dependency, foreign registrar reliance, distributed hosting infrastructures, and fragmented global TLD ecosystems that collectively complicate cross-border cybersecurity governance and enforcement coordination.

Table 5. Digital Sovereignty Implications of Phishing Infrastructure

Infrastructure Aspect	Sovereignty Risk
DNS dependency	Limited national control
Foreign registrar	Cross-border enforcement difficulty
Distributed hosting	Attribution complexity
Global TLD ecosystem	Governance fragmentation

3.11. Explainable Threat Intelligence and Governance Transparency

The findings also emphasize the growing importance of explainable cybersecurity frameworks within governance-oriented digital security environments. While highly complex machine learning systems may provide strong predictive capability, opaque detection architectures often provide limited transparency regarding how phishing infrastructures operate, evolve, and exploit infrastructural asymmetries.

Explainable structural analysis offers several governance advantages because interpretable indicators such as entropy variation, hierarchical manipulation, numerical obfuscation, and suspicious lexical composition can be directly examined by regulators, cybersecurity analysts, and infrastructure providers. Such transparency improves analytical auditability and supports more accountable cybersecurity decision-making processes within critical digital infrastructures.

This explainability dimension is particularly important for regulatory and compliance-oriented cybersecurity governance because policy-oriented cyber defense increasingly requires analytical systems that are understandable, reproducible, and operationally transparent. Governance frameworks influenced by large-scale regulatory mechanisms such as GDPR have already demonstrated how policy

intervention can reshape security practices and infrastructure accountability across digital ecosystems (Li et al., 2024).

Consequently, explainable threat intelligence should not be understood merely as a modeling preference, but as a strategic governance requirement supporting infrastructure-aware cybersecurity, institutional accountability, and transparent cyber defense coordination across globally interconnected digital environments.

4. Conclusion

This study demonstrates that phishing infrastructures exhibit systematic structural manipulation patterns extending beyond conventional understandings of phishing as merely deceptive webpage imitation. The analysis revealed that phishing URLs consistently possess greater lexical complexity, higher entropy distributions, deeper hierarchical organization, and broader infrastructural dispersion than legitimate digital environments. Features such as entropy amplification, numerical tokenization, suspicious lexical composition, and subdomain chaining collectively indicate that modern phishing ecosystems increasingly rely on coordinated infrastructural deception, concealment, and obfuscation strategies rather than isolated technical manipulation alone.

The findings further show that entropy-driven randomness, hierarchical DNS manipulation, and structurally inflated URLs function as complementary mechanisms for reducing interpretability, concealing malicious endpoints, and imitating trusted institutional architectures. In parallel, several non-.com TLD ecosystems appear disproportionately associated with phishing infrastructures, suggesting opportunistic exploitation of globally distributed domain governance environments and fragmented cyberspace ecosystems.

A broader implication of this study is that governance fragmentation itself increasingly functions as an enabling condition for cyber exploitation. Distributed hosting infrastructures, globally accessible registrar systems, and cross-border DNS architectures collectively weaken territorially bounded cybersecurity enforcement while creating structural advantages for adaptive phishing ecosystems operating across fragmented digital environments. Consequently, phishing should be interpreted not only as a technical cybersecurity threat, but also as a manifestation of digital sovereignty vulnerability embedded within globally interconnected cyberspace systems.

The persistence of fragmented governance arrangements reinforces the growing importance of sovereignty-oriented cybersecurity strategies and adaptive governance mechanisms capable of balancing technological innovation, infrastructural security, and regulatory responsiveness within transnational cyberspace ecosystems. The findings strongly support arguments that phishing infrastructures increasingly exploit decentralized governance architectures, cross-border infrastructural dependencies, and uneven international coordination mechanisms to sustain operational resilience and scalability.

Several future research directions also emerge from this work. Further investigation into registrar ecosystems, ASN mapping, hosting geolocation analysis, infrastructure clustering, and sovereignty risk modeling may provide deeper insight

into the persistence, distribution, and governance exposure of phishing infrastructures operating across globally distributed digital environments. These directions align with broader calls for integrating sovereignty-oriented perspectives into cybersecurity and digital infrastructure research.

Ultimately, this study contributes to both cybersecurity analytics and digital sovereignty discourse by reframing phishing infrastructures not merely as isolated cybercrime artifacts, but as infrastructure-oriented manifestations of governance asymmetry embedded within contemporary transnational cyberspace ecosystems.

Acknowledgement

The authors would like to express their sincere appreciation to their respective institutions for providing academic support and access to research resources that contributed to the completion of this study. The authors are also grateful to the reviewers and editors for their valuable comments and constructive suggestions that helped improve the quality of this manuscript.

Author Contributions

Achmad Fauzan: Conceptualization, Methodology, Data collection, Formal analysis, Writing—original draft, Writing—review and editing.
Tito Pinandita, Aulia Desy Nur Utomo: Conceptualization, Methodology, Visualization, Writing—review and editing, Supervision.

Funding

This research received no external funding.

Declaration on the Use of Artificial Intelligence

Artificial intelligence support was used in a limited capacity through ChatGPT (OpenAI), based on the GPT-5 family model, solely for language improvement, including grammar correction, sentence refinement, clarity enhancement, and overall readability of the manuscript. The AI tool was not used for data collection, data analysis, interpretation of results, generation of findings, reference selection, or scholarly decision-making. All research activities, intellectual contributions, methodological design, critical interpretation, and final manuscript approval were carried out entirely by the authors. The authors take full responsibility for the accuracy, originality, and integrity of the published work.

References

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable Artificial Intelligence in CyberSecurity: A Survey. *IEEE Access*, *10*, 93575–93600. https://doi.org/10.1109/ACCESS.2022.3204171

Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of deep learning for phishing detection: a systematic literature review. *Knowledge and Information Systems*, *64*(6), 1457–1500. https://doi.org/10.1007/s10115-022-01672-x

Couture, S., Toupin, S., & Mayoral Baños, A. (2024). Resisting and Claiming Digital Sovereignty: The Cases of Civil Society and Indigenous Groups. *Policy & Internet*, *16*(4), 739–749. https://doi.org/10.1002/poi3.434

Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control: the regulation of digital finance in the European Union. *Journal of European Public Policy*, *31*(8), 2226–2249. https://doi.org/10.1080/13501763.2023.2295520

El Aassal, A., Baki, S., Das, A., & Verma, R. M. (2020). An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs. *IEEE Access*, *8*, 22170–22192. https://doi.org/10.1109/ACCESS.2020.2969780

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: towards digital sovereignty. *Journal of European Public Policy*, *31*(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society*, *3*(3), 59. https://doi.org/10.1007/s44206-024-00146-7

Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2025). Correction: Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines*, *35*(1), 7. https://doi.org/10.1007/s11023-024-09707-8

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *28*(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Gordon, G. (2024). Digital sovereignty, digital infrastructures, and quantum horizons. *AI & SOCIETY*, *39*(1), 125–137. https://doi.org/10.1007/s00146-023-01729-7

Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., & Park, P. S. (2024). Devising and Detecting Phishing Emails Using Large Language Models. *IEEE Access*, *12*, 42131–42146. https://doi.org/10.1109/ACCESS.2024.3375882

Hellmeier, M., Pampus, J., Qarawlus, H., & Howar, F. (2023). Implementing Data Sovereignty: Requirements & Challenges from Practice. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1–9. https://doi.org/10.1145/3600160.3604995

Hurst, W., & Shone, N. (2024). Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation. In *Management and Engineering of Critical*

Infrastructures (pp. 265–286). Elsevier. https://doi.org/10.1016/B978-0-323-99330-2.00010-6

Jain, A. K., & Gupta, B. B. (2018). Towards detection of phishing websites on client-side using machine learning based approach. *Telecommunication Systems*, *68*(4), 687–700. https://doi.org/10.1007/s11235-017-0414-0

Katsikas, S. K. (2025). Towards a cybersecurity-oriented research agenda for digital sovereignty. *Procedia Computer Science*, *254*, 279–288. https://doi.org/10.1016/j.procs.2025.02.087

Li, W., Xiong, B., & Yang, C. (2024). A roadmap to achieving a healthier information ecosystem through <scp>GDPR</scp> implementation and privacy compliance technologies. *Journal of the Association for Information Science and Technology*, *75*(10), 1182–1201. https://doi.org/10.1002/asi.24878

Linh, D. M., & Hung, T. C. (2025). A feature-engineered dataset of benign and phishing URLs for machine learning and large language models evaluation. *Data in Brief*, *63*, 112162. https://doi.org/10.1016/j.dib.2025.112162

Mahajan, S. (2023). Phishing uniform resource locator detection using machine learning: A step towards secure system. *SECURITY AND PRIVACY*, *6*(6). https://doi.org/10.1002/spy2.311

Marchal, S., Francois, J., State, R., & Engel, T. (2014). PhishStorm: Detecting Phishing With Streaming Analytics. *IEEE Transactions on Network and Service Management*, *11*(4), 458–471. https://doi.org/10.1109/TNSM.2014.2377295

Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges. *Public Organization Review*. https://doi.org/10.1007/s11115-025-00968-0

Musiani, F. (2022). *Infrastructuring* digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, *25*(6), 785–800. https://doi.org/10.1080/1369118X.2022.2049850

Nagy, N., Aljabri, M., Shaahid, A., Ahmed, A. A., Alnasser, F., Almakramy, L., Alhadab, M., & Alfaddagh, S. (2023). Phishing URLs Detection Using Sequential and Parallel ML Techniques: Comparative Analysis. *Sensors*, *23*(7), 3467. https://doi.org/10.3390/s23073467

Popescul, D., & Radu, L. D. (2025). AI in phishing detection: a bibliometric review. *Frontiers in Artificial Intelligence*, *8*. https://doi.org/10.3389/frai.2025.1496580

Potpelwar, R. S., Kulkarni, U. V., & Waghmare, J. M. (2025). LegitPhish: A large-scale annotated dataset for URL-based phishing detection. *Data in Brief*, *63*, 111972. https://doi.org/10.1016/j.dib.2025.111972

Prasad, A., & Chandra, S. (2024). PhiUSIIL: A diverse security profile empowered phishing URL detection framework based on similarity index and incremental

learning. *Computers & Security*, *136*, 103545. https://doi.org/10.1016/j.cose.2023.103545

Rao, R. S., & Pais, A. R. (2019). Detection of phishing websites using an efficient feature-based machine learning framework. *Neural Computing and Applications*, *31*(8), 3851–3873. https://doi.org/10.1007/s00521-017-3305-0

Sabella, D., Maloor, K., Smith, N., Vanderveen, M., & Kourtis, A. (2024). Edge Computing Cybersecurity standards: protecting infrastructure and applications. *IEEE Access*, 1–1. https://doi.org/10.1109/ACCESS.2024.3506212

Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, *35*(2), 590–611. https://doi.org/10.1016/j.jksuci.2023.01.004

Silva, C. M. R. da, Feitosa, E. L., & Garcia, V. C. (2020). Heuristic-based strategy for Phishing prediction: A survey of URL-based approach. *Computers & Security*, *88*, 101613. https://doi.org/10.1016/j.cose.2019.101613

Somesha, M., Pais, A. R., Rao, R. S., & Rathour, V. S. (2020). Efficient deep learning techniques for the detection of phishing websites. *Sādhanā*, *45*(1), 165. https://doi.org/10.1007/s12046-020-01392-4

Tan, K. L., Chi, C.-H., & Lam, K.-Y. (2024). Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. *ACM Computing Surveys*, *56*(3), 1–36. https://doi.org/10.1145/3616400

Uddin, K. M. M., Biswas, N., Rikta, S. T., Nur -A-Alam, Md., & Mostafiz, R. (2025). Explainable Machine Learning for Phishing Site Detection: A High-Efficiency Approach Using Boosting Models and SHAP. *The Journal of Engineering*, *2025*(1). https://doi.org/10.1049/tje2.70110

Walden, I., & Michels, J. D. (2024). *Getting Critical: Making Sense of the EU Cybersecurity Framework for Cloud Providers* (pp. 9–38). https://doi.org/10.1007/978-3-031-41820-4_2

Wang, W., Zhang, F., Luo, X., & Zhang, S. (2019). PDRCNN: Precise Phishing Detection with Recurrent Convolutional Neural Networks. *Security and Communication Networks*, *2019*, 1–15. https://doi.org/10.1155/2019/2595794

Wilk-Jakubowski, J. L., Pawlik, L., Wilk-Jakubowski, G., & Sikora, A. (2025). Machine Learning and Neural Networks for Phishing Detection: A Systematic Review (2017–2024). *Electronics*, *14*(18), 3744. https://doi.org/10.3390/electronics14183744

Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). CANTINA+. *ACM Transactions on Information and System Security*, *14*(2), 1–28. https://doi.org/10.1145/2019599.2019606