Page: 331-387 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.278

PROTECTING LIBERIA'S CRITICAL INFRASTRUCTURE IN THE DIGITAL AGE: NATIONAL SECURITY LESSONS FROM THE ROBERTS INTERNATIONAL AIRPORT CCTV FOOTAGE INCIDENT

Dr. Ambrues Monboe Nebo (Doctor of Sociology)[1], Professor Edward Lama Wonkeryor, Ph.D.[2] & Professor Israel Obiasogu, Ph.D.[3]

I. ABSTRACT

This study examines the protection of critical infrastructure in Liberia's digital security environment, using the US$19.2 million cocaine seizure at Roberts International Airport (RIA) and the subsequent CCTV footage controversy as a focal case. The study examines the national security implications of vulnerabilities in surveillance systems, digital information governance, and institutional safeguards within Liberia's critical infrastructure architecture. Guided by Securitization Theory and critical infrastructure protection frameworks, the study analyzes how surveillance governance, legal arrangements, institutional coordination, and information control influence national security outcomes in the context of transnational organized crime. Methodologically, the study adopts a qualitative case study design based on document analysis of official statements, legal and policy documents, media reports, and scholarly literature to examine the security, governance, and institutional dimensions of the incident. Findings reveal that RIA represents a high-value critical infrastructure asset exposed not only to external threats from transnational criminal networks but also to internal vulnerabilities involving surveillance governance, information management, and institutional coordination. The analysis demonstrates that the circulation of CCTV footage generated concerns regarding digital evidence integrity, investigative confidentiality, cybersecurity governance, and the protection of sensitive operational

[1] Adjunct Faculty, Department of Criminal Justice and Forensic Science Program, African Methodist Episcopal University, Monrovia, Liberia, West Africa. Email: neboambrues@gmail.com
[2] Professor -Graduate School, Stella Maris Polytechnic University, St. Joseph Campus, Capitol Hill, Monrovia, Liberia, West Africa. Email: elamawonkeryor@gmail.com
[3] Professor of Socilogy, African Methodist Episcopal University, Monrovia, Liberia, West Africa Graduate Program in Education, University of Liberia, Monrovia, Liberia. Email: obiasoguisrael@gmail.com

information. The study further finds that the controversy reflected securitization dynamics in which perceived surveillance vulnerabilities were constructed as broader national security concerns, resulting in increased scrutiny of institutional resilience and governance capacity. The study concludes that Liberia's emerging cybersecurity and digital evidence framework should be strengthened through a comprehensive critical infrastructure protection strategy, sector-specific surveillance governance standards, improved inter-agency coordination, and enhanced cybersecurity controls for critical information systems. These measures are essential for strengthening national security resilience, protecting strategic infrastructure, and sustaining public trust in the digital age.

II. KEYWORDS

Critical infrastructure protection; cybersecurity governance; securitization theory; surveillance governance; Liberia.

III. INTRODUCTION

The protection of critical national infrastructure has become a central concern of contemporary national security policy in the digital age. As governments increasingly rely on interconnected information and communication technologies to manage strategic assets, the security of digital systems has become inseparable from the security of the state itself. Critical infrastructure, including airports, seaports, energy facilities, telecommunications networks, and financial systems, forms the backbone of national economic stability, public safety, and state sovereignty. Consequently, vulnerabilities within these infrastructures can generate far-reaching security implications that extend beyond their immediate operational environments (Lewis, 2006; Organisation for Economic Co-operation and Development [OECD], 2019).

In this context, critical infrastructure protection is not only a technical and operational responsibility but also a legal governance obligation requiring effective regulatory frameworks, institutional coordination, accountability mechanisms, and protection of sensitive information assets.

The growing digitalization of critical infrastructure has transformed the nature of contemporary security threats. Whereas infrastructure protection was traditionally concerned with physical threats such as sabotage, terrorism, and criminal attacks, contemporary security environments increasingly encompass cyber intrusions, data breaches, information manipulation, and unauthorized disclosures of sensitive information (Boin & McConnell, 2007; Singer & Friedman, 2014). This transformation has created new legal and institutional challenges concerning cybersecurity governance, digital evidence protection, surveillance accountability, and the regulation of access to sensitive operational information.

These challenges are particularly significant for developing countries, where the adoption of digital technologies often advances more rapidly than the establishment of comprehensive cybersecurity legislation, institutional safeguards, and technical capacities necessary to protect strategic national assets. As a result, vulnerabilities within critical infrastructure systems have become not only operational concerns but also matters of national security, legal governance, and state resilience.

Airports occupy a particularly significant position within the critical infrastructure landscape because they serve as gateways for international travel, trade, migration, and security operations. Beyond their economic importance, airports perform strategic national security functions, including border control, customs enforcement, intelligence gathering, and the interdiction of transnational organized crime. Consequently, aviation facilities have increasingly become targets of both physical and cyber threats, prompting governments worldwide to strengthen airport security, surveillance systems, and regulatory frameworks governing aviation security (International Civil Aviation Organization [ICAO], 2022).

Modern airport operations rely heavily on digital surveillance technologies, including closed-circuit television (CCTV) systems, biometric technologies, access-control mechanisms, and integrated information networks. While these technologies enhance operational efficiency and security monitoring, they simultaneously introduce new vulnerabilities associated with cyber intrusions, insider threats, unauthorized disclosure, and evidentiary management of digital records (Wall, 2017).

Roberts International Airport (RIA) represents one of Liberia's most strategically important critical infrastructure assets. Like major international airports elsewhere, RIA performs essential functions relating to national security, economic development, international connectivity, and border governance. Consequently, concerns regarding the security and integrity of its operational systems extend beyond airport administration to broader questions concerning national security, institutional resilience, and legal accountability. These concerns gained prominence following the investigation into the seizure of approximately 237.6 kilograms of cocaine, valued at more than US$19.2 million, at RIA in June 2026 (Watson, 2026; Verity News, 2026a).

During the period in which the Government of Liberia, through the Joint Investigative Task Force, was conducting investigations into the matter, CCTV footage allegedly linked to the incident surfaced on social media after being released by Verity Online News and circulated by a private citizen outside formal state channel (Verity News, 2026b). The incident generated significant public and institutional attention, raising questions not only about surveillance-system security but also about the legal governance of digital evidence, investigative confidentiality, and institutional responsibility for protecting sensitive operational information.

Within Liberia's existing legal framework, these concerns intersect with the Controlled Drugs and Substances Act of 2023, which provides the basis for prosecuting serious drug trafficking offences, the Criminal Procedure Law, which governs criminal investigations and evidentiary procedures, and the broader regulatory environment governing electronic communications and information security. However, the absence of a comprehensive statutory framework specifically addressing cybersecurity governance, digital evidence management, and critical infrastructure protection creates important questions concerning institutional capacity and legal preparedness.

The concerns raised by the controversy mirror broader debates within cybersecurity governance literature regarding the protection of surveillance systems and operational data within critical infrastructure environments. Cybersecurity governance literature increasingly emphasizes that unauthorized exposure of surveillance data in critical

infrastructure environments can undermine operational security, legal accountability, and institutional trust (Thistlethwaite & Henstra, 2026; Amod Agarkar et al., 2025; Ferguson, 2023). Moreover, recent research on critical infrastructure cybersecurity highlights that breaches or leaks of sensitive operational data, including surveillance and monitoring systems, can compromise confidentiality, integrity, and availability, thereby weaken operational resilience and expose systems to adversarial exploitation (Nott, 2025; NIST, 2024). Similarly, insider-threat and user-behavior studies demonstrate that unauthorized access or disclosure of security system data significantly increases institutional vulnerability and reduces public confidence in security governance structures (Amod Agarkar et al., 2025; Swire et al., 2024).

From a governance perspective, emerging policy frameworks such as the OECD cybersecurity governance guidelines emphasize that inadequate information-control mechanisms within critical infrastructure systems can undermine trust between governmental institutions and the public, particularly when sensitive security data is exposed or improperly disseminated (OECD, 2024). These concerns are especially relevant in environments where legal frameworks governing cybersecurity, digital evidence, and surveillance accountability remain fragmented. Although public discussions surrounding the RIA incident largely focused on the evidentiary value of the footage and the identities of individuals appearing in the recordings, the broader national security issue concerns the perception that surveillance footage associated with a critical national asset could be accessed and disseminated outside established institutional procedures.

From a national security and legal governance perspective, the issue is therefore not merely the content of the footage but the potential vulnerabilities—actual or perceived—that enabled its circulation. Such concerns raise important questions regarding cybersecurity governance, insider threats, access-control mechanisms, digital evidence preservation, chain-of-custody procedures, and institutional accountability. Whether actual or perceived, weaknesses within surveillance systems may undermine public confidence in the state's ability to protect strategic facilities and safeguard sensitive operational information.

Despite growing scholarly attention to critical infrastructure protection, cybersecurity governance, and airport security, relatively limited research has examined how surveillance-related controversies within critical infrastructure settings influence national security perceptions, legal debates, and institutional reform processes in developing states. Existing studies have focused primarily on technical vulnerabilities, cyberattacks, and infrastructure resilience in advanced industrialized contexts, leaving a significant gap in understanding how alleged information-security breaches are interpreted, contested, legally regulated, and securitized within emerging democracies and developing security environments. Consequently, there remains limited empirical and theoretical understanding of how incidents involving surveillance systems can shape public perceptions of infrastructure vulnerability and influence broader debates concerning national security governance and legal institutional capacity.

Against this backdrop, this article examines the national security implications of the CCTV footage controversy associated with RIA through the combined lenses of Critical Infrastructure Protection, Securitization Theory, and Liberia's legal and institutional framework governing criminal investigations, digital evidence, and information security. The article argues that the controversy should be understood not merely as a debate surrounding a criminal investigation but as a strategic warning regarding potential vulnerabilities within Liberia's critical infrastructure architecture and legal governance systems. Specifically, it explores how concerns relating to surveillance-system security, information governance, evidentiary integrity, and institutional safeguards can transform localized controversies into broader national security issues.

By analyzing the RIA CCTV footage controversy, the study contributes to emerging debates on critical infrastructure protection, cybersecurity governance, digital evidence regulation, the securitization of infrastructure vulnerabilities, and national security resilience in developing states. The article further provides policy recommendations aimed at strengthening Liberia's legal and institutional capacity to protect strategic national assets in an increasingly digitized security environment.

A. Background to the US$19.2 million cocaine seizure at RIA

RIA is Liberia's principal international gateway and a strategic national infrastructure asset for air transport, trade facilitation, border control, and national security operations. On 8 June 2026, the LDEA, working with joint security units assigned to the airport, intercepted approximately 237.6 kilograms of cocaine concealed in cargo destined for Europe and valued at more than US$19.2 million (Yaste, 2026; Watson, 2026).

The Government of Liberia subsequently initiated a multi-agency investigation through the National Joint Security under the National Security Council, reflecting concerns about transnational trafficking networks and possible internal facilitation within airport operations (LDEA, 2026; Yaste, 2026). The matter intensified when the 13th Judicial Circuit Court in Margibi County issued a subpoena requiring production of CCTV footage and cargo-handling records relevant to reconstructing the consignment's movement (KMTV News, 2026). The later circulation of CCTV-related materials on digital platforms raised broader concerns about evidence control, surveillance governance, institutional accountability, and the protection of sensitive security information within critical infrastructure environments.

B. Description of the Released CCTV Footage and Its Legal-Institutional Significance

The circulated CCTV footage that emerged within the Liberian social media environment was presented as a three-episode sequence documenting events allegedly associated with the movement and handling of a suspected narcotics consignment at RIA, with particular reference to activities occurring on Friday, 22 May 2026 (Verity Online News's Post, 2026). Although the authenticity, provenance, and evidentiary status of the footage remain matters requiring formal verification through appropriate investigative and judicial processes, the circulation of the material generated significant public and institutional debate regarding surveillance governance, digital evidence management, and the protection of sensitive information associated with critical infrastructure.

From a legal perspective, the significance of the footage extends beyond its visual content. Under Liberia's existing criminal procedure framework, digital materials such as CCTV

recordings may constitute potentially relevant evidence in criminal proceedings where issues of authenticity, reliability, relevance, and integrity can be established. However, the evidentiary value of such materials depends not only upon what the footage depicts but also upon the manner in which it was obtained, preserved, transferred, and presented. Consequently, questions concerning access authorization, chain of custody, institutional control, and possible alteration become central considerations when assessing the legal and investigative significance of surveillance footage.

Episode 1 presents a narrative concerning the transportation of approximately 100 kilograms of suspected cocaine to the airport premises using a yellow taxicab identified by license plate TX 10609. The footage reportedly shows multiple packaged items described as four boxes inside the vehicle. According to the accompanying narrative, the taxi entered the fenced premises of the Roberts Air Cargo Center at approximately 15:30 hours. The Air Cargo Center is identified as being operated and managed by GLS Menzies, a cargo-handling services concessionaire. The same vehicle is reportedly shown leaving the airport premises at approximately 15:49 hours, indicating a period of approximately nineteen minutes within the restricted cargo compound (Verity Online News's Post, 2026).

However, subsequent reporting based on Heathrow cargo and customs records contradicted the claim that the May 22 consignment constituted a successful cocaine shipment that "slipped through" RIA, indicating instead that the consignment was cleared by British customs and signed for by its named recipient on June 3. This later development substantially limits the empirical weight that can be placed on Episode 1 as proof of a prior drug shipment, while strengthening the securitization analysis by demonstrating how a disputed surveillance narrative may nevertheless generate public perceptions of critical-infrastructure vulnerability.

The legal significance of this sequence therefore lies less in treating the May 22 shipment narrative as independently established fact and more in the institutional questions generated by the circulation of the footage itself. If authenticated through appropriate investigative procedures, surveillance footage depicting activity within a controlled airport facility may provide relevant information concerning movement patterns, access

authorization, and operational procedures. However, where subsequent documentary reporting contradicts a central claim attached to the footage narrative, the material must be handled with caution and distinguished from verified evidence. The episode remains analytically relevant because its circulation outside formal investigative channels raised questions regarding institutional responsibility for safeguarding surveillance records, preventing misinformation around active investigations, and protecting sensitive operational information associated with critical infrastructure.

Episode 2 continues the sequence by presenting additional individuals and activities allegedly associated with the delivery and handling process of the consignment. The footage is accompanied by claims identifying certain actors connected to transportation and logistics functions as being involved in the movement of the cargo. The episode also refers to a corporate entity allegedly listed as the shipper or consignor on the relevant Air Waybill; however, secondary reports differ as to whether the entity was recorded as "Emre Venn Group of Companies" or "EM Van Group of Companies." Accordingly, the precise corporate name and Air Waybill number should be verified directly from the original Air Waybill or official court exhibits before final submission. The material further claims that the referenced entity could not be verified within Liberia's official business registration and tax systems (Verity Online News's Post, 2026).

Beyond the allegations presented in the footage narrative, this episode highlights broader institutional issues relating to cargo governance, corporate verification, regulatory oversight, and inter-agency information coordination. In critical infrastructure environments such as international airports, effective security governance requires cooperation among airport authorities, customs agencies, law enforcement institutions, immigration authorities, and private-sector logistics operators. The alleged inconsistencies involving cargo documentation and corporate identity therefore raise questions regarding the adequacy of information-sharing mechanisms and regulatory controls within Liberia's aviation security environment.

Episode 3 expands the sequence by presenting additional narrative claims regarding the logistical chain associated with the shipment. It references the continued use of the consignor identity in cargo documentation and outlines additional individuals and

entities allegedly connected to the transportation and handling process. The footage sequence also refers to the role of cargo-handling operations at the airport and the movement of goods through the Air Cargo Center under the supervision of relevant logistics operators (Verity Online News's Post, 2026).

Collectively, the three episodes present a chronological visual narrative concerning the alleged movement, handling, and documentation of a suspected narcotics consignment at RIA, structured around timestamped surveillance footage and accompanying documentary annotations. However, from a socio-legal perspective, the significance of the footage extends beyond the allegations depicted. The episode sequence raises fundamental questions regarding the governance of digital surveillance systems, the protection of electronic evidence, institutional accountability, and the legal safeguards necessary to protect critical infrastructure information.

The controversy surrounding the release of the footage demonstrates the tension between transparency and investigative confidentiality within criminal justice systems. While public access to information may contribute to accountability and institutional oversight, unauthorized disclosure of investigative materials may compromise ongoing investigations, affect evidentiary integrity, and undermine established legal procedures. This tension is particularly significant in Liberia's context, where the existing legal framework provides mechanisms for criminal investigation and evidentiary evaluation but lacks a comprehensive statutory regime specifically regulating digital surveillance governance, cybersecurity obligations, and critical infrastructure information protection. Accordingly, the CCTV footage controversy serves as an important case through which to examine how surveillance exposure within a strategic national asset can become securitized. The issue is not limited to the alleged criminal conduct depicted in the footage but extends to broader concerns regarding whether Liberia possesses sufficient legal, institutional, and technological safeguards to protect sensitive surveillance information and maintain public confidence in critical infrastructure governance**.**

C. Statement of the Problem

In the contemporary security environment, critical national infrastructure is increasingly exposed to complex and evolving threats that extend beyond traditional physical risks to include cyber vulnerabilities, information exposure, unauthorized access, and insider-enabled compromises. Airports, as strategic nodes within national and international security systems, are particularly sensitive because they perform dual functions: facilitating legitimate transnational mobility and trade while simultaneously serving as potential entry points for transnational organized crime, illicit trafficking networks, and other security threats.

In Liberia, the RIA constitutes the country's primary international aviation gateway and a critical component of its national infrastructure. Beyond its economic and transportation functions, RIA performs strategic security roles relating to border management, customs enforcement, migration control, and the prevention of transnational criminal activities. Consequently, the protection of its physical and digital security systems represents an essential component of Liberia's national security architecture. Recent developments surrounding the seizure of a significant quantity of cocaine allegedly transported through RIA have generated substantial public and institutional attention regarding the effectiveness of airport security governance and the integrity of surveillance and information-management systems.

Of particular concern is the circulation of CCTV footage on social media platforms depicting activities allegedly associated with the movement and handling of the suspected narcotics consignment within airport premises. Although questions concerning the authenticity, provenance, and evidentiary status of the footage require determination through appropriate investigative and judicial processes, its public dissemination raises important legal, institutional, and security concerns. Specifically, the incident highlights questions regarding the protection of digital evidence, the preservation of investigative confidentiality, access-control mechanisms, surveillance-system governance, and institutional responsibility for safeguarding sensitive information generated within critical infrastructure environments.

From a legal and governance perspective, the controversy exposes potential weaknesses within Liberia's existing framework for regulating digital surveillance and information security. While Liberia maintains legal provisions governing criminal investigations, drug trafficking offences, and evidentiary procedures through instruments such as the Controlled Drugs and Substances Act of 2023 and the Criminal Procedure Law, the country lacks a comprehensive statutory framework specifically addressing cybersecurity governance, digital evidence management, surveillance accountability, and critical information infrastructure protection. This regulatory fragmentation creates uncertainty concerning institutional obligations, cybersecurity standards, and accountability mechanisms for protecting sensitive surveillance systems operated within strategic national facilities.

The public dissemination of surveillance footage from a strategically sensitive facility therefore raises broader questions concerning the relationship between physical security operations and cybersecurity governance. Critical infrastructure protection increasingly requires integration between access-control systems, surveillance technologies, information-security protocols, and legal safeguards governing the collection, storage, disclosure, and use of digital information. Weaknesses in any of these areas may undermine operational security, compromise investigative processes, and reduce public confidence in state institutions responsible for protecting national assets.

Despite the strategic importance of airport security to national sovereignty and national security, limited empirical research has examined how vulnerabilities in surveillance systems, digital information management practices, and legal governance structures within Liberian critical infrastructure may influence broader security outcomes. Existing studies have largely focused on traditional security threats, drug trafficking, or institutional capacity challenges, leaving insufficient attention to how surveillance-related vulnerabilities may become national security concerns within developing-state contexts. Furthermore, the extent to which such vulnerabilities may arise through insider access, inadequate cybersecurity controls, weak evidence-management procedures, or institutional coordination failures remains insufficiently explored.

It is against this background that the problem of this study is situated: the limited understanding of how vulnerabilities in surveillance and information-security systems within Liberia's critical infrastructure, particularly Roberts International Airport, may compromise national security, legal accountability, institutional integrity, and operational resilience in an increasingly digitized security environment. The study therefore examines the RIA CCTV footage controversy as a socio-legal and security governance issue, analyzing how surveillance exposure within a critical national asset can reveal broader challenges relating to cybersecurity governance, digital evidence protection, institutional coordination, and the resilience of Liberia's national security architecture.

D. Research Objectives

The main objective of this study is to examine the national security, legal, and institutional implications of vulnerabilities in surveillance and information-security systems within Liberia's critical infrastructure, using the RIA CCTV footage controversy as a case study. Specifically, the study seeks to analyze how weaknesses in surveillance governance, digital evidence management, cybersecurity regulation, and institutional coordination may affect critical infrastructure protection, public trust, and national security resilience in Liberia. To achieve this aim, the study is guided by the following specific objectives:

1. To examine the legal and institutional framework governing critical infrastructure protection, digital evidence, and surveillance governance in Liberia.
2. To analyze how vulnerabilities in RIA's surveillance and information-security systems contributed to broader concerns regarding national security and institutional resilience.
3. To assess the implications of the CCTV footage controversy for digital evidence integrity, investigative confidentiality, and cybersecurity governance within Liberia's critical infrastructure environment.

4. To apply Securitization Theory to explain how perceived vulnerabilities in airport surveillance systems were constructed as national security concerns through public, institutional, and media discourse.
5. To identify legal, institutional, and policy reforms necessary to strengthen critical infrastructure protection and surveillance governance in Liberia's digital security environment.

E. Research Questions

What is the national security, legal, and institutional implications of vulnerabilities in surveillance and information-security systems within Liberia's critical infrastructure, as illustrated by the RIA CCTV footage controversy? To address this central question, the study is guided by the following specific research questions:

1. What legal and institutional frameworks govern critical infrastructure protection, digital evidence, and surveillance governance in Liberia?
2. How do vulnerabilities in surveillance and information-security systems within Roberts International Airport affect critical infrastructure protection, national security, and institutional resilience?
3. What are the implications of the RIA CCTV footage controversy for digital evidence integrity, investigative confidentiality, cybersecurity governance, and institutional accountability?
4. How does Securitization Theory explain the process through which perceived vulnerabilities in airport surveillance systems became framed as national security concerns?
5. What legal, institutional, and policy reforms are necessary to strengthen critical infrastructure protection, surveillance governance, and national security resilience in Liberia's digital security environment?

F. Research Methodology

This study adopted a qualitative research design to examine the national security implications of vulnerabilities in surveillance and information systems within Liberia's

critical infrastructure, using the RIA CCTV footage incident as a case study. The qualitative approach was considered appropriate because the study sought to interpret meanings, institutional practices, and security implications rather than measure statistical relationships. It enabled an in-depth exploration of how surveillance-related incidents were framed within national security discourse and how such framing related to critical infrastructure protection in the digital age (Creswell & Creswell, 2018).

G. Research Design

The study was structured as a single-case study design, focusing on the RIA CCTV footage incident as an illustrative case of critical infrastructure vulnerability. The case study approach was suitable for examining complex, real-world phenomena where contextual conditions were integral to understanding the issue under investigation (Yin, 2018). In this context, the RIA incident was treated as a critical event through which broader issues of cybersecurity governance, insider threats, and surveillance system vulnerabilities could be analytically examined.

1. **Data Sources:** The study relied exclusively on secondary data sources, including publicly circulated CCTV footage and associated documentary episodes available on social media platforms, official statements and public communications from relevant government and security institutions, policy documents on aviation security and critical infrastructure protection, national and international legal frameworks, legislation, and reports on cybersecurity and airport security (e.g., ICAO, NIST, OECD), and scholarly literature on critical infrastructure protection, cybersecurity governance, and Securitization Theory. These sources were used to construct a narrative and analytical understanding of the incident within the broader national security and cybersecurity governance context.
2. **Data Analysis:** Data were analyzed using qualitative content analysis. This involved systematic coding and interpretation of textual, visual, and documentary materials related to the CCTV footage narrative and associated commentary. The analysis focused on identifying recurring themes, including

surveillance system vulnerabilities, access control and information security weaknesses, insider threat indicators, institutional and governance gaps, and the national security framing of infrastructure-related incidents. Thematic interpretation was guided by Securitization Theory, which provided an analytical lens for understanding how surveillance-related incidents could be constructed as national security issues through discourse and institutional framing.

3. **Validity and Trustworthiness:** To enhance the credibility of the analysis, the study applied triangulation of sources by comparing multiple forms of publicly available data, including video narratives, policy documents, and academic literature. In addition, the study maintained analytical transparency by clearly distinguishing between descriptive reporting of circulated materials and theoretical interpretation.
4. **Ethical Considerations:** The study relies solely on publicly available materials circulated in the public domain. No private data collection or human subject interaction was conducted. Care is taken to avoid definitive attribution of criminal responsibility, as the focus of the study is on systemic vulnerabilities in critical infrastructure protection rather than legal adjudication of individual conduct.

H. Significance of the Study

This study contributes to scholarship on Securitization Theory, cybersecurity governance, critical infrastructure protection, and socio-legal approaches to digital security governance, particularly within developing-state contexts. Theoretically, it extends Securitization Theory beyond its traditional focus on military and terrorism-related threats by demonstrating its applicability to surveillance-system vulnerabilities, digital information exposure, and cybersecurity controversies within critical infrastructure environments. It shows how perceived exposure of surveillance data can be socially and institutionally constructed as a national security concern, thereby

expanding securitization analysis into emerging domains of cybersecurity, infrastructure governance, and digital resilience (Buzan et al., 1998; Wæver, 1995; Livingston, 2025).

Legally and institutionally, the study contributes to understanding the relationship between critical infrastructure protection, digital evidence governance, and national security regulation in Liberia. By examining the RIA CCTV footage controversy through the lens of Liberia's criminal justice, evidentiary, and information-security frameworks, the study highlights the importance of legal safeguards governing surveillance systems, digital evidence preservation, investigative confidentiality, and institutional accountability. It contributes to ongoing discussions regarding the need for comprehensive legal frameworks capable of addressing cybersecurity governance, digital surveillance protection, and the responsibilities of institutions operating strategic national assets.

Empirically, the study adds context-specific evidence from Liberia's RIA, addressing a gap in existing literature that has largely examined critical infrastructure cybersecurity and surveillance governance in advanced economies while giving comparatively limited attention to African aviation systems, developing-state security environments, and institutional capacity challenges (OECD, 2024; NIST, 2024). By focusing on the intersection between surveillance technology, transnational organized crime, legal governance, and national security, the study provides insights into how infrastructure vulnerabilities are perceived and managed in contexts where regulatory frameworks and institutional capacities remain under development.

From a policy perspective, the study highlights the importance of strengthening surveillance-system security, access-control mechanisms, cybersecurity governance structures, digital evidence management procedures, and inter-agency coordination within critical infrastructure environments. It further demonstrates that even where the authenticity or evidentiary status of a security-related incident remains contested, the perceived vulnerability and public framing of such incidents can generate significant national security implications through institutional interpretation, public discourse, and demands for governance reform.

 (ISSN: 2583-7753)

Ultimately, the study contributes to both theoretical and practical debates by demonstrating that critical infrastructure security in the digital age depends not only on technological capabilities but also on the strength of legal frameworks, institutional arrangements, and public trust mechanisms necessary to protect strategic national assets.

I. Delimitations of the Study

This study was delimited to examining the national security, legal, and institutional implications of surveillance-system vulnerabilities within Liberia's critical infrastructure, using the RIA CCTV footage controversy as a single illustrative case. Geographically, the study focused on Liberia, with specific reference to RIA as a strategic aviation facility within the country's national security architecture. Although international examples and comparative experiences were referenced selectively for contextual grounding, the study did not extend to comparative case analyses involving other jurisdictions.

Substantively, the study focused on the intersection between critical infrastructure protection, surveillance governance, cybersecurity, digital evidence management, and institutional resilience. The analysis examined how vulnerabilities associated with surveillance systems, access-control mechanisms, information-security practices, and regulatory arrangements may affect national security outcomes. It further considered the legal and institutional frameworks governing criminal investigations, digital evidence, investigative confidentiality, and information protection within Liberia. However, the study did not attempt to provide a comprehensive examination of all aspects of Liberian criminal law, cybersecurity regulation, or aviation security legislation beyond those directly relevant to the RIA CCTV footage controversy.

The study did not undertake a technical forensic investigation into the authenticity, source, ownership, or digital integrity of the circulated CCTV footage. Rather, the analysis focused on the governance, legal, and security implications arising from the circulation of the footage and how the incident was interpreted within public and institutional discourse. Accordingly, the study examined the footage controversy as a socio-legal and security governance phenomenon rather than as a forensic examination of digital evidence.

Methodologically, the study relied exclusively on secondary data sources, including publicly available media reports, official statements, policy documents, legislative instruments, international reports, and scholarly literature. No primary data collection, interviews, surveys, or access to restricted government, law enforcement, or airport security databases were undertaken. Therefore, the study's conclusions are limited to the information available through publicly accessible sources.

Conceptually, the study was guided by Securitization Theory and critical infrastructure protection frameworks, supplemented by socio-legal analysis of Liberia's legal and institutional arrangements governing surveillance systems, digital evidence, and information security. The study emphasizes how perceived vulnerabilities within strategic infrastructure can be socially and institutionally constructed as national security concerns, while recognizing the importance of legal safeguards and governance mechanisms in shaping responses to emerging digital security challenges within public and institutional discourse.

J. Limitations of the Study

This study is subject to several limitations that should be considered when interpreting its findings. First, the study relied exclusively on secondary data sources, including publicly available media reports, official statements, policy documents, legislative materials, and scholarly literature. Consequently, it did not involve primary data collection, such as interviews with airport administrators, law enforcement officials, cybersecurity specialists, legal practitioners, or national security personnel, which could have provided additional institutional perspectives regarding surveillance governance, digital evidence management, and critical infrastructure protection.

Second, the study did not undertake a technical forensic examination of the CCTV footage or the associated digital surveillance systems. Therefore, it did not independently verify the authenticity, origin, ownership, chain of custody, or technical integrity of the circulated footage. Instead, the analysis focused on the legal, institutional, and national security implications arising from the circulation of the footage and the manner in which

the controversy was interpreted, framed, and securitized within public and institutional discourse.

Third, although the study incorporated analysis of Liberia's legal and institutional framework governing criminal investigations, digital evidence, surveillance governance, and critical infrastructure protection, it was not designed as a comprehensive doctrinal examination of all aspects of Liberian criminal law, cybersecurity regulation, or aviation security legislation. The legal analysis was therefore limited to provisions and institutional arrangements directly relevant to understanding the RIA CCTV footage controversy.

Fourth, the study was limited to a single-case design focusing on Roberts International Airport in Liberia. While this approach enabled an in-depth contextual examination of the interaction between surveillance vulnerabilities, legal governance, and national security discourse, the findings may not be generalized directly to other critical infrastructure environments or jurisdictions without appropriate consideration of contextual differences.

Fifth, the analysis was primarily qualitative, interpretive, and discourse-based. As such, the findings are informed by the theoretical assumptions of Securitization Theory and critical infrastructure protection frameworks, which emphasize how threats are socially and institutionally constructed. This interpretive approach introduces a degree of analytical subjectivity inherent in qualitative research, although efforts were made to maintain methodological consistency through systematic document analysis.

Finally, the rapidly evolving nature of cybersecurity threats, digital surveillance technologies, and online information circulation means that additional evidence, institutional responses, or legal developments may emerge over time. Such developments may influence future interpretations of the RIA CCTV footage controversy and the broader assessment of Liberia's critical infrastructure protection capacity.

K. Literature Review

For the purpose of this article, the literature review focuses on the following thematic areas:

1. Critical Infrastructure Protection, Airports, and National Security

The literature on critical infrastructure protection consistently conceptualizes infrastructure systems as the backbone of national security, economic stability, and state functionality (National Institute of Standards and Technology [NIST], 2023; Organisation for Economic Co-operation and Development [OECD], 2024). Contemporary scholarship, however, increasingly emphasizes that critical infrastructure is no longer purely physical but embedded within cyber-physical ecosystems, where digital systems govern essential operational functions such as surveillance, logistics, and access control (Paulraj et al., 2025).

Airports are repeatedly identified as among the most sensitive categories of critical infrastructure due to their dual role in facilitating international mobility and enforcing national security controls (International Civil Aviation Organization [ICAO], 2023). Recent aviation security literature further demonstrates that airports are increasingly exposed to hybrid threats that combine physical intrusion, cyber manipulation, and information leakage (Florido-Benítez, 2024). In this regard, cargo terminals and surveillance systems represent particularly vulnerable nodes due to their integration of private operators, state agencies, and digital monitoring systems.

In the context of the RIA CCTV footage incident, these findings are directly relevant. The circulation of surveillance footage depicting alleged cargo movement within a restricted airport environment illustrates how digital surveillance systems embedded within critical infrastructure can become exposure points for sensitive operational information. The case reflects the exact vulnerability trajectory identified in the literature: the transition from secure physical infrastructure to digitally exposed operational intelligence.

2. Emerging Threats to Critical Infrastructure and the RIA Case

Recent cybersecurity governance literature identifies emerging threats to critical infrastructure as increasingly hybridized, involving ransomware, insider compromise, supply-chain infiltration, and data exfiltration (NIST, 2024; GAO, 2023). A particularly

relevant trend is the rise of cyber-physical convergence threats, where digital breaches directly affect physical operations and security environments (Paulraj et al., 2025).

The RIA CCTV incident aligns with this emerging threat pattern. Although no cyberattack is formally established in the case narrative, the public dissemination of surveillance footage demonstrates the operational consequences of information exposure within a critical infrastructure environment. The literature shows that even without system disruption, the unauthorized release of operational data can compromise security planning, expose procedural vulnerabilities, and enable adversarial mapping of infrastructure behavior (OECD, 2024).

In aviation contexts, global studies have shown that exposure of airport operational systems—including surveillance and cargo tracking systems- can create secondary security risks by revealing timing patterns, movement flows, and access procedures (Florido-Benítez, 2024). The RIA case reflects this concern through the public availability of timestamped footage allegedly showing cargo movement within restricted airport space.

3. Surveillance Systems, Cybersecurity, and the RIA Case

The literature on surveillance system security highlights that modern CCTV infrastructures are increasingly IP-based and interconnected with broader airport networks, making them vulnerable to unauthorized access, misconfiguration, or insider exploitation (NIST, 2023). These systems are particularly sensitive because they combine real-time monitoring with stored operational intelligence, often without sufficient segmentation from other digital systems.

In this context, the RIA CCTV footage incident illustrates a key vulnerability identified in cybersecurity literature: the potential for surveillance systems to become data leakage points rather than purely protective tools. NIST (2023, 2024) emphasizes that insufficient access controls, weak authentication mechanisms, and inadequate audit trails are common weaknesses in operational technology environments, including surveillance systems. The RIA case aligns with this concern by demonstrating how surveillance footage from a restricted airport environment entered the public domain through social

media circulation. While the precise mechanism of access is not established, the literature suggests several plausible pathways identified in similar global cases, including insider access misuse, credential compromise, or inadequate system segmentation.

4. Insider Threats and Institutional Vulnerabilities in the RIA Case

A dominant strand in cybersecurity governance literature identifies insider threats as one of the most significant risks to critical infrastructure systems, particularly in environments where multiple actors share access privileges (Swire et al., 2024; Amod Agarkar et al., 2025). Insider threats are not limited to malicious intent but also include negligence, procedural violations, and unauthorized information sharing. Airports represent high-risk environments for insider threats due to the presence of multi-agency operational ecosystems, including customs, immigration, private cargo handlers, security contractors, and law enforcement agencies. This fragmentation increases the complexity of access control and accountability systems.

The RIA CCTV footage incident fits squarely within this literature-based risk profile. The circulation of sensitive surveillance material from within a restricted airport environment suggests a breakdown in information governance and access accountability mechanisms, which are central concerns in insider threat research. Swire et al. (2024) further note that unauthorized disclosure of sensitive operational data not only compromises security but also weakens institutional trust in governance systems. In the RIA case, the public availability of surveillance footage depicting cargo movement within a secure airport environment directly reflects this dual risk: operational exposure and institutional legitimacy erosion.

IV. LEGAL AND INSTITUTIONAL FRAMEWORK GOVERNING CRITICAL INFRASTRUCTURE PROTECTION AND DIGITAL EVIDENCE IN LIBERIA

The protection of critical infrastructure has increasingly become both a national security and a legal governance concern, particularly in states confronting transnational organized crime and rapidly expanding digital technologies. While the concept of critical

infrastructure protection has traditionally been associated with security and emergency management, contemporary scholarship recognizes that effective protection requires a coherent legal and institutional framework capable of regulating infrastructure security, digital surveillance, electronic evidence, and inter-agency coordination. The RIA cocaine seizure and the subsequent controversy surrounding the circulation of CCTV footage illustrate the intersection between criminal law, evidence law, cybersecurity governance, and national security in Liberia.

From a doctrinal perspective, Liberia's legal framework governing this intersection remains fragmented. Although the country possesses legislation regulating criminal investigations and drug trafficking, it has yet to enact a comprehensive statutory framework specifically addressing critical infrastructure protection, cybersecurity governance, or the protection of digital surveillance systems. Consequently, the legal analysis of the present study draws upon four interrelated sources of law: the 1986 Constitution of Liberia, the Criminal Procedure Law, the Controlled Drugs and Substances Act of 2023, and Liberia's Telecommunications Act of 2007, as amended, supplemented by applicable principles of the common law of evidence and relevant international standards.

A. Constitutional and Institutional Foundations

The Constitution of Liberia establishes the rule of law as the foundation of public administration and vests the State with responsibility for protecting public order, national security, and the rights of citizens. Although the Constitution does not expressly define "critical infrastructure," its guarantees relating to public safety, due process, and the administration of justice provide the constitutional basis for governmental protection of strategic national assets, including airports, seaports, telecommunications systems, and other infrastructure essential to national security and economic stability.

Institutionally, responsibility for protecting critical infrastructure is dispersed among several public agencies. RIA operates under the Liberia Airport Authority, while law enforcement responsibilities are shared among the Liberia National Police, the Liberia Drug Enforcement Agency, the National Security Agency, immigration authorities,

customs officials, and the Ministry of Justice. This institutional arrangement reflects a multi-agency security model; however, the absence of a dedicated statutory framework defining institutional responsibilities for critical infrastructure protection creates overlapping mandates and coordination challenges, particularly during complex criminal investigations involving transnational organized crime.

B. Statutory Framework Governing Drug Trafficking and Criminal Investigation

The principal statutory instrument governing the prosecution of the RIA cocaine seizure is the Controlled Drugs and Substances Act of 2023. The Act significantly strengthened Liberia's legal response to illicit drug trafficking by introducing more stringent penalties, classifying major trafficking offences as serious felonies, expanding investigative powers, and reinforcing the State's commitment to combating organized criminal networks. The legislation reflects legislative recognition that large-scale narcotics trafficking constitutes not merely an ordinary criminal offence but a threat to national security, public health, economic stability, and international obligations.

The criminal investigation and prosecution of offences under the Act are further governed by the Criminal Procedure Law, which establishes procedural safeguards relating to search and seizure, arrest, admissibility of evidence, and defendants' constitutional rights. The Criminal Procedure Law also provides mechanisms for challenging unlawfully obtained evidence through motions to suppress, thereby balancing effective law enforcement with the protection of individual rights.

The interaction between these statutes demonstrates that successful prosecution of transnational drug trafficking depends not only upon seizure of illicit substances but also upon the integrity of investigative procedures, documentary evidence, digital surveillance records, and institutional compliance with established evidentiary standards.

Digital Evidence, CCTV Surveillance, and the Law of Evidence. The controversy surrounding the subpoena and subsequent public circulation of CCTV footage from RIA raises significant questions concerning the legal status of digital evidence in Liberia. Unlike several jurisdictions that have enacted specialized legislation governing electronic

evidence, Liberia principally relies upon the Criminal Procedure Law together with applicable principles of the common law of evidence.

Chapter 21 of the Criminal Procedure Law provides that the admissibility of evidence in criminal proceedings is governed first by the Criminal Procedure Law itself, second by applicable provisions of the Civil Procedure Law, and, where statutory guidance is absent, by the common law of evidence as interpreted by Liberian courts. This provision establishes the doctrinal basis upon which electronic evidence, including CCTV recordings, may be admitted, authenticated, and evaluated during criminal proceedings. Although the Criminal Procedure Law does not expressly regulate CCTV recordings or other forms of digital evidence, its reliance upon common-law evidentiary principles necessarily requires proof of authenticity, reliability, relevance, and integrity before such material may be admitted in judicial proceedings. Consequently, maintaining an uninterrupted chain of custody assumes particular importance. Every transfer, storage, duplication, or forensic examination of digital evidence should be capable of independent verification to ensure that the evidence has not been altered, manipulated, or contaminated.

The unauthorized disclosure or circulation of surveillance footage before judicial determination may not necessarily render the evidence inadmissible; however, it may compromise investigative confidentiality, prejudice criminal proceedings, undermine witness protection, and diminish public confidence in the administration of justice. The RIA incident therefore demonstrates that legal admissibility alone is insufficient. Effective governance also requires institutional protocols governing access control, digital preservation, evidence management, and accountability for unauthorized disclosure.

C. Cybersecurity and Information Security Governance

A significant weakness in Liberia's legal architecture concerns the regulation of cybersecurity and digital information systems. Current assessments indicate that Liberia has not enacted a comprehensive cybercrime statute or a dedicated data protection law comparable to those adopted in several other African jurisdictions. Instead, Liberia's

Telecommunications Act of 2007, as amended, provides only limited provisions relating to electronic communications, certain telecommunications offences, and procedural powers associated with search and seizure within the telecommunications sector.

This legislative gap has important implications for critical infrastructure protection. Modern surveillance systems—including airport CCTV networks, digital access controls, biometric databases, and electronic communication platforms—constitute components of national critical infrastructure whose compromise may threaten public safety, border security, and criminal investigations. Yet Liberia presently lacks an integrated statutory framework establishing minimum cybersecurity standards, mandatory incident reporting obligations, digital evidence preservation requirements, or institutional responsibilities for protecting these systems against cyber threats or unauthorized disclosure.

The absence of comprehensive cybersecurity legislation also complicates institutional accountability. Without clearly defined statutory duties governing digital surveillance governance, agencies responsible for operating critical infrastructure may rely primarily upon internal administrative procedures whose legal enforceability remains uncertain. The RIA CCTV controversy therefore exposes not merely an operational deficiency but a broader legislative gap requiring parliamentary intervention.

D. Implications for Critical Infrastructure Protection

The legal and institutional analysis demonstrates that Liberia possesses a relatively robust criminal justice framework for prosecuting serious drug trafficking offences but a comparatively underdeveloped legal regime governing digital surveillance, cybersecurity, and critical infrastructure protection. The RIA case illustrates how deficiencies in surveillance governance may compromise both criminal investigations and broader national security objectives.

Accordingly, effective critical infrastructure protection requires more than physical security measures. It necessitates an integrated legal framework establishing statutory obligations for cybersecurity governance, digital evidence management, surveillance accountability, inter-agency information sharing, and protection of critical national

infrastructure. Such reforms would strengthen prosecutorial effectiveness, enhance institutional accountability, preserve public confidence in the administration of justice, and improve Liberia's capacity to respond to emerging security threats within an increasingly digital environment.

V. THEORETICAL FRAMEWORK (SECURITIZATION THEORY)

This study adopts Securitization Theory to examine how the RIA CCTV footage controversy was framed as a national security concern. Developed by the Copenhagen School, Securitization Theory explains how issues become treated as security threats not only because of their objective characteristics but also because political, institutional, and public actors construct them as threats through discourse and practice (Buzan et al., 1998; Wæver, 1995).

The theory is particularly useful for this study because the national security significance of the RIA controversy does not depend solely on final proof of the footage's authenticity or evidentiary status. Rather, the controversy became significant because the circulation of alleged airport surveillance footage generated public and institutional perceptions of vulnerability within a strategic national asset. In this sense, the case illustrates how perceived weaknesses in surveillance governance, digital evidence protection, and critical infrastructure security can be elevated from an operational concern into a broader national security issue.

The contemporary relevance of Securitization Theory has expanded significantly beyond traditional military and political security concerns. Recent studies demonstrate its growing application in cybersecurity governance, artificial intelligence regulation, and critical infrastructure protection, where digital vulnerabilities are increasingly framed as existential threats to state stability, economic resilience, and public safety (Livingston, 2025; Wagner, 2026). This evolution reflects the growing recognition that modern security environments are characterized by complex interactions between physical and digital systems, making information security an integral component of national security.

A. Infrastructure Vulnerabilities and the Securitization of Risk

One of the most significant contributions of Securitization Theory is its ability to explain how seemingly technical or administrative problems evolve into broader national security concerns. Within conventional security frameworks, issues such as surveillance failures, data leaks, or cybersecurity weaknesses are often treated as operational or managerial deficiencies. Securitization Theory, however, demonstrates how such vulnerabilities can be transformed into matters of national survival, state sovereignty, and institutional legitimacy through political and societal framing (Buzan et al., 1998).

This perspective is particularly relevant in the context of critical infrastructure protection. Recent scholarship highlights the increasing securitization of cyber-physical systems, particularly those associated with transportation, aviation, and logistics networks, due to their susceptibility to cyber intrusions, ransomware attacks, insider threats, credential misuse, surveillance-data exposure, and disruptions to mobility systems (NIST, 2024; OECD, 2024). As critical infrastructures become increasingly dependent on digital technologies, the consequences of information compromise extend beyond technical malfunction to encompass broader concerns regarding public safety, economic continuity, and state resilience.

Contemporary examples illustrate this trend. European airport cyber incidents between 2023 and 2024, including disruptions to passenger-processing and operational systems, were rapidly framed by governments and regulatory institutions as national security challenges rather than mere technical failures (Florido-Benítez, 2024). Likewise, ransomware attacks targeting transport and logistics networks have increasingly been viewed as threats to economic security and supply-chain stability, prompting extraordinary regulatory and policy responses (Bridewell, 2026). In Africa, concerns over the vulnerability of critical transportation and digital infrastructure have similarly become matters of national security. As governments become increasingly dependent on digital systems to manage transportation, communications, and public services, cyber threats are no longer viewed solely as technical challenges but as risks to state resilience, economic stability, and public safety. This concern is reflected in continental instruments

and policy processes such as the African Union Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, and subsequent AU initiatives calling for the development of a Continental Cybersecurity Strategy. However, unlike the Malabo Convention, the precise status, title, and adoption date of any document styled as an "African Union Cybersecurity Strategy and Action Plan" should be verified against official AU policy repositories before being cited as an adopted instrument. Available materials indicate that the AU Commission was directed to expedite development of a Continental Cybersecurity Strategy, rather than clearly confirming adoption of a finalized strategy and action plan. These developments nevertheless demonstrate a growing continental recognition that vulnerabilities affecting essential infrastructure may have far-reaching implications for national security and governance.

B. Applying Securitization Theory to the RIA CCTV Footage Controversy

The relevance of Securitization Theory to this study lies in its capacity to explain how the RIA CCTV footage controversy evolved beyond a discussion of surveillance footage into a broader debate concerning critical infrastructure security, legal governance, and national resilience. Importantly, the analytical value of the theory does not depend on establishing whether the circulated footage was authentic, originated from RIA, or formed part of the official investigation. Rather, the theory focuses on how the controversy was perceived, interpreted, and framed within public and institutional discourse. This perspective is further strengthened by examining the legal and institutional framework governing critical infrastructure protection and digital evidence in Liberia, which provides the doctrinal context within which securitization processes unfold.

From a doctrinal perspective, Liberia's legal framework governing critical infrastructure protection is dispersed across constitutional provisions, criminal legislation, procedural law, and sector-specific regulatory instruments rather than a single comprehensive statute. The Constitution of the Republic of Liberia (1986) establishes the rule of law as the foundation of public administration and obligates the State to safeguard public order,

national security, and the administration of justice. Although the Constitution does not expressly define critical infrastructure, its guarantees relating to public safety and state security provide the constitutional basis for protecting strategic national assets such as RIA. Complementing this constitutional foundation, the Controlled Drugs and Substances Act of 2023 strengthens Liberia's legal response to transnational drug trafficking by expanding investigative powers, imposing stringent penalties for trafficking offences, and recognizing the broader security implications of organized narcotics crime. These statutory provisions demonstrate that the RIA cocaine seizure was not merely a criminal justice matter but one implicating national security and institutional integrity.

The legal framework governing criminal investigations is further established by Liberia's Criminal Procedure Law, which regulates search and seizure, arrest procedures, evidentiary standards, and the admissibility of evidence in criminal proceedings. Of particular relevance to this study is the legal status of electronic evidence. Although Liberia has not enacted a dedicated electronic evidence statute, Chapter 21 of the Criminal Procedure Law provides that questions concerning admissibility are governed by statutory provisions and, where legislation is silent, by the applicable common law of evidence. Consequently, CCTV recordings constitute potentially admissible digital evidence provided that their authenticity, relevance, reliability, and integrity can be established through appropriate evidentiary procedures.

This legal position underscores the importance of maintaining an uninterrupted chain of custody and secure evidence management throughout criminal investigations involving digital surveillance records.

The controversy surrounding the subpoena and subsequent public circulation of CCTV footage therefore raises issues extending beyond investigative confidentiality. It also implicates fundamental evidentiary principles governing digital evidence preservation, authentication, access control, and institutional accountability.

Unauthorized disclosure of surveillance footage may not automatically render such evidence inadmissible; however, it can compromise investigative confidentiality, prejudice pending criminal proceedings, undermine witness protection, and weaken

public confidence in the administration of justice. These legal considerations reinforce the study's broader argument that effective surveillance governance requires not only operational safeguards but also clearly articulated legal standards governing the custody, disclosure, and evidentiary use of digital surveillance materials.

The incident also exposes significant shortcomings within Liberia's broader cybersecurity and information security governance framework. While Liberia's Telecommunications Act of 2007, as amended, regulates aspects of electronic communications and telecommunications services, Liberia presently lacks a comprehensive statutory regime governing cybersecurity, cybercrime, digital surveillance governance, data protection, or the protection of critical information infrastructure.

Consequently, agencies responsible for operating strategic facilities such as Roberts International Airport rely largely upon internal administrative procedures rather than comprehensive statutory obligations regulating cybersecurity, digital evidence preservation, and surveillance governance. This legislative fragmentation creates uncertainty regarding institutional responsibilities, accountability mechanisms, and minimum-security standards for protecting digital surveillance systems against unauthorized access or disclosure.

Against this legal backdrop, the relevance of Securitization Theory becomes particularly evident. From a securitization perspective, the significance of the RIA CCTV footage controversy lies less in the objective authenticity of the footage than in how the incident was perceived and framed as a potential threat to national security. Regardless of whether the footage was authentic, originated from RIA, or was ultimately linked to the cocaine investigation, the widespread public belief that sensitive airport surveillance footage could be accessed and disseminated exposed concerns about critical infrastructure security, surveillance governance, digital evidence protection, and institutional resilience. In accordance with the central assumptions of Securitization Theory, the controversy became significant not necessarily because of what was objectively known about the footage, but because it generated public and institutional perceptions of vulnerability within a strategic national asset and stimulated debate

concerning both the adequacy of existing legal safeguards and the effectiveness of institutional security mechanisms (Buzan et al., 1998; Wæver, 1995).

From this perspective, the circulation of CCTV footage allegedly depicting activities within a restricted airport environment generated concerns regarding the security of surveillance systems, access-control mechanisms, digital evidence management, and information governance structures associated with a strategic national asset. The controversy therefore created conditions under which deficiencies in both the legal framework and institutional governance of critical infrastructure could be interpreted as national security concerns.

Three interrelated securitization dynamics are particularly relevant to this study.

First, the securitizing actors included state security institutions, the Ministry of Justice, the Liberia Drug Enforcement Agency, the Liberia National Police, media organizations, civil society actors, and public commentators, all of whom contributed through official statements, legal processes, media reporting, and public discourse to framing the controversy as a matter of national concern.

Second, the referent object extended beyond the individuals implicated in the alleged drug trafficking operation to encompass the integrity, legal protection, security, and resilience of Liberia's critical infrastructure system, particularly Roberts International Airport as a strategic aviation facility. Within this framework, concerns regarding surveillance-system exposure simultaneously became concerns regarding compliance with legal obligations governing digital evidence and critical infrastructure governance.

Third, existential threat construction occurred when the circulation of the footage was interpreted as evidence whether actual or perceived of weaknesses in airport surveillance systems, evidentiary safeguards, cybersecurity governance, access-control mechanisms, information security protocols, and institutional oversight. Through this process, what might otherwise have remained a technical or administrative issue was transformed into a broader discourse concerning state capacity, the adequacy of Liberia's legal and institutional framework for protecting critical infrastructure, and the resilience of national security governance in the face of evolving transnational threats.

C. Analytical Relevance to the Study

Recent global developments reinforce the usefulness of Securitization Theory for understanding contemporary infrastructure-security challenges. In an increasingly digitized security environment, vulnerabilities affecting critical infrastructure systems, particularly those involving surveillance networks, electronic data, and information-security architecture, are increasingly interpreted not merely as technical failures but as threats to national security and institutional resilience. Cyber incidents affecting aviation infrastructure in Europe, for example, have increasingly been framed as regional security threats requiring coordinated governmental responses (Florido-Benítez, 2024).

Similarly, cybersecurity policy developments in the United States increasingly conceptualize infrastructure data exposure and digital vulnerabilities as national security concerns requiring enhanced regulatory oversight and institutional intervention (Livingston, 2025). The OECD (2024) further observes that breaches involving critical infrastructure data can undermine public confidence in institutions, thereby intensifying securitization processes by transforming technical vulnerabilities into broader concerns regarding state capacity, governance, and public trust.

Applied to the Liberian context, Securitization Theory provides a useful analytical lens for understanding how the RIA CCTV footage controversy developed from an incident involving alleged surveillance exposure into a broader national security discourse concerning critical infrastructure protection, cybersecurity governance, institutional accountability, and state resilience. The theory enables this study to examine how perceived vulnerabilities within a strategic national asset were socially and politically constructed as security concerns rather than treating the incident solely as a question of whether the footage was authentic, legally obtained, or evidentially admissible.

This analytical approach is particularly significant when considered alongside Liberia's existing legal and institutional framework. As discussed in the preceding section, Liberia's governance regime for critical infrastructure protection and digital evidence remains fragmented across constitutional principles, criminal legislation, procedural rules, and sector-specific regulations. While the Controlled Drugs and Substances Act of

2023 provides a strengthened legal basis for addressing transnational drug trafficking, and the Criminal Procedure Law establishes procedural safeguards concerning evidence and criminal investigations, the absence of a comprehensive statutory framework regulating cybersecurity, digital surveillance governance, and critical information infrastructure creates institutional vulnerabilities. These legal gaps provide the conditions through which surveillance-related incidents may become securitized because weaknesses in information governance are interpreted as indicators of broader threats to national security.

From this perspective, the RIA CCTV footage controversy represents not only a question of surveillance management but also a challenge involving legal authority, institutional coordination, evidentiary integrity, and public confidence in state security institutions. The controversy illustrates how the perceived failure to adequately protect sensitive surveillance information can generate demands for exceptional security responses, stronger regulatory controls, and institutional reform. In accordance with Securitization Theory, the significance of the incident therefore lies in the process through which actors—including government institutions, law enforcement agencies, media organizations, and the public constructed surveillance exposure as a matter requiring urgent security attention (Buzan et al., 1998; Wæver, 1995).

Accordingly, Securitization Theory provides this study with a framework for analyzing the intersection of surveillance governance, critical infrastructure protection, digital evidence management, and national security in Liberia's evolving digital environment. By integrating theoretical analysis with the applicable legal and institutional context, the study demonstrates that critical infrastructure security is shaped not only by physical protection measures but also by the adequacy of legal frameworks, institutional practices, and public perceptions of state capacity.

VI. EMPIRICAL ANALYSIS

Guided by Securitization Theory and informed by Liberia’s legal and institutional framework governing critical infrastructure protection, criminal investigations, digital evidence, and surveillance governance, the empirical analysis of the RIA CCTV footage

controversy demonstrates that the significance of the case extends beyond the technical authenticity of the circulated material. Rather, the importance of the controversy lies in how the footage was socially, institutionally, and legally interpreted as a potential indicator of vulnerabilities within a strategic national asset.

The findings reveal that the RIA CCTV footage controversy represented an intersection between national security governance, digital evidence management, cybersecurity challenges, and institutional accountability. While the footage itself became the immediate focus of public attention, the broader implications concerned questions regarding access control, surveillance-system protection, investigative confidentiality, evidentiary integrity, and the adequacy of existing legal and institutional safeguards for protecting critical infrastructure information.

From a securitization perspective, the findings demonstrate that actors including government institutions, law enforcement agencies, media organizations, and members of the public contributed to framing surveillance exposure as a security concern. The controversy transformed what could have been perceived as an administrative or technical failure into a broader national security discussion concerning the resilience of Liberia's critical infrastructure architecture.

The analysis further reveals that the incident exposed significant governance challenges, including fragmented institutional responsibilities, limited regulatory mechanisms for digital surveillance protection, weaknesses in cybersecurity governance, and uncertainties surrounding the management and disclosure of digital evidence. These findings suggest that critical infrastructure protection in Liberia requires not only enhanced technological safeguards but also stronger legal frameworks, institutional coordination mechanisms, and accountability structures.

In furtherance of the study objectives and research questions, the findings are organized around the following themes:

A. Construction of Surveillance Exposure as a Security Concern

The analysis indicates that the circulation of CCTV footage associated with RIA was widely interpreted within public and digital spaces as evidence of possible vulnerabilities

within a strategic national infrastructure asset. Regardless of the absence of verified technical confirmation regarding the authenticity, origin, or chain of custody of the circulated footage, the perception of surveillance exposure itself became securitized because it was framed as indicative of weaknesses in airport surveillance governance, access-control mechanisms, information-security practices, and institutional oversight.

From a legal and institutional perspective, the significance of the controversy extended beyond the content of the footage to questions concerning the governance of digital surveillance information. CCTV recordings generated within critical infrastructure environments may constitute sensitive operational information and, depending on their authentication and relevance, may also become important forms of digital evidence within criminal investigations. Consequently, the perceived unauthorized access and dissemination of such material raised concerns regarding evidence preservation, investigative confidentiality, institutional responsibility, and the adequacy of existing safeguards governing surveillance systems.

This finding aligns with Securitization Theory, which posits that issues become security concerns through processes of social and political construction rather than through objective conditions alone (Buzan et al., 1998; Wæver, 1995). In the RIA case, the controversy became significant not solely because of what the footage objectively demonstrated, but because public discourse interpreted the alleged exposure of airport surveillance systems as evidence of broader vulnerabilities affecting a critical national asset.

The securitization process was reinforced by the institutional context in which the incident occurred. Liberia's existing legal framework provides mechanisms for criminal investigation, evidentiary evaluation, and prosecution of serious offences, including drug trafficking, but lacks a comprehensive statutory regime specifically regulating cybersecurity governance, digital surveillance protection, and critical information infrastructure. As a result, the controversy exposed a perceived gap between the increasing reliance on digital surveillance technologies within critical infrastructure environments and the legal and institutional mechanisms available to protect such systems.

Accordingly, the circulation of the RIA CCTV footage transformed a surveillance-related controversy into a broader national security concern involving infrastructure resilience, cybersecurity governance, digital evidence integrity, and public confidence in state institutions. The finding demonstrates that in contemporary digital security environments, perceived weaknesses in information protection can become securitized when they are interpreted as threats to the state's capacity to safeguard strategic assets and maintain institutional control over sensitive security information.

B. Emergence of Multiple Securitizing Actors

The analysis identified multiple actors that contributed to the framing of the RIA CCTV footage controversy as a national security concern, including state security institutions, law enforcement authorities, media organizations, civil society actors, and online commentators. Rather than emerging from a single authoritative securitizing actor, the process was fragmented and decentralized, with different actors shaping competing interpretations regarding surveillance governance, institutional responsibility, public accountability, and national security risk.

State institutions and security stakeholders contributed to the securitization process by responding to concerns surrounding the alleged narcotics trafficking incident, the integrity of the ongoing investigation, and the protection of sensitive operational information. Their responses reflected broader concerns regarding the preservation of investigative confidentiality, the protection of critical infrastructure assets, and the need to maintain institutional control over information generated within a restricted security environment.

Media platforms and online actors played an equally significant role by transforming the circulation of the CCTV footage into a wider public debate. Through publication, commentary, and digital dissemination, these actors amplified concerns regarding possible weaknesses in airport surveillance governance, access-control procedures, and information-security mechanisms. In doing so, digital platforms became important spaces where questions about institutional competence, legal safeguards, and state capacity were negotiated and contested.

From a socio-legal perspective, the involvement of multiple securitizing actors also influenced public debate regarding the legal status and management of digital information. Discussions surrounding the footage extended beyond the alleged events depicted in the recordings to include questions about who possessed authority to access, disclose, preserve, or rely upon surveillance material potentially relevant to a criminal investigation. Consequently, media narratives and public commentary contributed to broader debates concerning digital evidence integrity, investigative confidentiality, and the adequacy of Liberia's legal framework for governing sensitive surveillance information.

This finding reflects contemporary securitization dynamics in digital environments, where security narratives are increasingly shaped not only by governments and traditional security institutions but also by non-state actors operating through information networks (Wæver, 1995; Buzan et al., 1998; Innes, 2024). In the RIA case, digital media platforms functioned as important securitizing spaces through which perceptions of surveillance vulnerability were constructed, amplified, and connected to broader concerns about critical infrastructure protection and institutional resilience.

Therefore, the emergence of multiple securitizing actors demonstrates that contemporary security governance is no longer exclusively controlled by state institutions. Instead, security meanings are produced through interactions among legal institutions, security agencies, media actors, and the public, making effective critical infrastructure protection dependent not only on technical safeguards but also on transparent, accountable, and legally grounded information governance mechanisms.

C. Referent Object Shift: From Individuals to Critical Infrastructure

A key empirical observation was the shift in the referent object of concern. While initial public discussions focused on individuals allegedly appearing in the footage and their possible involvement in the narcotics investigation, the dominant framing gradually shifted toward the security, integrity, and governance of RIA as a critical national asset. This shift demonstrates classic securitization dynamics, where attention moves from

specific actors or events toward the protection of broader systemic structures considered essential to state security and economic stability.

From a legal and institutional perspective, this shift also redirected attention toward questions of institutional responsibility, surveillance governance, digital evidence protection, and the adequacy of safeguards for sensitive information generated within critical infrastructure environments. The controversy therefore became less about individual conduct alone and more about whether Liberia's legal and institutional mechanisms were sufficient to protect strategic infrastructure, maintain control over surveillance systems, and preserve confidence in national security institutions.

D. Construction of Existential Threat Narratives

The analysis further revealed that the controversy was framed around perceived vulnerabilities in airport surveillance systems, information-security governance structures, access-control and authorization mechanisms, and institutional oversight arrangements. These elements were collectively constructed as indicators of broader institutional weaknesses, suggesting potential exposure of strategic infrastructure to misuse, unauthorized disclosure, or exploitation.

Moreover, from a legal and institutional perspective, these concerns also highlighted questions regarding the protection of digital evidence, accountability for surveillance information management, and the adequacy of existing regulatory safeguards governing critical infrastructure systems. In securitization terms, these narratives contributed to the construction of an existential threat to state capacity and infrastructure resilience, regardless of whether a verified security breach had occurred.

E. Perception-Based Security Implications

A central empirical finding is that the national security implications of the RIA CCTV controversy were driven primarily by perception, institutional interpretation, and public discourse rather than confirmed technical evidence. The widespread belief that surveillance footage from a critical airport could be accessed and publicly disseminated was sufficient to generate concerns regarding institutional vulnerability, information-security governance, and the protection of sensitive operational data. From a legal and

institutional perspective, the controversy also raised critical questions regarding digital evidence integrity, surveillance accountability, and the adequacy of safeguards governing access to and disclosure of security-related information. This supports the theoretical proposition that securitization is fundamentally grounded in audience perception and acceptance of threat narratives rather than the objective verification of the threat itself (Floyd, 2020; Buzan et al., 1998).

F. Institutional Trust and Governance Sensitivities

Finally, the analysis indicates that the controversy contributed to broader concerns regarding institutional trust, governance capacity, and accountability in managing sensitive surveillance infrastructure. Even in the absence of a confirmed system compromise, the perception of possible exposure was sufficient to raise questions about cybersecurity preparedness, inter-agency coordination, oversight effectiveness, and the protection of sensitive digital information.

From a legal and institutional perspective, the controversy also highlighted concerns regarding surveillance governance, digital evidence protection, investigative confidentiality, and the adequacy of regulatory safeguards for critical infrastructure information systems. This finding is consistent with cybersecurity governance literature, which emphasizes that perceived vulnerabilities in critical infrastructure can produce tangible effects on public confidence and institutional legitimacy (OECD, 2024; NIST, 2024).

The release of the CCTV footage reinforced public demands for greater transparency and accountability in the investigation. Many citizens argued that public disclosure was necessary to verify official accounts amid longstanding concerns about corruption and impunity in Liberia's criminal justice system (FrontPage Africa, 2026). Such reactions are consistent with research demonstrating that transparency enhances public confidence in government institutions when citizens perceive official communication as inadequate (Grimmelikhuijsen & Meijer, 2014).

In summation, the empirical analysis demonstrates that the RIA CCTV footage controversy functioned primarily as a discursive security event, where meaning,

perception, and institutional interpretation played a more decisive role than technical verification. Through securitization processes, the issue was transformed into a broader national security concern centered on critical infrastructure vulnerability, legal accountability, institutional trust, and surveillance governance.

VII. DISCUSSION

A. Interpretation of Findings in Relation to Research Questions

The findings of this study indicate that the US$19.2 million cocaine seizure at RIA evolved beyond a routine law enforcement incident into a broader matter involving national security discourse, legal governance, and institutional accountability.

In relation to the first research question concerning the relationship between critical infrastructure vulnerabilities and transnational drug trafficking, the evidence suggests that Liberia's principal international aviation gateway exhibits structural and operational vulnerabilities consistent with broader patterns of illicit trafficking affecting West African transportation networks (UNODC, 2026). The interception of a significant cocaine shipment highlights not only the activities of transnational criminal networks but also the importance of effective legal, institutional, and security frameworks for protecting strategic infrastructure.

Regarding the second research question on surveillance systems and airport security governance, the emergence and circulation of CCTV-related materials revealed tensions between evidence control, investigative confidentiality, transparency, and institutional accountability. While surveillance systems are designed to strengthen security operations, the controversy demonstrates that such technologies also require effective legal safeguards governing access, preservation, disclosure, and use of digital information.

The third research question, focusing on the implications of the CCTV controversy for digital evidence integrity, cybersecurity governance, and institutional legitimacy, is reflected in the heightened public and media attention surrounding the case. Although this study did not measure public opinion directly, the discourse surrounding the incident suggests increased scrutiny of surveillance governance practices, institutional

coordination, and the capacity of security institutions to protect sensitive operational information.

Overall, the findings demonstrate that the RIA controversy represents the intersection of national security, legal governance, and critical infrastructure protection. The incident illustrates that vulnerabilities within surveillance and information-security systems may generate broader security concerns when existing legal and institutional mechanisms are perceived as insufficient to ensure accountability, protect digital evidence, and maintain public trust.

B. Theoretical Interpretation: Securitization Framework

Drawing on the securitization theory advanced by Buzan et al. (1998), the RIA cocaine seizure can be interpreted as a process through which a law enforcement matter was reframed into a broader national security concern. The involvement of the National Joint Security under the National Security Council demonstrates a shift from a conventional criminal justice response toward a securitized policy domain, where drug trafficking was constructed not merely as an offence but as a potential threat to national stability, institutional integrity, and border sovereignty.

From a legal and institutional perspective, this securitization process also reflects the interaction between criminal justice mechanisms, security governance structures, and critical infrastructure protection responsibilities. While the Controlled Drugs and Substances Act of 2023 and related criminal procedures provide the legal basis for addressing narcotics offences, the elevation of the incident to a national security matter demonstrates how certain threats require coordination beyond ordinary law enforcement responses.

Furthermore, the circulation of CCTV-related materials can be understood through securitization logic. Surveillance footage, ordinarily functioning as administrative records or potential digital evidence within investigative processes, became re-signified as a security-sensitive asset whose unauthorized disclosure was perceived as a potential threat to institutional authority, investigative confidentiality, and operational security.

Thus, the RIA controversy illustrates how securitization extends beyond the original criminal event to encompass vulnerabilities in information governance, surveillance protection, and institutional resilience. The case demonstrates that in contemporary security environments, the protection of critical infrastructure depends not only on preventing physical threats but also on maintaining legal safeguards, cybersecurity controls, and institutional capacity to manage sensitive digital information.

C. Surveillance Governance and Critical Infrastructure Security

The findings further align with critical infrastructure security literature, which emphasizes that surveillance systems are dual-use technologies that simultaneously support security enforcement and create new vulnerabilities when inadequately governed (Sedrati, 2026). In the RIA case, CCTV systems functioned both as investigative resources and as the subject of institutional controversy, illustrating the complex challenges associated with surveillance governance in high-risk environments.

From a legal and institutional perspective, the findings demonstrate that weaknesses in surveillance governance, including unauthorized dissemination, unclear custodial responsibility, inadequate access controls, or fragmented institutional oversight, may affect not only security operations but also the integrity of digital evidence and public confidence in investigative processes. The controversy highlights the importance of clear legal frameworks governing the collection, preservation, disclosure, and use of surveillance information within critical infrastructure settings.

This finding aligns with cybersecurity and critical infrastructure scholarship, which argues that exposure of sensitive information can be as consequential as physical breaches because it may compromise confidentiality, operational resilience, and institutional trust (Cybersecurity and Infrastructure Security Agency [CISA], 2024; European Union Agency for Cybersecurity [ENISA], 2024; National Institute of Standards and Technology [NIST], 2024; Trump et al., 2025). Therefore, effective surveillance governance requires not only technological safeguards but also enforceable legal standards, institutional accountability mechanisms, and coordinated cybersecurity practices.

 (ISSN: 2583-7753)

D. Institutional Coordination and National Security Response

A key finding is the centrality of multi-agency coordination in responding to the cocaine seizure at RIA. The activation of the National Joint Security apparatus reflects institutional recognition that drug trafficking within a strategic aviation facility constitutes a cross-sectoral security threat requiring coordinated responses among law enforcement, intelligence, customs, and other relevant oversight institutions.

From a legal and institutional perspective, the study further reveals that effective coordination requires not only operational collaboration but also clear mechanisms for information governance, evidence management, and institutional accountability. The parallel existence of judicial proceedings, investigative activities, and media reporting demonstrates the complexity of managing sensitive information within a critical infrastructure environment where transparency must be balanced with investigative confidentiality and evidentiary integrity.

However, the analysis identifies coordination challenges, particularly concerning information management, communication control, and custodial responsibility for surveillance materials. Fragmented authority over security information may create uncertainty regarding access, disclosure, and protection of digital evidence, thereby increasing perceptions of institutional vulnerability. Strengthening inter-agency coordination, supported by clear legal protocols and cybersecurity governance standards, is therefore essential for enhancing Liberia's critical infrastructure resilience and national security response capacity.

E. Framing the Problem: Lessons from the RIA CCTV Footage Incident

The RIA controversy illustrates how criminal investigations involving strategic infrastructure may quickly evolve into broader debates concerning national security, digital evidence integrity, surveillance governance, and institutional accountability. These findings provide the basis for the policy-oriented suggestions and recommendations set out below. The incident demonstrates that contemporary threats to critical infrastructure extend beyond physical sabotage, trafficking operations, or unauthorized access to include data exposure, surveillance governance failures,

weaknesses in digital evidence management, and fragmented institutional control over sensitive security information.

From a securitization perspective, the case illustrates how a criminal incident can rapidly evolve into a national security concern when surveillance data, institutional credibility, legal accountability, and public trust become contested (Buzan et al., 1998). The controversy demonstrates that protecting critical infrastructure requires more than operational security measures; it also requires effective legal frameworks, cybersecurity standards, clear institutional responsibilities, and safeguards governing the management and disclosure of digital information.

Accordingly, the RIA incident underscores the need for reforms that integrate physical infrastructure protection with digital surveillance governance, evidence protection mechanisms, and institutional accountability structures. Against this background, strengthening Liberia's national security architecture requires attention to the following legal, institutional, and policy recommendations:

VIII. ESTABLISHING A NATIONAL CRITICAL INFRASTRUCTURE PROTECTION FRAMEWORK

The protection of critical infrastructure in the digital age requires more than isolated cybersecurity legislation; it requires an integrated national framework that identifies strategic assets, establishes protection standards, coordinates institutional responsibilities, and creates mechanisms for continuous risk assessment and resilience building. While Liberia has historically lacked a comprehensive standalone Critical Infrastructure Protection (CIP) framework comparable to those established in advanced cybersecurity governance systems, recent legislative developments demonstrate significant progress toward strengthening the country's digital security architecture.

Most notably, Liberia's Cybercrime Act of 2025, if signed into law and brought into force, would represent an important advancement in the country's cybersecurity governance framework. Available reporting indicates that the bill was passed by the Legislature and cleared for forwarding to President Joseph Nyuma Boakai for signature; however, in the absence of confirmed presidential assent and an effective date, it should not be treated as

operative legislation. The bill reportedly contains mechanisms relevant to the protection of Critical National Information Infrastructure (CNII), including authority to designate computer systems, networks, and information infrastructure considered vital to national security or socioeconomic wellbeing.

It also appears to contemplate broader cybersecurity governance measures, including institutional coordination, cyber-incident obligations, and provisions relevant to digital evidence preservation. These proposed provisions are particularly relevant to the RIA CCTV footage controversy because they indicate an emerging legal foundation for addressing digital evidence integrity, information security, and protection of sensitive infrastructure data, while also demonstrating that Liberia's cybersecurity framework remains incomplete until the bill's legal status is formally confirmed.

However, even if the Cybercrime Act of 2025 receives presidential assent and becomes operative, it would not by itself constitute a complete national Critical Infrastructure Protection framework. A comprehensive CIP regime requires a broader whole-of-government approach that extends beyond cybercrime prevention to include the identification and classification of critical sectors, mandatory security standards, risk-management obligations, public-private coordination mechanisms, and sector-specific resilience strategies. Liberia's National Cyber Security Strategy similarly recognizes the need to strengthen cybersecurity governance, protect national information infrastructure, establish operational cybersecurity capabilities, and develop supporting legal and regulatory frameworks.

Across Africa, several states have developed partial CIP-related governance models through cybersecurity strategies, critical infrastructure regulations, and national security frameworks. South Africa, for example, has developed cybersecurity governance mechanisms aimed at coordinating responses to threats affecting essential services and national infrastructure. Nigeria's cybersecurity framework, anchored in the Cybercrimes Act and National Cybersecurity Policy and Strategy, provides an emerging institutional basis for protecting critical digital infrastructure, although implementation and coordination challenges remain (Falade & Osho, 2025). At the regional level, the African Union has promoted harmonized cybersecurity governance through instruments such as

the Malabo Convention and related digital transformation initiatives aimed at strengthening resilience against cyber-enabled threats (Ifeanyi-Ajufo, 2024).

Liberia's current approach should therefore be characterized as an emerging cybersecurity and critical information infrastructure governance system rather than a fully mature national CIP regime. Pending confirmation of the Cybercrime Act's presidential assent and effective date, the Act should be discussed as a proposed or pending legal instrument rather than as an established source of binding obligations. Existing and proposed legal developments provide important foundations, but additional institutional and policy measures are required to translate these foundations into a comprehensive protection architecture. In particular, Liberia requires a coordinated CIP framework that clearly identifies strategic assets such as RIA, seaports, telecommunications networks, and border facilities as critical national infrastructure requiring tailored protection measures.

The RIA CCTV footage controversy demonstrates why such a framework is necessary. Airports are dual-risk environments: they function as gateways for legitimate international movement while simultaneously serving as potential targets for transnational criminal networks and repositories of sensitive operational information. A comprehensive CIP framework would establish minimum cybersecurity and surveillance governance standards, clarify institutional responsibilities for protecting digital assets, require periodic risk assessments, and strengthen coordination between airport authorities, security agencies, cybersecurity institutions, and private-sector operators.

Accordingly, the policy objective should not be the creation of an entirely new regulatory system but rather the consolidation and operationalization of Liberia's emerging cybersecurity architecture into a broader national Critical Infrastructure Protection framework. Such an approach would enable Liberia to transition from reactive responses to security incidents toward proactive infrastructure resilience, ensuring that strategic national assets are protected against both physical and digital threats.

A. Establishment of a National Surveillance Governance and CCTV Custodial Framework

The RIA CCTV controversy demonstrates that surveillance systems, while designed to strengthen security monitoring and investigative capacity, can themselves become sources of institutional vulnerability when governance mechanisms are inadequate. Instead of enhancing public confidence, poorly regulated surveillance information can undermine institutional legitimacy, compromise operational confidentiality, and raise concerns regarding accountability for sensitive security data.

The circulation and contested handling of CCTV footage associated with RIA exposed the need for a more comprehensive national surveillance governance framework that clearly defines the ownership, custody, access, retention, disclosure, and protection requirements applicable to surveillance data generated within critical infrastructure environments. Such a framework should establish standardized procedures for the management of CCTV evidence, including clear chain-of-custody requirements, authorized access protocols, audit mechanisms, secure digital storage systems, and accountability measures for misuse or unauthorized disclosure.

Liberia's existing legal framework provides partial foundations for addressing aspects of information governance. The Freedom of Information Act of 2010 establishes limitations on public access to certain categories of information, including criminal investigation records, personal information, and privileged communications. However, these provisions primarily regulate disclosure obligations of public authorities and exemptions from information requests; they do not establish a comprehensive regime governing the unauthorized dissemination of surveillance footage or the custodial responsibilities of institutions managing sensitive digital surveillance data.

Recent developments under Liberia's Cybercrime Act of 2025 provide additional legal support for protecting digital information systems by addressing cyber-related offences, electronic evidence management, and protection of critical information infrastructure. However, cybersecurity legislation alone does not fully address the operational realities of surveillance governance within airports and other critical infrastructure environments.

Specific regulatory measures are therefore required to establish institutional responsibilities for CCTV management, define lawful access and disclosure procedures, and create accountability mechanisms for unauthorized handling of surveillance materials.

Accordingly, Liberia should develop a national surveillance governance and CCTV custodial framework that complements existing cybersecurity legislation by addressing the unique security, legal, and evidentiary challenges associated with surveillance systems. Such a framework would strengthen digital evidence integrity, protect investigative confidentiality, enhance institutional accountability, and improve public confidence in the management of surveillance technologies within strategic national assets.

B. Cybersecurity Integration into Physical Infrastructure Security

In the digital age, surveillance systems are no longer passive tools; they are networked cyber-physical systems vulnerable to hacking, leakage, or misuse (Amin et al., 2024; CISA, 2024; OECD, 2024). The CCTV controversy highlights that information exposure can be as damaging as physical breaches, especially when sensitive security footage enters uncontrolled digital spaces. Therefore, it is imperative to consider or prioritize the encryption of all CCTV and surveillance data streams, secure cloud or hybrid storage systems, and periodic cybersecurity audits of airport systems.

IX. SUGGESTIONS AND RECOMMENDATIONS

The RIA CCTV footage controversy demonstrates the need for a more coherent legal, institutional, and cybersecurity framework for protecting Liberia's critical infrastructure in the digital age. The following recommendations synthesize the policy reforms arising from the study's findings.

1. First, Liberia should establish a comprehensive National Critical Infrastructure Protection framework that clearly identifies strategic assets such as Roberts International Airport, seaports, telecommunications networks, border facilities, and other essential systems as critical national infrastructure. Such a framework

should define institutional responsibilities, establish sector-specific protection standards, require periodic risk assessments, and promote coordinated public-private security governance.

2. Second, Liberia should develop a dedicated surveillance governance and CCTV custodial framework for critical infrastructure environments. This framework should regulate access to surveillance footage, custody and preservation of digital recordings, authorized disclosure procedures, audit trails, evidentiary handling, and accountability for unauthorized release. Such safeguards are necessary to preserve investigative confidentiality, protect digital evidence integrity, and maintain public confidence in security institutions.
3. Third, cybersecurity governance should be integrated into physical infrastructure security planning. Airport security should no longer be treated solely as a matter of perimeter control, personnel screening, or cargo inspection. It must also include protection of digital surveillance systems, access-control technologies, cargo information systems, communication networks, and other cyber-physical assets that support airport operations.
4. Fourth, Liberia should strengthen inter-agency coordination among the Liberia Airport Authority, Liberia Drug Enforcement Agency, Liberia National Police, customs authorities, immigration authorities, intelligence institutions, prosecutors, and relevant private-sector operators. Clear protocols should govern information sharing, evidence handling, incident reporting, and public communication during investigations involving critical infrastructure.

5. Finally, the legal status of pending or recently proposed cybersecurity legislation, including the Cybercrime Act of 2025, should be verified before final submission. If the instrument has not received presidential assent and an effective commencement date, it should be discussed as pending legislation rather than operative law. This clarification is necessary because cybersecurity legislation is central to the manuscript's recommendations on critical information infrastructure protection.

X. CONCLUSION

The RIA cocaine seizure and subsequent CCTV footage controversy demonstrate that vulnerabilities affecting Liberia's critical infrastructure are no longer limited to operational or physical security challenges but increasingly involve institutional, legal, informational, and digital dimensions. The incident illustrates how weaknesses in surveillance governance, information management, and institutional coordination can generate broader national security concerns when sensitive security-related information becomes exposed or contested.

The analysis further demonstrates that Liberia's legal and institutional architecture for managing digital security threats is evolving. Recent legislative developments, particularly the Cybercrime Act of 2025, provide important foundations for cybersecurity governance, protection of critical information infrastructure, and the management of digital evidence. However, the RIA case reveals that effective critical infrastructure protection requires more than isolated legal provisions; it requires the integration of cybersecurity legislation, sector-specific protection standards, surveillance governance mechanisms, institutional accountability frameworks, and coordinated national security practices.

Through the lens of Securitization Theory (Buzan et al., 1998), the case illustrates how infrastructure-related incidents can rapidly develop into national security concerns when surveillance systems, legal governance structures, institutional credibility, and public information flows intersect. The controversy demonstrates that perceived vulnerabilities may produce significant security consequences even where technical confirmation of a breach remains uncertain, because public trust and institutional legitimacy are central components of contemporary security governance.

Ultimately, strengthening Liberia's critical infrastructure resilience requires a transition from reactive incident management toward proactive risk governance. This involves operationalizing existing cybersecurity and digital evidence frameworks, developing a comprehensive critical infrastructure protection strategy, establishing effective surveillance governance standards, and enhancing coordination among security

institutions, regulatory authorities, and infrastructure operators. Such measures are essential for ensuring that strategic national assets, including RIA, remain resilient against both physical and digital threats in an increasingly interconnected security environment.

XI. REFERENCES

1. Amod Agarkar, A., Karyakarte, M., Kulkarni, R. V., Bag, V., Abhang, S. P., & Sule, B. (2025). Assessing the impact of user behavior and insider threats on critical infrastructure. Information Security Journal: A Global Perspective, 1–12. https://doi.org/10.1080/19393555.2025.2502553
2. Amin, R., et al. (2024). Security modelling for cyber-physical systems: A systematic literature review. arXiv. https://doi.org/10.48550/arXiv.2404.07527
3. Amod Agarkar, A., et al. (2025). Insider threats and critical infrastructure security. Information Security Journal. https://doi.org/10.1080/19393555.2025.2502553
4. African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union Commission.
5. African Union. (2024). African Union cybersecurity strategy and action plan. African Union Commission.
6. Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management, 15(1), 50–59.
7. Bridewell. (2026). Cybersecurity in critical national infrastructure organisations report. https://www.bridewell.com
8. Balzacq, T., Léonard, S., & Ruzicka, J. (2016). Securitization revisited: Theory and cases. International Relations, 30(4), 494–513.
9. Bridewell. (2026). Critical national infrastructure cybersecurity report. https://www.bridewell.com
10. Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

11. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.
12. Cybersecurity and Infrastructure Security Agency. (2024). Cross-sector cybersecurity performance goals for critical infrastructure. https://www.cisa.gov
13. Council of Europe. (2024). Cybercrime country profile: Liberia. https://www.coe.int
14. European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. https://www.enisa.europa.eu
15. Florido-Benítez, L. (2024). Identifying and classifying cyberattacks on airports. Cyber Security: A Peer-Reviewed Journal, 8(1), 63–79. https://doi.org/10.69554/TWHW5595
16. Floyd, R. (2020). The morality of security: A theory of securitization. Cambridge University Press.
17. Ferguson, D. D. S. (2023). The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. International Cybersecurity Law Review. 4, 371–386. https://doi.org/10.1365/s43439-023-00097-8
18. Fonseca, R.S. (2026). South Africa's national security strategy and cyber statecraft https://doi.org/10.3389/fpos.2026.1749367
19. Falade, P.V. & Osho, O. (2025). Nigeria's Digital Sovereignty: Analysis of Cybersecurity Legislation, Policies, and Strategies https://doi.org/10.48550/arXiv.2601.06050
20. FrontPage Africa. (2026). Liberia: Questions mount over leaked CCTV footage in US$19.2 million cocaine investigation.
21. Grimmelikhuijsen, S., & Meijer, A. (2014). Effects of transparency on the perceived trustworthiness of a government organization: Evidence from an online experiment. Journal of Public Administration Research and Theory, 24(1), 137–157.
22. International Civil Aviation Organization. (2022). Global aviation security plan (GASeP). ICAO.
23. International Telecommunication Union. (2026). Cybersecurity and critical infrastructure protection in developing states. https://www.itu.int

24. Innes, A. (2024). Un-siloing securitization: an intersectional intervention https://doi.org/10.1057/s41311-024-00584-7
25. KOACI. (2026). Liberia: Seizure of 237 kg of cocaine worth over $19 million at RIA under investigation. https://www.koaci.com
26. KMTV News. (2026). Court orders RIA to produce CCTV footage in US$19.2 million cocaine case. https://mykmtvnews.com
27. Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies.
28. Livingston, M. (2025). AI vulnerability, national security, and securitization of critical systems. SSRN Working Paper. https://ssrn.com/abstract=5010934
29. Liberia Drug Enforcement Agency. (2026). Press release: LDEA addresses public concerns regarding major RIA cocaine investigation. https://ldea.gov.lr
30. Liberia Drug Enforcement Agency (2026). LDEA Addresses Public Concerns Regarding Disclosure of Suspects in Major RIA Cocaine Investigation https://www.ldea.gov.lr/news.php?id=30
31. Nott, C. (2025). Organizational adaptation to generative AI in cybersecurity. arXiv. https://arxiv.org/abs/2506.12060
32. Ifeanyi-Ajufo, N. (2024). The AU took important action on cybersecurity at its 2024 summit – but more is needed https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed?
33. National Institute of Standards and Technology. (2023). Guide to operational technology (OT) security. https://www.nist.gov
34. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://www.nist.gov
35. National Institute of Standards and Technology. (2024). Fiscal year 2023 cybersecurity and privacy annual report (SP 800-229). https://doi.org/10.6028/NIST.SP.800-229
36. Organisation for Economic Co-operation and Development. (2024). OECD framework for the classification of AI systems and AI governance. OECD Publishing. https://www.oecd.org

37. Paulraj, J., et al. (2025). Autonomous AI-based cybersecurity framework for critical infrastructure. arXiv. https://arxiv.org/abs/2507.07416
38. Rüffin, N. (2026). Research security and securitization under geopolitical pressure. Global Policy. https://doi.org/10.1111/1758-5899.70103
39. Republic of Liberia. (1972). Criminal Procedure Law (Title 2, Liberian Code of Laws Revised). Government of Liberia.
40. Republic of Liberia. (1986). Constitution of the Republic of Liberia.
41. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to
42. Republic of Liberia. (2007). Telecommunications Act of 2007. Government of Liberia. (as amended).
43. Republic of Liberia. (2023). Controlled Drugs and Substances Act of 2023
44. know. Oxford University Press.
45. Swire, P., et al. (2024). Risks to cybersecurity from data localization. Journal of Cyber Policy, 9(1), 1–27. https://doi.org/10.1080/23738871.2024.2384724
46. Swire, P., Kennedy-Mayo, D., Bagley, D., Modak, A., Krasser, S., & Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. Journal of Cyber Policy, 9(1), 1–27. https://doi.org/10.1080/23738871.2024.2384724
47. Sedrati, A. (2026). Unconsented sensing: A sociotechnical governance framework for 6G ISAC. arXiv. https://arxiv.org/abs/2605.07328
48. Thistlethwaite, J., & Henstra, D. (2026). Policy instruments to strengthen the cybersecurity of critical infrastructure. Journal of Cyber Policy, 1 https://doi.org/10.1080/23738871.2026.2648977
49. Trump, B. Det al. (2025). Threat-Agnostic Resilience: Framing and Application for Critical Infrastructure. https://doi.org/10.48550/arXiv.2501.01318
50. U.S. Cybersecurity and Infrastructure Security Agency. (2024). Advisory on AVTECH IP camera vulnerability (CVE-2024-7029). CISA. https://www.cisa.gov
51. United Nations Office on Drugs and Crime (UNODC). (2020). Handbook on digital evidence.

52. United Nations Office on Drugs and Crime (UNODC). (2023). World drug report 2023.
53. Verity News. (2026). $19.2M cocaine case widens as LDEA confirms joint security investigation. https://verityonlinenews.com
54. Verity Online News's Post. (2026). Breaking News (Read Episode #3 Documentary Evidence) https://www.facebook.com/61558522477978/posts/122257740230284082/?rdid=J7FsEt5hiUHzxUeA
55. Verity News. (2026). BREAKING: Liberian activist Martin K. N. Kollie has released what he describes as Episode 2 of his ongoing investigation into the reported US$19.2 million https://www.facebook.com/reel/1185706993685560
56. Van Rythoven, E. (2024). Audience acceptance in securitization processes: Revisiting theory. Security Dialogue, 55(2), 120–137.
57. Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity landscape. Routledge.
58. Watson, E. (2026). US$19.2M Cocaine Shipment Busted at RIA https://www.liberianobserver.com/news/us-19-2m-cocaine-shipment-busted-at-ria/article_02d8e17d-a137-4a08-a2c0-64dde2f03dd0.html
59. Wagner, C. (2026). The securitization of science: Policy and measurement systems. arXiv. https://arxiv.org/abs/2605.20313
60. Wæver, O. (1995). Securitization and desecuritization. In R. Lipschutz (Ed.), On security. Columbia University Press.
61. Yaste, D. (2026). LDEA Says RIA Cocaine Case Now Targets Global Criminal Syndicates https://www.liberianobserver.com/news/ldea-says-ria-cocaine-case-now-targets-global-criminal-syndicates/article_d9c7c96c-1408-4efe-a4bf-b8ac3eb6e557.html
62. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.