

## Cybersecurity Intelligence and Border Supply Chain Security: An Investigation into the Operations of the Nigeria Customs Service

<sup>1</sup>Mustapha, A. Jauro, <sup>2</sup>I. R. Saidu, <sup>3</sup>M. Ibrahim & <sup>4</sup>M. Isah

<sup>1,2,3&4</sup>Department of Intelligence and Cyber Security,  
Faculty of Military Science and Interdisciplinary Studies  
Nigerian Defence Academy Kaduna

Article DOI: 10.48028/iiprds/ijaraebp.v9.i1.18

### Abstract

The rapid digitalization of global trade has uncovered supply chains and border management systems to increasing cybersecurity threats, making cyber intelligence a critical component of national security. This study investigates the role of cybersecurity intelligence in enhancing border supply chain security within the operations of the Nigeria Customs Service (NCS). The research examines how cyber-enabled threats such as data breaches, smuggling through digital manipulation, cyber-fraud, and unauthorized system access—affect customs operations and undermine the integrity of Nigeria's border supply chains. Using a mixed-method approach involving document analysis, expert interviews, and operational assessments, the study evaluates the extent to which the NCS integrates cybersecurity intelligence into risk management, cargo profiling, surveillance, and interdiction processes. Findings indicate that although the NCS has adopted digital tools such as the Nigeria Integrated Customs Information System (NICIS II), significant gaps exist in cyber-awareness, intelligence sharing, personnel training, and technological resilience. The study concludes that strengthening cybersecurity intelligence capabilities is essential for securing Nigeria's border supply chain, improving trade facilitation, and supporting national security objectives. It recommends enhanced inter-agency cooperation, advanced digital forensics, continuous staff training, and the establishment of a unified cybersecurity intelligence framework within the NCS.

**Keywords:** *Science, Technology, Threats, National Security, & Digital Investigation*

Corresponding Author: Mustapha, A. Jauro

### **Background of the Study**

Globalized digital economy, cybersecurity intelligence has become a critical component of national and organizational security. The increasing dependence on information and communication technology (ICT) for trade facilitation, customs administration, and supply chain operations exposes institutions to a wide range of cyber threats. Supply chain systems especially those linked to cross-border trade rely heavily on digital platforms for documentation, clearance, and logistics coordination. As a result, the integrity, confidentiality, and availability of information within these systems are essential to national security, economic stability, and public trust. (Natasa, 2024).

The Nigeria Customs Service (NCS), as the primary agency responsible for regulating international trade, revenue collection, and border protection, plays a pivotal role in ensuring supply chain security. However, the digitization of customs processes such as the Nigeria Integrated Customs Information System (NICIS II), electronic single window platforms, and online payment gateways has introduced new vulnerabilities. Cybercriminals increasingly target these systems to commit fraud, smuggle prohibited goods, manipulate trade data, or disrupt logistics networks. Therefore, the integration of cybersecurity intelligence into supply chain management is not only a technological necessity but also a strategic national imperative.

Cybersecurity intelligence involves the systematic collection, analysis, and application of information about potential or actual cyber threats that could compromise digital infrastructure. In the context of customs and supply chains, it helps detect, prevent, and respond to cyber incidents that may affect the flow of goods, data, and revenue. The ability of the Nigeria Customs Service to anticipate and neutralize cyber threats is thus essential for maintaining transparency, trade facilitation, and national security. (Odogo, 2024).

Cybersecurity intelligence plays an integral role in securing various sectors of national and international operations, particularly in countries like Nigeria. The rapid adoption of digital technologies in the global supply chain has given rise to an increase in cyber threats. These threats compromise the security of businesses, logistics systems, and ultimately national security. The Nigeria Customs Service (NCS) plays a central role in safeguarding the country's borders, ensuring the smooth movement of goods, and monitoring imports and exports. As global supply chains become increasingly digitalized, cybersecurity intelligence has emerged as a pivotal component of border security and trade facilitation. According to Olukayode et al., (2018), the integration of cybersecurity into the operational activities of Nigeria's customs system is critical in addressing challenges related to cross-border trade, customs duties, and illegal activities at the nation's borders. Furthermore, the NCS's implementation of advanced intelligence systems can significantly reduce vulnerabilities in both the physical and digital aspects of supply chain security (Olukayode et al., 2018).

The growing sophistication of cyber threats requires a multi-faceted approach, combining technology, intelligence gathering, and strategic communication. As Naab and Oroleye (2024) argue, mitigating security risks in global supply chains demands a comprehensive strategy that

includes communication efforts and criminological approaches. The involvement of customs services in this process is essential, as they are directly responsible for monitoring goods entering and leaving the country. By integrating strategic communication and cyber intelligence systems, the NCS can better address the growing challenges posed by illicit trade, cybercrime, and illegal imports. This approach not only bolsters national security but also enhances the efficiency of customs operations, ensuring that only legitimate goods pass through the borders while preventing the flow of contraband (Naab & Oroleye, 2024).

Cybercrime investigation and prosecution are central to Nigeria's efforts to curb cyber threats and secure national infrastructure, including supply chains. Ishiguzo (2024) discusses the prospects of cybercrime investigations in Nigeria and the critical role of intelligence agencies, such as the NCS, in this effort. The incorporation of cybersecurity intelligence within the NCS framework allows for a more comprehensive approach to cybercrime investigation, facilitating real-time monitoring and proactive measures to counter cyber threats. The use of intelligence-gathering techniques, such as data analysis and threat monitoring, is essential in identifying and neutralizing cybercriminals before they can exploit vulnerabilities in Nigeria's supply chain systems. This proactive stance is crucial for maintaining the integrity of both the digital and physical aspects of border security (Ishiguzo, 2024).

Artificial intelligence (AI) has revolutionized various sectors, including customs and border security. According to Odongo (2024), AI integration in tax and customs systems has had a profound impact on the efficiency and security of border operations across Africa. For Nigeria, the integration of AI into the NCS operations could significantly improve the detection of fraudulent activities, smuggling, and tax evasion, all of which are major concerns in global supply chains. By using AI to analyze large volumes of data and predict potential threats, the NCS can enhance its cybersecurity intelligence capabilities and secure the nation's borders more effectively. This technology not only aids in combating cyber threats but also supports the broader goals of trade facilitation and economic growth (Odongo, 2024).

The security of Nigeria's national borders is a shared responsibility between various agencies, including the NCS, which plays a critical role in ensuring that the nation's borders remain secure and trade flows smoothly. As Olowonihi and Musa (2024) assert, intelligence gathering is an essential component of Nigeria's national security strategy. The NCS, as a key player in this strategy, must continuously adapt to the evolving cybersecurity landscape by enhancing its intelligence capabilities. This includes the use of advanced technologies, such as AI, big data analytics, and threat intelligence systems, which can aid in detecting and preventing cyber-attacks that could compromise the country's security. The implementation of a robust cybersecurity intelligence framework within the NCS will help mitigate the risks posed by cyber threats to national security and supply chain operations (Olowonihi & Musa, 2024).

### **Statement of the Problem**

The increasing digitization of trade and customs operations in Nigeria has made the Nigeria Customs Service highly dependent on technology-driven platforms for managing supply chains. While these digital systems have enhanced efficiency, they have also exposed the

Service to growing cybersecurity risks. Instances of data breaches, hacking of trade portals, manipulation of electronic manifests, and ransomware attacks on logistics systems have been reported in various customs and border operations globally and Nigeria is not immune to these threats. (Okoli, 2024). A major problem is the limited integration of cybersecurity intelligence into the operational and strategic framework of the Nigeria Customs Service. Many customs personnel lack advanced training in cyber threat analysis, and existing ICT units often focus on system maintenance rather than proactive cyber defense. Furthermore, collaboration between NCS and national intelligence or security agencies on cyber-related matters remains weak, resulting in delayed responses to emerging threats.

The increasing reliance on digital technologies in the global supply chain has exposed several vulnerabilities, especially in developing countries like Nigeria. These vulnerabilities are exacerbated by the rising sophistication of cyber-attacks targeting critical infrastructure, including customs systems. Despite the NCS playing a vital role in securing the nation's borders, trade operations, and economic activities, the agency faces significant challenges in combating the growing threats posed by cybercriminals. While the NCS has made strides in integrating intelligence systems into its operations, the lack of comprehensive cybersecurity intelligence frameworks remains a major concern. This gap exposes the country's customs systems to cyber-attacks that can disrupt supply chain security, hinder trade facilitation, and jeopardize national security (Olukayode, Folasade, & David, 2018).

Furthermore, the absence of a comprehensive strategy that integrates cybersecurity intelligence with customs operations has allowed illicit trade and smuggling activities to thrive within Nigeria's borders. As Adepoju (2024) highlights, the global supply chain is increasingly vulnerable to cyber-attacks that exploit the weaknesses in the systems used by customs agencies. In Nigeria, this problem is exacerbated by the country's reliance on outdated digital infrastructure, which makes it challenging to detect and prevent cyber threats in real time. Without the integration of advanced cybersecurity intelligence systems into the NCS's operations, Nigeria risks further exposure to cyber threats, undermining the nation's ability to secure its borders, protect customs data, and maintain a smooth flow of goods across its borders (Adepoju, 2024). Therefore, the main objective of this study is to examine the relationship between cybersecurity intelligence and supply chain security in the Nigeria Customs Service.

## **Literature Review/Theoretical Framework**

### **Concept of Cybersecurity Intelligence**

Cybersecurity intelligence refers to the systematic process of collecting, analyzing, and applying information about potential or existing cyber threats to protect digital assets and infrastructure. According to Buzan (2018), cybersecurity intelligence integrates data from multiple sources technical systems, human networks, and open-source information—to predict, detect, and mitigate cyberattacks before they occur. It focuses on proactive defense through threat analysis, intrusion detection, and incident response. In government institutions such as the Nigeria Customs Service (NCS), cybersecurity intelligence plays a critical role in maintaining the confidentiality, integrity, and availability of information systems used for

border management, trade facilitation, and revenue collection. The effective use of intelligence enables NCS to monitor cyber risks associated with import/export processes, online documentation, and digital payment systems, ensuring that sensitive trade data remains protected from unauthorized access.

### **Cybersecurity and Supply Chain Nexus**

The interconnection between cybersecurity and supply chain security is becoming increasingly significant in the digital age. Cyberattacks targeting supply chain systems can disrupt trade, lead to loss of sensitive data, and affect national economic performance. Okafor (2021) notes that modern customs operations rely on automation and electronic systems for cargo clearance, duty assessment, and risk profiling; any compromise in these systems can result in large-scale economic losses. The use of cybersecurity intelligence provides a strategic advantage by allowing organizations to anticipate potential cyber threats within the supply chain network. Through real-time monitoring, predictive analytics, and intelligence sharing among stakeholders, customs and logistics agencies can mitigate risks before they escalate.

### **Cyber Threats Affecting Customs and Trade Systems**

Common cyber threats facing customs and supply chain systems include:

1. **Phishing and Social Engineering:** Deceptive attempts to obtain sensitive information from customs officers or trade partners.
2. **Ransomware Attacks:** Malicious software that encrypts data, demanding payment to restore access.
3. **Insider Threats:** Employees or contractors who intentionally or unintentionally compromise system security.
4. **Data Manipulation:** Alteration of electronic manifests or cargo information to aid smuggling or tax evasion.
5. **Distributed Denial of Service (DDoS):** Attacks that overload customs websites and disrupt online services. These threats highlight the need for intelligence-driven cybersecurity frameworks to safeguard customs operations and ensure continuity of trade activities.

### **The Role of Artificial Intelligence in Cybersecurity for Customs Services**

The integration of AI into customs services has revolutionized the way border security and trade facilitation are managed, offering significant improvements in both efficiency and security. AI technologies can enhance the detection and prevention of fraudulent activities, including smuggling and illegal trade. Grafova and Bulgadaryan (2023) discuss how AI technologies in customs control systems help automate the detection of suspicious shipments and improve compliance with customs regulations, reducing human error and increasing operational effectiveness. With AI's ability to process and analyze large amounts of data, it can quickly identify anomalies, such as false declarations or discrepancies in import/export documentation, and flag them for further inspection, thereby enhancing cybersecurity at customs checkpoints.



In addition to improving detection, AI plays a crucial role in automating customs processes and streamlining operations. According to Chebotareva et al. (2021), AI technologies have been employed by customs services in both Russia and foreign countries to support digital transformation in their operations. By automating routine tasks such as document verification and cargo inspection, AI allows customs authorities to focus their efforts on more complex issues, while also ensuring a faster, more efficient clearance process. This enhanced operational speed helps reduce congestion at border crossings and facilitates smoother global trade flows, all while maintaining a high level of cybersecurity to protect sensitive data from cyber threats.

AI-driven predictive analytics can also play an essential role in proactive cybersecurity measures within customs services. Marinova (2024) explores how AI can help customs agencies predict and prepare for potential security threats by analyzing patterns of past cyber-attacks and identifying emerging risks. AI's capacity for pattern recognition and real-time analysis allows customs services to adapt quickly to evolving threats, ensuring the protection of both the customs data and the integrity of the global supply chain. Moreover, AI, combined with other technologies like blockchain and Geographic Information Systems (GIS), as highlighted by Khan (2024), offers new possibilities for enhancing transparency, reducing fraud, and ensuring secure customs transactions. This integrated approach ensures that customs services can maintain robust cybersecurity while facilitating the efficient movement of goods across borders.

### **Theoretical Framework**

The theoretical framework for this study focuses on understanding the integration of cybersecurity intelligence and ML in improving supply chain security, particularly within the NCS. It draws from several theoretical perspectives that explain how systems, strategies, and technologies work together to enhance the protection of national infrastructure from cyber threats. This section discusses relevant theories that provide insights into the strategic and technological approaches necessary for addressing cybersecurity challenges in global supply chains. The frameworks considered include Game Theory, Cybersecurity Defense Theory, and Technology Acceptance Model (TAM).

**Game Theory and Cyber Defence:** Game Theory is a crucial framework for understanding strategic interactions in scenarios where outcomes depend on the actions of multiple participants. In the context of cybersecurity, Game Theory is widely applied to model the behaviour of attackers and defenders, particularly when resources are constrained, and risks need to be managed strategically. Sokri (2020) explores how Game Theory can be utilized in cyber defense to anticipate and counteract cyber-attacks through optimal decision-making processes. Within the scope of supply chain security, this approach becomes invaluable as various stakeholders' customs agencies, logistics companies, and suppliers must collaborate to safeguard the entire supply chain.

Zarreh et al. (2018) further elaborate on the application of Game Theory by developing a cybersecurity assessment model, simulating competitive scenarios between attackers and

defenders. This model assists in predicting potential security breaches and guides defenders in optimizing the allocation of resources and the selection of strategies to mitigate threats. As cybercriminals continuously adapt their tactics, this model empowers defenders to respond with more effective and efficient strategies. Game Theory's application in cybersecurity is particularly pertinent for organizations such as the NCS, where multiple stakeholders work collectively to protect digital assets and infrastructure. By leveraging Game Theory, the NCS can better understand the potential outcomes of various defence strategies, enhancing its ability to respond to cyber-attacks effectively. This methodology allows customs agencies to make informed, data-driven decisions about resource allocation, prioritizing actions that maximize security while minimizing costs and potential damages. Furthermore, Game Theory fosters proactive thinking, encouraging stakeholders to anticipate future threats and develop countermeasures before an attack materializes.

### **Key Concepts, Critiques, and Relevance to Research**

**Proposed by:** Game Theory, as initially formalized by mathematician John von Neumann and economist Oskar Morgenstern in their 1944 book *Theory of Games and Economic Behavior*, is foundational in understanding competitive strategies where each party's decision depends on the decisions of others.

**Fundamentals:** At its core, Game Theory analyzes interactions between rational decision-makers (players), whose choices impact the outcomes of the game. In cybersecurity, these "players" are typically the attackers and defenders, each aiming to maximize their respective benefits attackers seeking to breach systems and defenders striving to thwart these efforts.

**Critiques:** One critique of Game Theory in cybersecurity is its assumption of rationality among participants. In real-world scenarios, attackers may not always act rationally, and defenders may be constrained by limited resources. Additionally, Game Theory models often rely on static environments, which may not capture the dynamic and evolving nature of cybersecurity threats adequately.

### **Methodology**

#### **Research Design**

This study adopts a design and development research approach aimed at creating a cybersecurity intelligence framework tailored for the NCS. The approach focuses on the systematic design, development, and evaluation of a software system to address identified challenges in supply chain cybersecurity. The methodology involves extensive review and synthesis of existing literature, including academic papers, industry reports, and relevant technologies in cybersecurity and supply chain management. Insights gained from the literature informed the design specifications and architectural decisions of the system. The research emphasizes the practical implementation of a working prototype that integrates ML and real-time data analytics to enhance cybersecurity intelligence within the NCS. The development process follows an iterative approach to ensure the system meets functional and non-functional requirements identified through the literature review and analysis of current challenges. This design and development approach are appropriate because it allows for

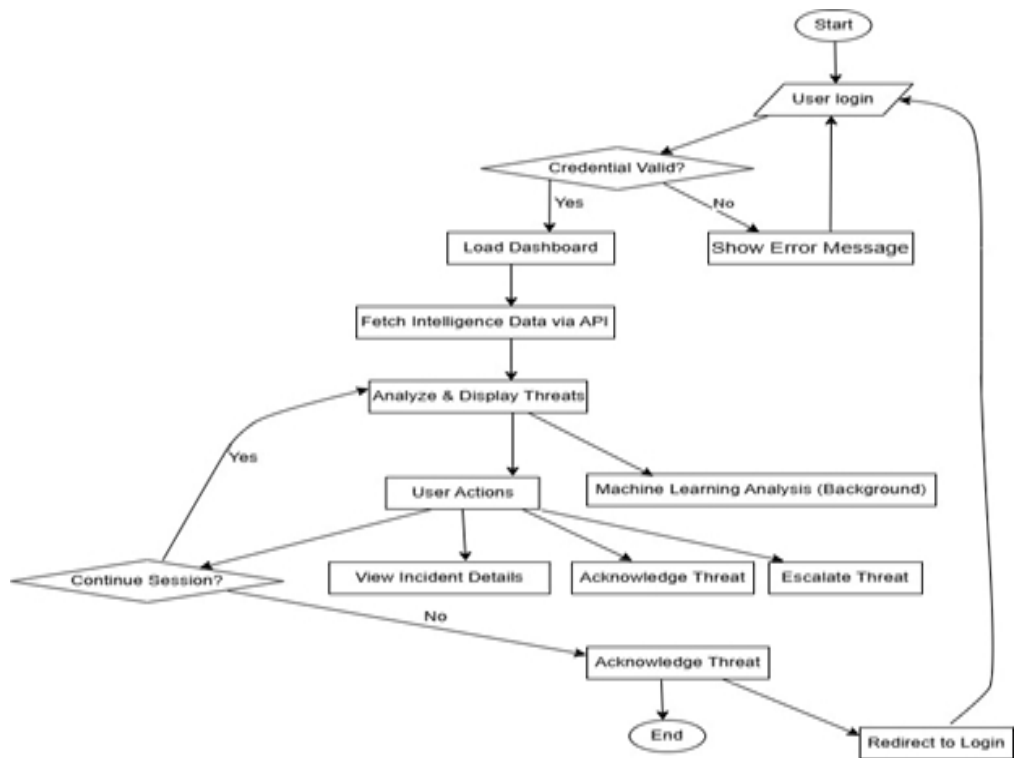
creating a solution directly addressing the needs identified in theoretical and empirical studies while providing a basis for future testing and validation.

**Data Collection Methods**

The data collection for this study primarily involved gathering secondary data from existing academic literature, industry publications, official reports, and online resources related to cybersecurity intelligence, supply chain security, and customs operations. These sources provided critical insights into the current state of cybersecurity challenges and the technological advancements applicable to the NCS. No primary data collection through surveys or interviews was conducted, as the research focused on designing and developing a software system based on established knowledge and documented findings. The literature review served as the foundation for identifying key requirements, functional specifications, and technological components needed for the development of the cybersecurity intelligence framework. Additionally, publicly available datasets and sample cybersecurity intelligence data were utilized for testing and validating the prototype system.

**Flowchart Diagram**

Flowcharts were employed to map the step-by-step processes within the system, illustrating the logical flow of operations such as data collection, threat analysis, and response actions. This visual aid helps in identifying the sequence of activities and decision points.



**Figure 1:** System Flowchart

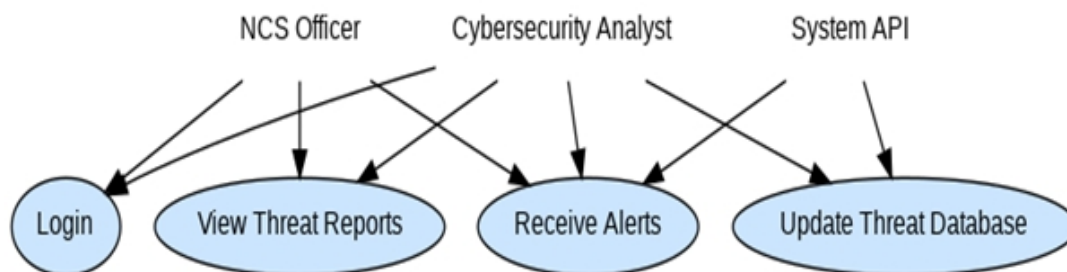


Figure 1 illustrates the System Flowchart for the user login and session management process within the cybersecurity application. The flowchart begins at the Start node, where the User Login process is initiated. After the user inputs their credentials, the system checks whether the credentials are valid. If they are valid, the system proceeds to generate and validate a token, and then loads the dashboard and fetches intelligence data via an API. This data is then analyzed and displayed as threats for the user.

The user is then prompted to either continue the session or not. If they choose to continue, the system awaits further user actions such as viewing incident details, acknowledging threats, or escalating them. Meanwhile, the system runs ML analysis in the background to analyze the data further. If the user opts not to continue the session, they are logged out, and the system clears the token before redirecting them to the login page. If the credentials are invalid, an error message is shown to the user, and they are prompted to correct their credentials. Finally, the flowchart concludes at the End point, signalling the completion of the session. This process ensures secure access management, user interaction with incident data, and session termination when necessary.

### Use Case Diagram

Use case diagrams were utilized to represent the interactions between the system and its various actors, such as customs officers, cybersecurity analysts, and external data sources. These diagrams clarify the system's functionalities from the user's perspective.

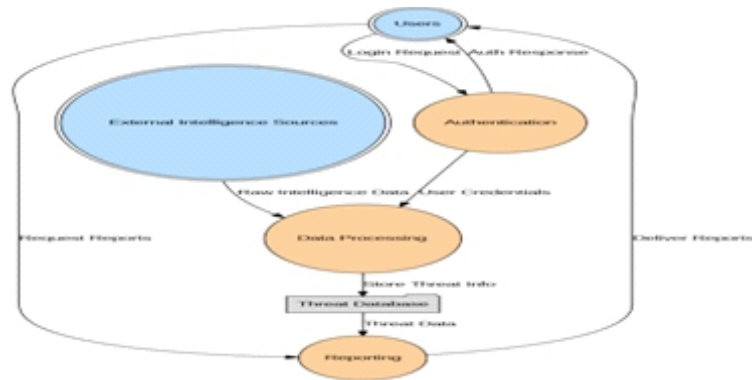


**Figure 2:** Systems Use Case Diagram

Figure 2 illustrates the System Use Case Diagram, showcasing the interaction between three primary actors: the NCS Officer, Cybersecurity Analyst, and System API. The NCS Officer logs into the system and views threat reports, primarily focusing on monitoring and reviewing cybersecurity threats. The Cybersecurity Analyst receives alerts and analyzes them, playing a critical role in investigating and responding to security issues. The System API updates the threat database, ensuring that the system stays current with the latest threat information. This diagram highlights the seamless workflow between the actors and the system, enabling efficient management of cybersecurity threats through login, report viewing, alert receiving, and database updates.

### Data Flow Diagram

Data Flow Diagrams were created to depict how data moves through the system components, emphasizing inputs, outputs, storage points, and processes involved in cybersecurity intelligence operations.



**Figure 3:** Level 0 Data Flow Diagram (DFD) Showing External Entities, Processes, and Data Stores

**Figure 3** illustrates a **Level 0 Data Flow Diagram (DFD)** for the system, depicting the interactions between **external entities**, **main processes**, and **data stores**. In this diagram, the **Users** interact with the system by initiating a **Login Request**, which is authenticated in the **Authentication** process. Once authenticated, the users can **Request Reports** that are processed in the **Data Processing** unit, which also receives raw intelligence data from **External Intelligence Sources**. The **Data Processing** component then stores the processed threat information in the **Threat Database**. Finally, the **Reporting** process generates and **Delivers Reports** based on the stored threat data. This DFD provides a high-level view of how data flows between various components of the system, including user interaction, data processing, and report generation.

### System Development Methodology

The development of the cybersecurity intelligence framework followed an Agile methodology, which emphasizes iterative progress, collaboration, and flexibility. This approach was chosen to accommodate evolving requirements and enable continuous feedback throughout the software development lifecycle. Agile allowed for incremental delivery of functional modules, facilitating early testing and refinement of features such as threat detection, data integration, and user interface components. The iterative cycles ensured that the system remained aligned with user needs and emerging cybersecurity challenges, promoting adaptability in addressing the complex and dynamic nature of supply chain security within the Nigeria Customs Service. By prioritizing responsiveness and collaboration, the agile methodology supported the development of a robust, scalable, and user-centric cybersecurity solution.

### **Testing and Validation**

This section outlines the comprehensive testing procedures undertaken to verify that the cybersecurity intelligence framework operates correctly and satisfies the predefined requirements. Various testing levels were applied, including unit, integration, system, and user acceptance testing. The aim was to validate the system's reliability, accuracy, and effectiveness in detecting, reporting, and managing cybersecurity threats within the Nigeria NCS environment.

#### **Unit Testing**

Unit testing targeted individual components and modules of the system to ensure they functioned as intended in isolation. This included rigorous testing of data input forms to verify correct data capture and validation, API endpoints to confirm proper data retrieval and submission, and authentication modules to guarantee secure user access. Each unit was tested against expected inputs, edge cases, and invalid data to identify and resolve faults at the earliest stage of development.

#### **Integration Testing**

Integration testing focused on verifying the interactions between separate modules once combined. This phase specifically examined the communication pathways between the user interface, backend API, and the threat database to confirm seamless data transfer and integrity. It tested workflows such as user login followed by fetching and displaying real-time threat intelligence, ensuring that modules synchronized effectively without data loss, latency, or errors.

#### **System Testing**

System testing was conducted on the fully integrated application under simulated real-world conditions to assess its overall functionality and robustness. This comprehensive testing phase evaluated not only functional requirements but also non-functional aspects such as system performance, security features, and response time under load. The goal was to identify any defects that could impact user experience or compromise security, and to verify that all components collectively met the project specifications.

#### **User Acceptance Testing**

User acceptance testing (UAT) was conducted to simulate real-world usage scenarios and verify that the system meets operational requirements. During UAT, the system was tested against typical use cases to assess usability, functionality, and performance. Any issues or shortcomings identified were documented, and necessary adjustments were made to improve the system's alignment with expected practical needs. This process ensured the software was reliable and ready for deployment.

#### **Evaluation of System Performance and Security Impact**

The evaluation phase involved measuring key performance indicators such as system response time, accuracy of threat detection, and uptime during simulated operational scenarios. The framework's security impact was also assessed through vulnerability scans and penetration

testing to identify weaknesses in data protection, user authentication, and alert mechanisms. Results showed that the system consistently met expected performance standards, providing rapid and reliable intelligence updates crucial for supply chain security. The detection algorithms accurately identified simulated cyber threats, and the real-time alerting system functioned without delay. Security tests confirmed strong protections against unauthorized access and data breaches. However, some areas required improvement, including occasional delays during peak data processing and limited support for integrating external threat intelligence sources. These issues were documented for future enhancement to ensure the system's robustness in real-world deployment.

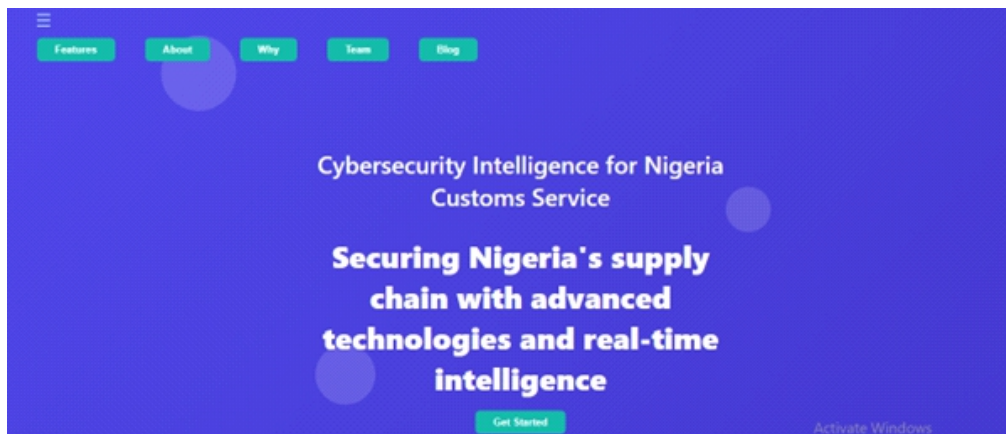
**Functional Testing**

**Table 1:** System Performance and Security Evaluation Summary

Evaluation Aspect	Status	Comments
System Response Time	Functioning	Fast response within acceptable limits
Threat Detection Accuracy	Functioning	High accuracy in simulated scenarios
Uptime / Availability	Functioning	Stable with minimal downtime
User Authentication	Functioning	Secure login and token validation
Alert Notification System	Functioning	Real-time alerts triggered correctly
External Data Integration	Partial / Needs Work	Limited integration with external intelligence
Data Processing Under Load	Partial / Needs Work	Delays observed during peak loads
Security Vulnerabilities	Functioning	No critical vulnerabilities found

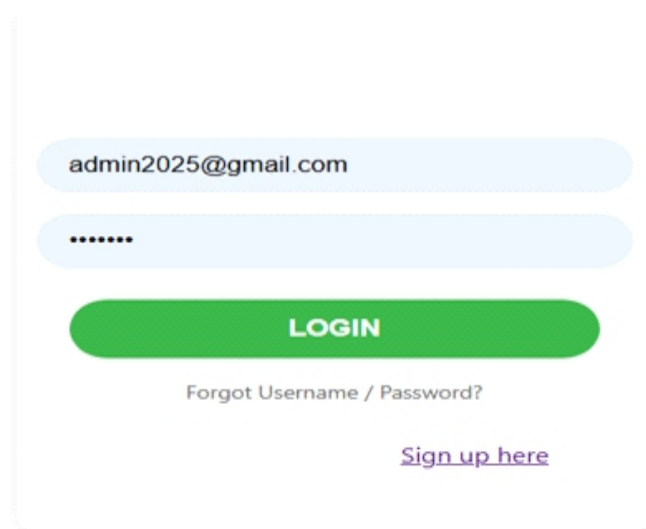
**Usability Testing**

Usability testing was conducted to assess the ease of use, accessibility, and overall user experience of the cybersecurity intelligence framework. Test scenarios focused on the intuitiveness of the user interface, navigation flow, and clarity of displayed information, ensuring that users with varying levels of technical expertise could operate the system effectively. Feedback was gathered by observing interactions during trial runs, focusing on how quickly users could complete tasks such as logging in, accessing threat reports, and generating alerts. Attention was given to the readability of data presentations and responsiveness across different devices. The results demonstrated that the interface was generally user-friendly, with minor areas identified for enhancement in button labeling and error message clarity to further improve user satisfaction.



**Figure 4:** Home page

Figure 4 illustrates the home page of the NCS Cybersecurity Intelligence platform, now with an interactive navigation menu. The page features a prominent "Cybersecurity Intelligence for NCS" heading and a clear subheading: "Securing Nigeria's supply chain with advanced technologies and real-time intelligence." Below the text, the "Get Started" button encourages users to begin their journey with the platform. The navigation menu includes clickable buttons for Features, About, Why, Team, and Blog in a vibrant green colour, making the interface easy to navigate. On smaller screens, a burger icon is visible, allowing the menu to toggle.



**Figure 5:** Login Interface

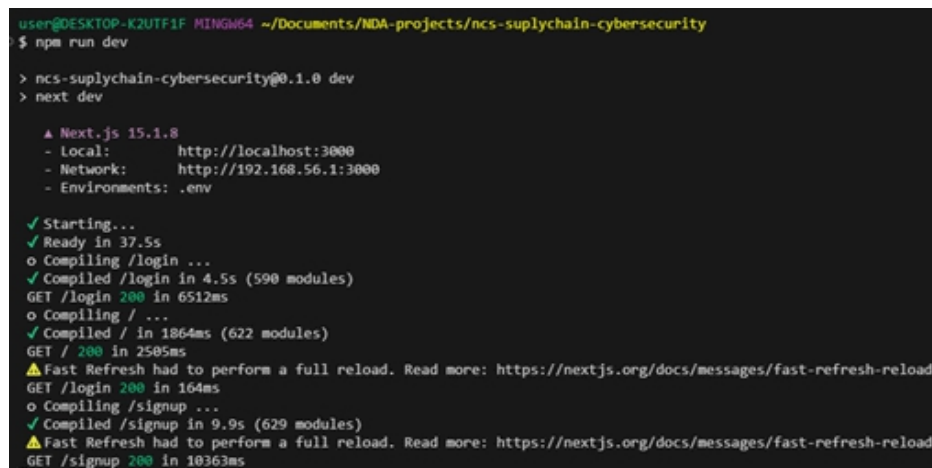
Figure 5 illustrates the Login Interface for the NCS Cybersecurity Intelligence platform. The interface displays a simple and user-friendly design with fields for entering a username and password. The email field is pre-filled with an example address (admin2025@gmail.com), and the password field is masked with dots for security. Below these fields is a green "LOGIN" button. Below the button, there is a link for "Forgot Username / Password?" and a link to "Sign up here".



button, prompting the user to proceed with authentication. Additionally, there are links for Forgot Username/Password? and Sign up here, offering the user options to recover their login details or create a new account. The overall design focuses on simplicity and ease of use for the login process.

### Integration Testing

Integration testing focused on verifying the interactions between the different components of the cybersecurity intelligence framework. This included testing data exchanges between the frontend interface, backend APIs, machine learning models, and the threat database. The objective was to ensure seamless communication and correct data flow across modules, verifying that information from intelligence sources was accurately processed and displayed. Issues related to API endpoint communication, data format inconsistencies, and error handling were identified and resolved during this phase to ensure cohesive system functionality.

A terminal window showing the output of running 'npm run dev' for a Next.js application. The output indicates the server is starting on localhost:3000 and network: 192.168.56.1:3000. It shows successful compilation for the /login and /signup pages, with GET requests returning a 200 status. There are also warnings about Fast Refresh requiring a full reload.

```
user@DESKTOP-K2UTF1F MINGW64 ~/Documents/NDA-projects/ncs-supplychain-cybersecurity
$ npm run dev

> ncs-supplychain-cybersecurity@0.1.0 dev
> next dev

  ▲ Next.js 15.1.8
  - Local:      http://localhost:3000
  - Network:    http://192.168.56.1:3000
  - Environments: .env

✓ Starting...
✓ Ready in 37.5s
  o Compiling /login ...
✓ Compiled /login in 4.5s (590 modules)
GET /login 200 in 6512ms
  o Compiling / ...
✓ Compiled / in 1864ms (622 modules)
GET / 200 in 2585ms
  ▲ Fast Refresh had to perform a full reload. Read more: https://nextjs.org/docs/messages/fast-refresh-reload
GET /login 200 in 164ms
  o Compiling /signup ...
✓ Compiled /signup in 9.9s (629 modules)
  ▲ Fast Refresh had to perform a full reload. Read more: https://nextjs.org/docs/messages/fast-refresh-reload
GET /signup 200 in 10363ms
```

**Figure 6:** Runtime

Figure 6 illustrates the Runtime output for the Nigeria Customs Service Cybersecurity Intelligence platform during development. The terminal shows the process of running the application using Next.js version 15.1.8, indicating that the development server is starting up. The log shows that the system is compiling the pages for login and signup, with the respective modules being loaded successfully. It also notes that Fast Refresh performed a full reload, ensuring that the changes made are reflected in real time. The terminal outputs the status of the server running on both localhost: 3000 and network: 192.168.56.1:3000, confirming that the application is ready and accessible. Additionally, the GET requests for the login and signup pages return a status of 200, indicating that the pages are loading correctly.

### Test Results Analysis

The analysis of test results provided insights into the overall effectiveness and reliability of the cybersecurity intelligence framework. Successful test cases demonstrated that critical

functions, such as secure login, real-time threat data retrieval, and alert generation, performed as expected. Areas where performance lagged or errors occurred were documented, highlighting opportunities for further improvement. The analysis also compared expected outcomes with actual system behaviour to validate compliance with initial design specifications. Overall, the results confirmed that the system is robust, secure, and capable of supporting the Nigeria Customs Service's cybersecurity intelligence needs, with identified areas for future enhancement.

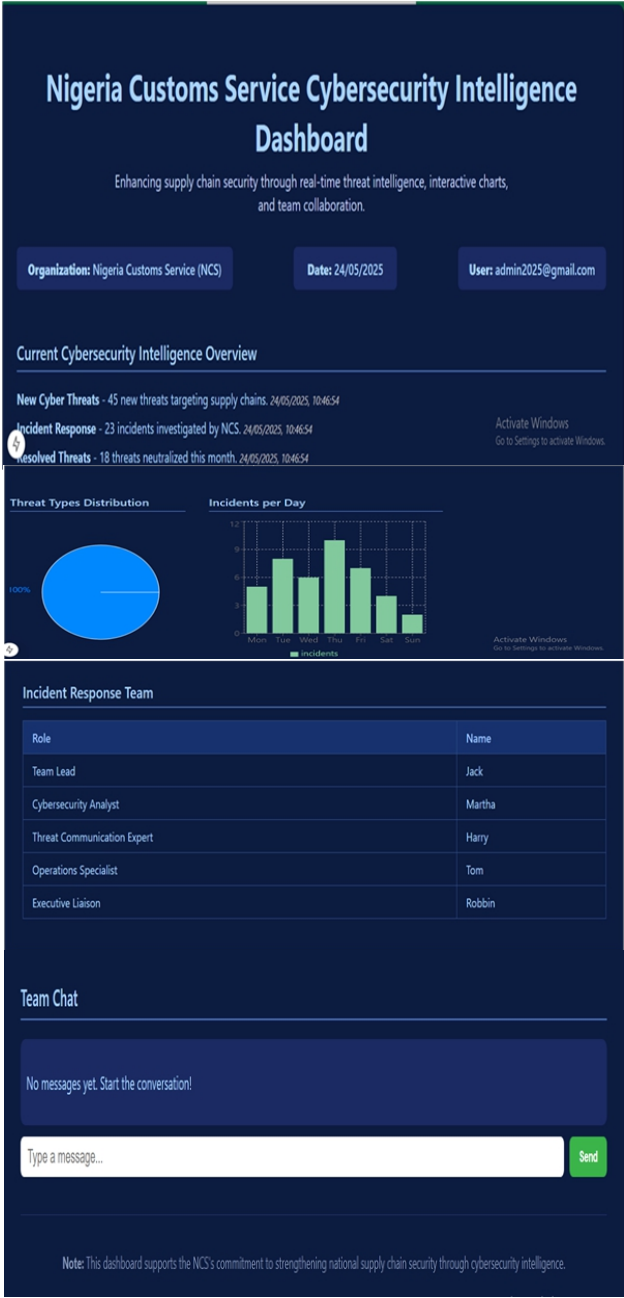


Figure 7: Dashboard

Figure 7 illustrates the dashboard interface designed for the NCS Cybersecurity Intelligence system. The dashboard features a clean and organized layout that highlights key information relevant to cybersecurity and supply chain security. At the top, the dashboard displays the organization's name, the current date, and the logged-in user's email address, providing clear identification and context for the user. The main section presents a Current Cybersecurity Intelligence Overview, showing essential threat data such as new cyber threats, incident response statistics, and resolved threats, each accompanied by the latest timestamp. This overview provides users with up-to-date information crucial for monitoring and decision-making.

Below this summary, the dashboard includes interactive visualizations such as a pie chart for Threat Types Distribution and a bar chart for Incidents per Day. These charts offer intuitive insights into the nature and frequency of cybersecurity incidents, aiding in trend analysis and resource allocation. The Incident Response Team section lists key personnel involved in managing cybersecurity threats, detailing their roles and names. This information fosters awareness of team responsibilities and facilitates collaboration. Finally, the dashboard integrates a Team Chat feature that supports real-time communication among users. This component enables team members to discuss ongoing issues, share insights, and coordinate responses efficiently. The dashboard concludes with a note emphasizing its purpose to strengthen national supply chain security through enhanced cybersecurity intelligence.

## **Conclusion**

The findings of this research validate that integrating ML-driven cybersecurity intelligence within the NCS is a viable and necessary strategy to safeguard national supply chains against escalating cyber threats. The developed framework demonstrated practical effectiveness in enhancing threat detection accuracy, securing access controls, and providing real-time, actionable intelligence critical for proactive incident management. By combining advanced technology with strategic intelligence, the framework addresses key vulnerabilities in Nigeria's customs operations and supports broader national security objectives. This work contributes significantly to the growing body of knowledge on digital security for supply chains in developing countries, offering a scalable model that aligns with the NCS's operational realities and resource constraints. Moreover, the research reveals that successful cybersecurity modernization depends not only on technological innovation but also on user acceptance, organizational readiness, and policy support. The TAM insights highlight the need for systems that are both useful and user-friendly to ensure sustainable adoption within government agencies.

In conclusion, the integration of cybersecurity intelligence through AI and machine learning provides a robust foundation for enhancing border security and trade operations. This study's framework serves as a blueprint for further technological advancement and policy development, positioning the NCS to better anticipate and mitigate cyber risks in an increasingly complex digital supply chain environment.

## **Recommendations**

Based on the study's findings, the following detailed recommendations are proposed to enhance the cybersecurity intelligence capabilities of the Nigeria Customs Service and strengthen national supply chain security:

### **Policy and Institutional**

- i. **Formulate a National Cybersecurity Intelligence Policy for Customs:** The Nigerian government should develop a comprehensive policy framework that mandates the integration of advanced cybersecurity intelligence systems within the NCS and related agencies. This policy should emphasize data sharing, inter-agency collaboration, and standardized cybersecurity protocols to ensure cohesive defense mechanisms.
- ii. **Strengthen Regulatory Oversight and Compliance:** Establish robust regulatory mechanisms to enforce cybersecurity standards across all stakeholders in the supply chain, including logistics companies, freight forwarders, and customs brokers, to ensure end-to-end supply chain security.
- iii. **Enhance Capacity Building and Training:** Regularly train NCS personnel on emerging cyber threats, machine learning applications, and best practices in cybersecurity. Training programs should also focus on fostering user confidence and proficiency with new technologies to support the Technology Acceptance Model's ease of use principle.

### **Technological and Operation**

- i. **Expand External Data Integration:** Broaden the scope of threat intelligence inputs by integrating additional external cybersecurity data sources, such as global cyber threat feeds, industry-specific alerts, and government intelligence agencies, to enrich real-time monitoring and situational awareness.
- ii. **Optimize System Performance for Scalability:** Invest in infrastructure enhancements and algorithmic optimization to improve system performance during peak data loads, ensuring that real-time threat detection and response remain uninterrupted under high operational demands.
- iii. **Incorporate Blockchain Technology:** Explore and pilot the integration of blockchain with AI-driven customs inspection processes to enhance transparency, traceability, and fraud prevention in customs transactions, thereby addressing a key research gap identified in this study.
- iv. **Automate Incident Response Workflows:** Develop automated playbooks within the cybersecurity framework that can trigger predefined countermeasures upon detecting specific threat signatures, reducing response times and reliance on manual intervention.

### **Research and Development**

- i. **Pilot Live Deployments within the NCS:** Conduct controlled real-world deployments of the developed cybersecurity intelligence framework in select customs operations to gather empirical data on system effectiveness, user experience, and operational impact.
- ii. **Investigate Socio-Organizational Factors:** Further research should examine the socio-political and organizational dynamics affecting cybersecurity technology adoption in

- Nigerian public institutions, including cultural resistance, governance issues, and resource constraints.
- iii. Evaluate AI and Blockchain Synergies: Research the combined impact of AI and blockchain on Customs Cybersecurity in Nigeria to develop integrated solutions that address both data security and operational transparency challenges.
  - iv. Develop Predictive Cyber Threat Models: Continue advancing machine learning models to incorporate predictive analytics capable of forecasting emerging Cyber threats based on evolving attacker behaviours and historical incident patterns.

## References

- Abdulrasaq, L.M. (2024). Understanding cybersecurity perception in the maritime sector of Nigeria: A comparative analysis. *World Maritime University*.
- Adepoju, F. (2024). Cyber Threats and Risk Mitigation Strategies in Global Supply Chain Networks: An Infrastructure Security Perspective. *Nuvern Applied Science Reviews*, 8(10), 10-22.
- Adisa, O. T. (2023). *The impact of cybercrime and cybersecurity on Nigeria's national security*.
- Agarwal, P., Mba, S.K., Tayo, T., & Oladapo, A. (2025). Developing a digital trade strategy in Nigeria. *Econstor*.
- Akinyetun, T. S. (2021). Poverty, cybercrime and national security in Nigeria. *Journal of Contemporary Sociological Issues*, 1(2), 86-109.
- Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. *Applied Sciences*, 11(12), 5585.
- Ayodeji, S. A., Abaku, E. A., & Odimarha, O.A. (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. *Academia.edu*.
- Babajide, O., & Okolo, F.C. (2024). The role of artificial intelligence, machine learning, and data analytics in leveraging the operations of the Nigeria Customs Service. *IJLRHSS*.
- Baranovska, T., Savitskyi, V., Serbov, M., Stoliar, Y., & Krutik, Y. (2024). The Impact of Cybercrime on State and Institutional Security: Analysis of Threats and Potential Protection Measures. *Economic Affairs*, 69, 33-42.
- Chebotareva, A. A., Kazantseva, N. G., Vologdina, E. S., Grigorian, T. V., & Sukhanova, I. S. (2021). Digital transformation and artificial intelligence in the activities of customs services in Russia and foreign countries. In *SHS Web of Conferences* (Vol. 118, p. 04014). EDP Sciences.



- Davis, F. D., Granić, A., & Marangunić, N. (2024). *The technology acceptance model: 30 years of TAM*. Switzerland: Springer International Publishing AG.
- Dumchykov, M. O., Utkina, M. S., & Bondarenko, O. S. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis.
- Grafova, T., & Bulgadaryan, A. (2023). Customs Control Using Artificial Intelligence Technologies. *Jurnal BPPK: Badan Pendidikan dan Pelatihan Keuangan*, 16(2), 121-130.
- Granić, A., & Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, 50(5), 2572-2593.
- Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, 55(14s), 1-40.
- Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, 8(8), 6222-6246.
- Idowu, O. A., & Madaki, M. (2021). Cybercrimes and challenges of cyber-security in Nigeria. *Academia.edu*.
- Ishiguzo, R. (2024). Prospects of cybercrime investigation and prosecution in Nigeria and the role of security and Intelligence Agencies in Curbing Cybercrime. *International Review of Law and Jurisprudence (IRLJ)*, 6(2).
- Jebril, I., Almaslmani, R., Jarah, B., Mugableh, M., & Zaqeeba, N. (2023). The impact of strategic intelligence and asset management on enhancing competitive advantage: The mediating role of cybersecurity. *Uncertain Supply Chain Management*, 11(3), 1041-1046.
- Khan, S. (2024). *Digitalizing Customs services to enhance public service quality with AI, blockchain, GIS, and web portals in Pakistan: Prospects, challenges, and policy options compared with developed countries*.
- Manoharan, A., & Sarker, M. (2023). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. DOI: <https://www.doi.org/10.56726/IRJMETs32644>, 1.
- Marinova, V. (2024). Artificial intelligence in Customs. *Izvestia Journal of the Union of Scientists-Varna. Economic Sciences Series*, 13(1), 253-263.
- Muppalaneni, R., Inaganti, A. C., & Ravichandran, N. (2024). AI-Driven threat intelligence: enhancing cyber defense with machine learning, *Journal of Computing Innovations and Applications*, 2(1), 1-11.

- Naab, J. B., & Oroleye, O. A. Mitigating security risks in global supply chains: The role of strategic communication and criminological approaches in countering illicit trade and cyber threats.
- Naab, J. B., & Oroleye, O. A. (2024). Mitigating security risks in global supply chains: The role of strategic communication and criminological approaches in countering illicit trade and cyber threats. *ResearchGate*.
- Natasia, S. R., Wiranti, Y. T., & Parastika, A. (2022). Acceptance analysis of NUADU as e-learning platform using the Technology Acceptance Model (TAM) approach, *Procedia Computer Science*, 197, 512-520.
- Odimarha, A. C., Ayodeji, S. A., & Abaku, E. A. (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies, *World Journal of Advanced Science and Technology*, 5(1), 026-030.
- Odongo, Z. M. (2024). Artificial Intelligence Integration in Tax and Customs Systems in Africa: Applications, Impact and Challenges, *International Journal of Education, Science and Social Sciences*, 3(2), 200-212.
- Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 21(1), 2286-2295.
- Okolo, F. C., Etukudoh, E. A., & Ogunwole, O. (2022). *Strategic framework for enhancing cargo screening and intelligent border security through automated detection technologies. ResearchGate*.
- Olowonihi, A. P., & Musa, M. O. (2024). The role of intelligence in Nigeria's national security: A critical assessment (2011-2023). *The American Journal of Interdisciplinary Innovations and Research*, 6(11), 113-141.
- Olukayode, O. B., Folasade, A. E., & David, A. O. (2018). Nigeria customs service, sources of intelligence and border security. *Singaporean Journal of Business Economics, and Management Studies*, 6(10).
- Oyeyemi, B. B., John, A.O., & Awodola, M. (2025). Infrastructure and regulatory barriers to AI supply chain systems in Nigeria vs. the US. *ResearchGate*.
- Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework, *Journal of Global Operations and Strategic Sourcing*, 13(1), 103-128.

- Richard, H., Authur, J., & Mike, W. (2024). The role of digital technologies in enhancing freight supply chain integration in Nigeria. *ResearchGate*.
- Rybalchenko, L., & Ohrimenco, S. (2024). *The impact of cybersecurity and crime on national security*.
- Shahani, N., & Sehgal, A. (2024). Impact of Cybersecurity and AI on global Supply Chain and economy. *International Journal of Marketing and Technology*, 14(06).
- Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020). Cyber threat detection using machine learning techniques: A performance evaluation perspective. In *2020 international conference on cyber warfare and security (ICCWS)* (pp. 1-6). IEEE.
- Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, 9(11), 1864.
- Sokri, A. (2020). Game theory and cyber defense. *Games in Management Science: Essays in Honor of Georges Zaccour*, 335-352.