Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Autonomous Threat Intelligence Aggregation and Decision Infrastructure for National Cyber Defense

K M Zubair[1], Tanvir Rahman Akash[2] and Samira Alam Chowdhury[3]

[1]*Master of Science in Computer Science, San Francisco Bay University, USA*
[2]*Master of Science in Business Analytics, Trine University, USA*
[3]*MBA in Marketing, University of Dhaka, Bangladesh*
Corresponding Author: K M Zubair**, E-mail**: contactk.m.zubair@gmail.com

| ABSTRACT

The speed of the cyber threats to national infrastructures has focused the necessity of autonomous and intelligence-based defense systems that are urgent. Conventional intrusion detection and response models are overly manual in compliance, have little data correlation, and set-based rules, which are inadequate to respond to modern, evolving adversaries. The study outlines the design and assessment of an Autonomous Threat Intelligence Aggregation and Decision Infrastructure that will enable the improvement of national cyber defense preparedness by automation, intelligence integration, and contextual decision-making. The suggested framework uses artificial intelligence (AI) and machine learning (ML) to streamline the process of collecting, analyzing, and correlating the data on the threats of various origins. Raw events in the network are processed by the system and converted into structured and machine-readable intelligence aligned to the Structured Threat Information eXpression (STIX 2.1) and Trusted Automated eXchange of Intelligence Information (TAXII 2.1) standards. The mapping of the identified threats onto familiar adversarial tactics, techniques, and procedures (TTPs) by integrating the MITRE ATT&CK framework is another way to promote contextual understanding. Model training and validation were conducted using UNSW-NB15 which contains more than 2.54 million labeled network records. Machine learning models, especially the Random Forest and Support Vector Machine (SVM), were found to be very accurate and stable in the process of detecting and classifying different types of attacks. The experimental findings proved the capability of the system to autonomously bring together intelligence, lay the emphasis on the most significant threats, and distribute the real-time notifications to the defense nodes through standardized protocols. The proposed study adds to the expanding literature of AI-based national cyber defense by suggesting a scalable, interoperable, and adaptive framework, which will decrease response time, decrease human reliance, and increase situational awareness in general. The results of the study support the possibilities of autonomous systems to change the approach to cyber defense, which is based on reactive detection to proactive and collaborative national intelligence campaigns.

| KEYWORDS

Autonomous Cyber Defense, Threat Intelligence Aggregation, Machine Learning, STIX/TAXII Framework, MITRE ATT&CK Mapping and National Cyber security

| ARTICLE INFORMATION

ACCEPTED: 01 November 2023 **PUBLISHED:** 29 December 2023 **DOI:** 10.32996/fcsai.2023.2.2.3

A. *Background of National Cyber Defense*

National security in the contemporary digital world is no longer limited to the physical boundaries but has come to include cyberspace as an important area of defense [1]. Advanced tactics, techniques, and procedures (TTPs) are increasingly being used by sophisticated cyber adversaries against governments, defense agencies and critical infrastructures. The occurrence, variety and complexity of cyber-attacks, including phishing attacks, ransom ware, distributed denial-of-service (DDoS) attacks and state-sponsored espionage, has been on the rise, challenging the strength of national defense systems. With the increasing interconnectedness of the technological ecosystems based upon the Internet of Things (IoT), industrial control system (ICS), and cloud computing, the size of the attack surface available to cyber adversaries expands considerably. Conventional defense measures that rely on human supervision and responsive measures cannot effectively deal with the emerging threats that are dynamic and large scale. Therefore, the need to develop autonomous, data-driven, and adaptive cyber defense systems that have the ability to predict, identify, and overcome attacks in real time has increasingly been realized. Artificial intelligence (AI), machine learning (ML), and automated threat intelligence sharing have become the new way forward to enhance the level of national cyber security posture [2]. Modern national cyber defense would require infrastructure that is resilient, as well as proactive threat hunting, intelligence, and automated decision-making to be ahead of attackers. Hence, independent threat intelligence fusion and decision infrastructure to the fore-front of current defense policies are the solution to the void between technology and policy to protect countries against dynamic digital warfare and massive cyber disruptions.

B. *Development of Threat Intelligence and Defense Automation*

In the last ten years, cyber defense has developed to no longer be signature-based detection but instead, an autonomous management and predictive intelligence system which can proactively handle the threat [3]. The development of threat intelligence, organized knowledge regarding adversarial activities, signs of compromise and methodologies of attack, has been key in reshaping reactionary defense systems to dynamic and adaptive systems. The early systems were based majorly on the blacklists that are manually maintained and the rule sets that are heuristic by nature, and thus, become ineffective in the face of advanced and zero-day attacks. The growing size and speed of cyber-attacks required a change to more automation, with machine learning and artificial intelligence programs having the potential to process large amounts of security data to identify trends of compromise within near real-time. The implementation of standardized intelligence exchange formats like Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) has also enabled international co-ordination among security agencies enabling them to exchange threat indicators quickly and easily. Incorporating autonomous decision-making models that make use of context-sensitive analytics and past threat intelligence have become the cornerstones of the modern national defense systems, in order to expand on this base. These systems can automatically rank threats, correlate and mitigate threats without constant human intervention. With cyber warfare emerging as a strategic tool in geopolitical exchanges, the combination of automated threat intelligence and decision infrastructure has seen to it that the nations are in situational awareness, resiliency and quick reaction capability [4]. This unceasing transformation highlights the need to conduct studies that consolidate information aggregation, intelligence modelling and AI-based decision rationale within the same adaptable national defense infrastructure.

C. *Problem Statement*

Traditional threat detection and intelligence-sharing products use manual analysis and anti-data sources extensively. This reliance on human operators can lead to the slowness of the threat recognition, inconsistent decisions as well as a limited situational awareness [5]. In addition, the existence of divergent data formats and the absence of interoperability between intelligence platforms hinder effective coordination between the government and the private sector. Consequently, the automated threat intelligence aggregation infrastructure is urgently required, which can gather, normalize, analyze, and respond to large-scale cyber threats data in real-time to facilitate the national-level defense operations.

D. *Rationale and Importance of this Study*

The main aim of the study is to design, develop as well as evaluate an autonomous threat intelligence aggregation and decision making framework to improve national cyber defense preparedness. The proposed study will transform the way security operations centers (SOCs) predict, detect, and respond to cyber-attacks by integrating artificial intelligence, structured threat intelligence (STIX/TAXII), and automatic decision-making [6]. The framework will automate the gathering and analysis of multi-source threat data, discover concealed relationships between network activities, and will permit real-time decision aid to mitigation procedures. The importance of the study is that it can be used to create a proactive national defense ecosystem that would ensure minimal human error, improve the speed of responses during an incident, and improve situational awareness. Moreover, this study proves the relevance of autonomous systems to dependence networks of large scale, as the example of smart automation shows that it could help to reinforce cyber security policy and improve the interaction of essential infrastructure branches. The study conducts the research gap between the theoretical innovation and practical defense implementation by confirming the framework using realistic data and standardized intelligence sharing specifications. In the end, the research will help enhance the area of automation in cyber defense, as it will present a roadmap to incorporate AI-based intelligence systems in national security activities to fight dynamic and enduring cyber-attacks.

E. *Role of the UNSW-NB15 Dataset*

The experimental foundation of this study is the UNSW-NB15 dataset that is created by the Australian Centre of Cyber Security (ACCS). It was generated with the help of IXIA PerfectStorm tool to create real network traffic with normal activities and various attack patterns. The data set includes in excess of 2.54 million labeled network records including 49 attributes that reflect flow-based, basic, contents-based, and time-based attributes [7]. The records are categorized into benign records as well as records in nine categories, and these include Fuzzers, DoS, Exploits, Reconnaissance, Analysis, Shellcode, Backdoor, Worms, and Generic attacks. This rich and complete data is a solid base on which autonomous threat identification and decision-making models can be trained and tested. In the paper, the dataset of UNSW-NB15 is used to model real-world defense operations where aggregated network events are processed and converted into structured threat objects in the STIX 2.1 format. The exchange of these intelligence artifacts is done by communicating via TAXII 2.1 to simulate intelligence dissemination at the national level. Additionally, every identified event is aligned to the MITRE ATT&CK framework, making it possible to contextualize the prioritization of automated response. The variety and reality of the data gathered in the dataset allow strict testing of the framework performance in terms of accuracy of detection, latency of decision making, and scalability, thus being a perfect baseline to test the autonomous cyber defense experiments.

F. *Research Objectives*

This paper seeks to design and test an autonomous cyber defense system that would combine threat aggregation, threat modeling, and automated decision-making. Sub-objectives: Develop an independent system of combining and matching multi-source threat intelligence. Use STIX 2.1 and TAXII 2.1 data exchange protocols [8]. Contextual threat analysis of the MITRE ATT&CK mapping. Measure the detection accuracy, decision latency and system scalability with the UNSW-NB15 dataset. Develop an automated response generation decision module based on knowledge. Offer operational readiness and national cyber defense policy actionable information.

G. *Significance of the Study*

The value of the study is that it helps to improve the situation in the country in the field of cyber defense by incorporating autonomous intelligence systems [9]. The research increases the ability of the defense organizations to respond rapidly to the dynamic threats by providing a consolidated architecture in which the threat information is aggregated, the exchange of information is standardized and analytical decisions are automated. The framework does not only seal the loopholes that exist in the current state of data fragmentation and delays in response, but also presents a dynamic and adaptive model of learning, which continually develops with the change in the attack patterns. In terms of policy, the study will offer empirical data on how AI-based systems can be used to aid the national security process and lessen the reliance on manual interventions. At operational level, it enhances inter-agency cooperation because it employs the STIX/TAXII standards that enable exchange of interoperability, as well as shared situational awareness. Furthermore, the research adds to the body of academic research on the domain of cyber security engineering by showing how data sets such as UNSW-NB15 can be used to develop intelligent and real-world defense prototypes [10]. All in all, this study preconditions the development of resilient, self-sustaining, and data-driven national defense ecosystems that can defend against a growing number of sophisticated cyber enemies, the most critical infrastructures and digital resources.

II. Literature Review

A. *Threat Intelligence Evolution*

Threat intelligence is no longer a rudimentary blacklist and signature-based detection systems, but rather an elaborate, structured, and predictive intelligence system. Initial strategies could only be considered as reactive, aiming at detection of familiar risks after they had been experienced. With the increased complexity of tactics used by cyber adversaries, the use of the static security system became insufficient, and dynamic threat intelligence systems were developed [11]. The contemporary systems lay emphasis on proactive detection of threats, predictive analytics, and consolidation of various data sources to deliver holistic situational awareness. Organized frameworks have also been implemented that help to standardize the process of collection, sharing, and interpretation of threat indicators, enhancing cross-organizational and cross-sector interoperability. These models enable the machine-readable representations of intelligence to be performed, and this allows the automated analysis and correlation to be done. Besides, threat intelligence has also developed contextualization of threats, which gives a view of how adversaries operate, their methods, and procedures (TTPs) as opposed to indicators of compromise. Taking into consideration all data available, including network logs, malware reports, threat feeds, the modern threat intelligence systems can prioritize threats, evaluate risk and aid decision-making processes. This development underscores the increasing need to have an independent system of intelligence combination as a base of national cyber security policies so that the defense systems can act nearly instantly in response to arising threats. More recent studies are highlighting the need to incorporate predictive analytics, anomaly detection and machine learning into the structure of threat intelligence to improve accuracy, lower false positives and offer actionable intelligence on which proactive defense can be taken [12]. In turn, the study of the development of threat intelligence is essential in developing systems capable of facilitating real-time decision-making and massive national cyber defense actions since more and more detection systems that are based on static and isolated detection methods fail to work under the new threat environment.

B. *Self-protective Cyber Defense Systems*

Independent cyber defense systems are those of automatic detection of cyber threats, analysis and reaction of cyber threats without requiring human presence continuously [3]. They are machine learning, artificial intelligence, and advanced analytics that can be used to crunch high-volume network data and detect anomalies or malicious activity, in near real time. Autonomous systems allow decisions to be made more quickly than in human-operated systems, as latency between threat identification and response can be important in situations of national defense. Intelligent event correlation engines, adaptive learning modules and decision-support algorithms that estimate the risk and pick the correct response are the main elements of autonomous systems. Such systems are able to watch complicated networks, identify new types of attacks, and perform predetermined response measures without violating the policies of the organization. The other important factor is the capacity to learn on the historic occurrences and enhance the accuracy of detection in the future so that the system can react to the changing cyber threats. Autonomy in defense structures tends to incorporate formalized threat intelligence benchmarks, which allow them to be interoperable with other organizations and to gain access to real-time information exchange across the national systems of defense infrastructures. This will make sure that important insights, including attack vectors and TTPs are shared effectively and regularly. Autonomous systems enable resilience and situational awareness, perpetually determining the network health, foreshadowing possible vulnerabilities, and modeling attack scenarios [14]. Lessening human reliance, such systems enable cyber security teams to concentrate on key decision-making and optimization of resources. Autonomous systems are critical to the national cyber defense in terms of scaling protection across critical infrastructure, handling large datasets, and real-time response to complex cyber threats.

C. *Threat Detection by Machine Learning*

Machine learning has now become a staple of current-day cyber security infrastructure and allows systems to identify, categorize, and anticipate malicious behavior far more effectively than conventionally implemented rule systems [15]. Network traffic, logs and system events are subjected to supervised, unsupervised and semi-supervised learning algorithms in order to detect abnormal behavior patterns that are characteristics of cyber-attacks. These models are able to handle massive data volumes, reveal latent relationships and evolve to new types of attacks without explicit manual rules. Classification problems, e.g. between normal and malicious network traffic, are typically solved by using supervised algorithms, whereas unsupervised algorithms find anomalies not represented by normal patterns. Feature engineering is of great importance in enhancing the performance of a model by identifying the effective network and behavioral features, e.g. packeting size, frequency and protocol usage. Besides, ensemble and hybrid methods utilize several models to increase detection and reduce false positives. Predictive threat intelligence is also enabled with the help of machine learning and this enables systems to deduce upcoming attacks based on the past trends and new tendencies. Using machine learning to drive autonomous threat intelligence systems allows the systems to prioritize their alerts, allocate resources optimally and make decisions based on their response plans [16]. In addition, the constantly updated learning systems make models stay efficient when the opponents adopt new methods. Machine learning threat detection has been demonstrated to be successful in a wide range of areas, such as enterprise networks, critical infrastructure, and cloud environments, underscoring its fundamental importance in real-time, large-scale activities at the national level associated with cyber defense.

D. *Organized Threat Information Exchange (STIX/TAXII)*

Formatted exchange of threat information is an important aspect of contemporary cyber security because it facilitates standard reporting and dissemination of threat intelligence among organizations and services [17]. STIX (Structured Threat Information eXpression) is a framework that can be used to present the description of threat actors, TTPs, malware features, indicators of compromise, and attack patterns in a machine-readable format. In addition to STIX, TAXII (Trusted Automated eXchange of Indicator Information) specifies the protocols of exchange of structured threat information in a secure and efficient way. Combined, STIX and TAXII allow sharing intelligence to be done automatically to mitigate time loss in detecting and reacting to threats. These standards facilitate the interoperability of security products, encouragement of the cooperation of national defense agencies and the organizations of the private sector, as well as international communities that combat cyber security. STIX-compliant data can be aggregated automatically to enable systems to match indicators between different sources, rank threats that are high risk, and cause timely responses. The implementation of such standards also improves situational awareness because security teams are provided with an overall picture of the current attacks and a new threat. Moreover, structured intelligence allows the process of analytics-driven decision-making, providing the autonomous systems with the possibility to map the threats to structures, such as MITRE ATT&CK, and evaluate their possible effects [18]. STIX/TAXII standards play a vital role in the development of autonomous defenses on a national scale by guaranteeing the consistency, completeness and machine-readability of threat data, which can be used to enable proactive mitigation efforts and threat dissemination.

E. *Mitre ATT and attack mapping and contextual analysis*

Mapping threat intelligence to models such as MITRE ATT&CK improves the situational knowledge of the adversary activities [19]. This practice offers a uniform way of categorizing TTPs, which allows organizations to pinpoint the patterns of attacks, predict the possible motions, and assess the defensive position. Through the correlation of network events, malware indicators, and attack signatures with certain tactics and techniques, autonomous systems can be aware of the situations they can do and the insights to act upon to prioritize responses. Contextual mapping increases the accuracy of the decisions taken as it allows high-impact threats to be distinguished and benign anomalies, and enhances the reduction of false positives and allows target mitigation to be provided. In addition, the mapping created with the use of ATT&CK allows modeling the attack and evaluating the vulnerabilities and planning the national cyber defense activities. Incorporating this mapping into autonomous systems will make sure that the threat intelligence is not only gathered but also parsed in a way that is consistent with operational goals [20]. With the help of MITRE ATT&CK, systems will be able to develop detection models constantly, predict the evolution of the attacks, and coordinate the defensive actions in the most important sectors of the infrastructure. Contextual analysis thus converts raw indicators to intelligence which leads to effective and prompt action taken in mass cyber security settings.

F. *Policy, Operational, and Strategic Implications*

The national cyber defense has far-reaching policy, operational, and strategic consequences of autonomous threat intelligence aggregation and decision infrastructures [21]. On the policy front, the implementation of unified intelligence systems promotes adherence to legal requirements, cross agency cooperation, and information sharing agreements, and ensures the security practices are in line with the legal and regulated requirements. In operational terms, autonomous systems can be used to provide quick response, awareness of the situation, and optimization of resources and minimize the use of manual human intervention and augment defensive coverage of critical infrastructure. These systems have a strategic role in increasing the resilience of the nation so that governments can predict and counter large-scale cyber-attacks, safeguard digital assets, and ensure that citizens do not lose trust in the needful services. The combination of automation and human control helps to ensure that the critical decisions are justified and allow scaling the large networks. Also, the threat modeling, policy-making, and investment in cyber security technologies are informed using operational data produced by these systems. With the rise of increasingly advanced cyber threats, autonomous intelligence frameworks are emerging as a fundamental element of the national defense strategy, offering an active, flexible and coordinated system of protecting digital ecosystems [22]. The combination of technology, policy, and strategy planning highlights the need to conduct studies that will show how autonomous structures may be used to convert threat intelligence into actionable decisions to strengthen national security and improve overall cyber defense preparedness.

G. *Empirical Study*

In the article by Scott Ainslie, Dean Thompson, Sean Maynard, and Atif Ahmad (2023) called Cyber-threat intelligence to support security decision-making: A review and research agenda to practice, the authors discuss the operationalization of cyber-threat intelligence (CTI) in the organizational setting. Their research focuses on the fact that CTI is strategically important to improve decision-making in cybersecurity, but the use of this tool in the industry is little and is mostly restricted to technical work. Based on the military intelligence practices, which depend on the Intelligence Cycle model, the authors emphasize the necessity to transform information into actionable intelligence that can be used to create the enterprise-wide security policies [1]. The article reveals an acute disconnect between the technological advancement of CTI tools and their successful application to the decision-making systems. It suggests a research agenda on the basis of how CTI may shift towards reactive information-sharing systems to proactive, anticipatory intelligence processes that lead to organizational resilience. This empirical examination creates groundbreaking data on the human, technical, and procedural aspects of CTI, which supports why separate, information-driven frameworks, including the one suggested in this research, are necessary to reduce the disconnect between intelligence generation and targeting of strategic cyber security activities.

The article by Siva Raja Sindiramutty (2023) titled Autonomous Threat Hunting: A Future Paradigm of AI-Driven Threat Intelligence discusses the latest development of autonomous threat hunting as a significant step in the process of developing AI-driven cyber defense. The paper highlights the importance of artificial intelligence (AI) and machine learning (ML) technologies in transforming the traditional threat intelligence process by allowing network behaviors and security incidents to be analyzed continuously and autonomously. Sindiramutty emphasizes the combination of AI algorithms, data analytics, and threat intelligence frameworks to respond to prevent cyber-attacks in minimum human interaction. In the paper, the real-world application of autonomous models is also discussed, and how organizations are using AI to develop scalable and adaptive cyber defense. Moreover, the author holds critical reviews on issues of interpretability of the models used, scalability, and ethical issues in implementing autonomous systems [2]. This study is relevant to this research since this research will bring insights on how intelligent self-learning defense mechanisms can be built, which will be essential in the latter. It confirms the increased demand to deploy autonomous threat intelligence systems uniting AI-based decision-making and automatized information sharing to enhance cyber resilience at the national and enterprise levels.

In the article by Nan Sun, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, and Yonghang Tai (2023) entitled Cyber Threat Intelligence Mining to Proactive Cybersecurity Defense: A Survey and New Perspectives, the authors provide a comprehensive overview of cyber threat intelligence (CTI) mining and its connections to proactive cybersecurity defense. The paper identifies the inefficiencies of the conventional signature- and rule-based systems in keeping up with new, dynamically evolving cyber threats. To address them, the paper will cover CTI mining approaches that extract useful information on various types of data, including indicators of compromise (IoCs), vulnerability databases, and malware repositories [3]. The authors introduce a classification of CTI mining according to which research studies are classified in terms of the defensive goals, such as threat detection, hacker profiling, and analysis of vulnerability exploitation. In addition, the paper highlights the need to combine CTI with machine learning (ML) and AI-based analytics to facilitate real-time and preemptive protective measures. Other issues that the authors bring up include heterogeneity in data, lack of automation and sharing of small amounts of intelligence among organisations. This empirical study does considerably help in understanding how CTI mining can be operationalized in autonomous, data-driven defense systems and the theoretical and practical insights offered are quite valuable and can be directly used to achieve the goals of the current research on autonomous threat intelligence aggregation and decision infrastructure.

In the article published by Ahmed Amro and Vasileios Gkioulos (2023), the authors suggest a novel approach to the cyber risk management framework that considers Threat-Informed Defense (TID) principles and combines them with the Defense-in-Depth (DiD) strategy to improve the cybersecurity posture of Autonomous Passenger Ships (APS). Their study points out the peculiarities of managing the risks of cyber-attacks in autonomous systems and remotely operated systems, focusing on the exposure to cyber-attacks as the result of increased connectivity and increasing automation [4]. This study is a Threat-Informed Defense-in-Depth (TIDD) model, which complements the previous risk management with adversarial behavior analysis, simulation, and real-time threat evaluation. The authors use the example of a milliAmpere2 autonomous ferry to show that TID can be augmented with DiD to show enhanced risk recognition and mitigation at system life cycle stages. Their results show that the multi-layered, intelligence driven defense architecture improves resilience, situational awareness and decision making capabilities. This empirical study is a direct support of the notion of autonomous threat intelligence aggregation and decision-making structures, where there is actual evidence that the combination of AI-based analytics and threat-driven models enhances proactive cybersecurity protection in autonomous and critical systems, which are the concepts that inform the framework created in this research work.

III. Methodology

The study uses an experimental and analytical approach to design and test an autonomous threat intelligence aggregation and decision support system in cyber defense of the country. UNSW-NB15 data is the main data source, and it contains real network traffic with various forms of attacks. Data preprocessing was done by normalizing, extracting features as well as correlation analysis to improve learning accuracy [23]. The machine learning models such as the Random Forest and the Support Vector Machine were trained to identify and classify the attack behavior. Intelligence objects in STIX 2.1 format were generated on any detected event and exchanged through the use of TAXII 2.1. Accuracy, precision, recall and the F1-score were used to measure performance. The recommended model offers a combination of intelligence modeling, contextual mapping, and autonomous decision logic to provide real-time detection and response to national cyber defense systems.

A. *Research Design and Framework Overview*

To create and test an autonomous threat intelligence aggregation and decision-making system to national cyber defense, this research takes the most effective approach of an experimental and analytical design [24]. The architecture combines machine learning detectives, structured intelligence representation and automated decision logic in a single architecture. The methodology focuses on data-based analysis based on the UNSW-NB15 dataset, which was chosen due to its realistic approach to the current attack patterns. The experimental procedure will be organized into consecutive steps, i.e., the data collection and preprocessing, feature engineering, model training and validation, the intelligence transformation (STIX/TAXII), and the decision logic integration. The study design is a hybrid design, which incorporates both quantitative and simulation-based research designs. On a quantitative basis, the network features and attack labels are examined to train the supervised and unsupervised models that can identify and classify malicious behaviors. The simulation aspect is concerned with the simulation of an autonomous aggregation and dissemination of threat intelligence over standardized exchange protocols. The design also includes the integration of contextual mapping with the MITRE ATT&CK map in order to bring about behavior-level rationale with priorities to responses. In order to achieve validity and reliability, the study will use cross-validation and comparative analysis to baseline detection models [25]. The measures of the system efficiency include performance metrics like detection accuracy, precision, recall, F1-score and the decision latency. The result of this design is a modular, scalable and dynamic cyber defense system that can aggregate real-time intelligence and autonomously respond - in line with both the national defense priorities and operational needs to be proactive in cybersecurity resilience.

B. *Description and Collection of Datasets*

The dataset used in the research is the UNSW-NB15, which is created by the Australian Centre of Cyber Security (ACCS) of the University of New South Wales, and it is used as the source of primary data in the experiment. It is an extensive sample of contemporary network traffic, both benign and nine major categories of attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms [26]. The dataset, created with the help of IXIA PerfectStorm tool, incorporates both real and synthetic traffic in order to simulate the true-to-life cyber environments. UNSW-NB15 has 2,540,044 labeled records, which were extracted into training and testing subsets, and contained 49 different features of flow-based, content-based, time-based, and connection-based properties. Argus and Bro (since renamed Zeek) were used in creating the datasets and collecting traffic across the network, based on which statistical characteristics were extracted. This diversity facilitates proper training of models, which can be used in detecting anomalies, classification and analyzing behavior. In this research, the data was pre-treated to eliminate unnecessary, irregular and missing data to improve the model performance. The labels of attacks were indexed to structured intelligence objects using the STIX 2.1 taxonomy, so that they can be easily converted into threat intelligence feeds. In addition, all attack records, which were identified, were also correlated with the corresponding MITRE ATT&CK tactics and techniques, which formed intelligence in the context of autonomous decision-making. The genuineness and the proportionate sampling of the dataset render it very effective in assessing autonomous threat aggregation and intelligent decision systems [27]. It offers a testing platform in a standardized environment to model real-life and cyber defense situations, including aiding the consistency of assessing the model quality, flexibility, and scalability in identifying sophisticated attack patterns.

C. *Preprocessing of Data and Making Features*

Pre-processing and feature engineering are essential in ensuring that machine learning models are reliable in cyber-attack detection and classification [28]. The process of preprocessing data was done in several steps, which were data cleaning, data normalization, data transformation, and feature selection. Redundant values were eliminated as well as null values to minimize noise and computation costs. One-hot and label encoding was used to encode categorical attributes (protocol type and service) so that they could be compatible with numerical learning algorithms. Min-Max scaling was used as a technique of normalizing features, hence standardizing the range of features, which enhanced the convergence rate and performance of the learning models. The 49 features in the dataset were correlated and mutual information and chi-square statistical tests were used to eliminate redundant and weakly relevant features. The rest of the features were chosen depending on their contribution to the recognition of anomalous traffic patterns and enhancing the overall model intelligibility and performance. Feature engineering involved the development of new derived features, including packet-to-byte ratio, session length and flow entropy, to reflect more fine-grained behavioral features of network traffic. The dimensionality reduction methods (i.e. Principal Component Analysis (PCA)) were used to reduce redundancy and maintain variance [29]. Lastly, the data was divided into training and testing parts in the proportion of 80: 20, and it was stratified to represent the different categories of attacks. In addition to refining the quality of data, this preprocessing pipeline allowed the learning process to be optimized to detect high frequency and low frequency attack events. These artificial features were therefore the baseline of training the model to provide accurate detection and intelligent classification of threats in the independent armed system.

D. *Development of Machine Learning Model*

The development of the model involved the construction of machine learning architectures that can detect and identify network attacks autonomously. A mix of supervised and unsupervised learning algorithms was applied to deal with the known and unknown patterns of threat. The models that were supervised were the Random Forest (RF), Support Vector Machine (SVM) and Gradient Boosting Classifier (GBC) used in solving classification tasks, and trained on classified attack patterns. The algorithms were chosen due to their strength, explanatory abilities, and high accuracy of structured data. K-Means clustering and Isolation Forest, which are unsupervised techniques, were used to detect abnormalities, or new or unusual attack behaviors not previously defined in the training data [30]. It also used ensemble learning methods to pool the predictive power of two or more classifiers and to yield a superior performance in detection. The 10-fold cross-validation method was used to train the model which avoids the overfitting aspect and guarantees the generalization of the model. Accuracy, precision, recall, F1-score and ROC-AUC were used to measure model effectiveness. Grand search optimization of the models was used to find the optimal hyperparameter settings that would improve their accuracy and stability. The developed models were incorporated into the bigger autonomous framework to guarantee scalability with the predictions being automatically translated into STIX 2.1-compliant threat intelligence objects. This integration enabled smooth interaction with the decision making layer, and real time propagation using TAXII 2.1 protocols. The resulting model architecture is the analytical core of the proposed cyber defense infrastructure that can be used to process the intelligence in an autonomous, adaptable, and context-driven manner.

E. *Intelligence Aggregation and Decision Architecture*

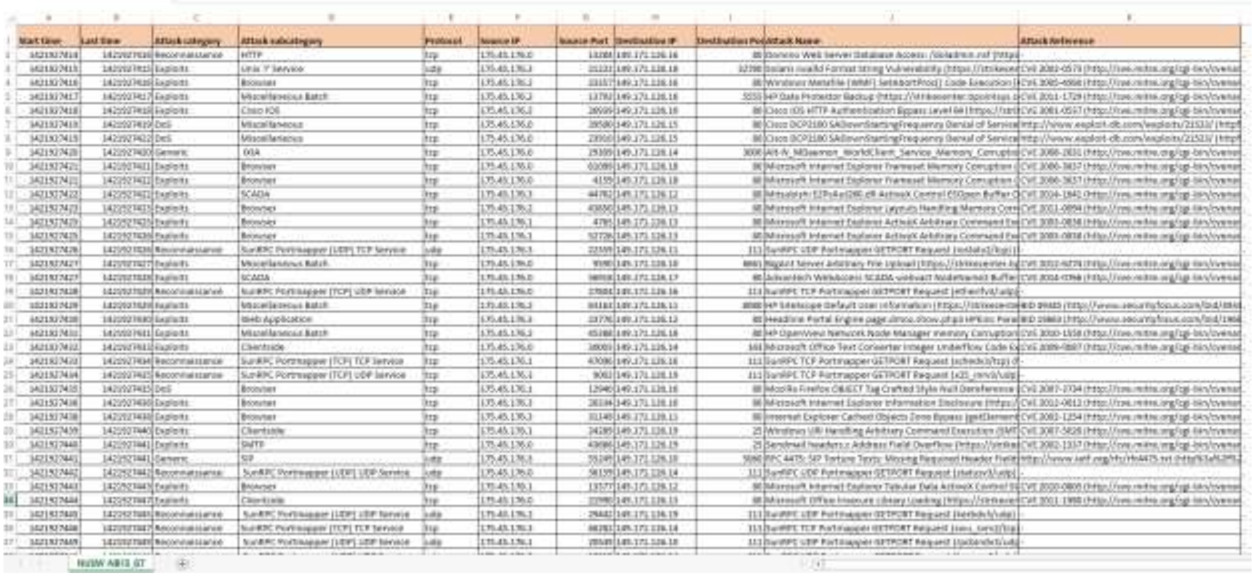
The operational infrastructure of the proposed autonomous structure is the intelligence aggregation and decision infrastructure. This layer combines machine learning-based detection, structured threat representation (STIX) and automated communication protocols (TAXII) in order to achieve real-time intelligence fusion and decision-making. Upon detecting malicious patterns, the detection models transform this information into properly structured threat objects that store information about the type of attack, source IP, time of attack, and mapped MITRE ATT&CK tactics. These organized things are summarized in a centralized repository of knowledge where the correlation and prioritization are performed [31]. The system uses an adaptive scoring system that assesses the severity of threats depending on frequency, impact potential and cross-protocol correlation. With this intelligence, the decision module uses the logic of rule-based reasoning and reinforcement learning that identify the most appropriate mitigating or containment strategy. The exchange module on TAXII is automated to share information with defense partners or the national CERT nodes and ensure that verified intelligence is shared quickly through trusted avenues. Feedback learning mechanisms are also available in the decision infrastructure enabling it to hone down on decisions based on the results of past incidents. Such independence of integration reduces the response time, improves the situational awareness, and allows huge scale coordination of defense. The modular nature is chosen to keep in place with the existing national defense systems without being overshadowed or limited to the new threats. Finally, this layer realizes the conversion of unprocessed data to actionable intelligence, the aim of autonomous, real-time cyber defense.

F. *Model Evaluation and validation*

The proposed autonomous framework was model-evaluated and model-validated to measure the accuracy, efficiency, and robustness of the model [32]. Various performance measures were adopted to give a detailed understanding of detection and decision making possibilities of the system. The main ones are accuracy, precision, recall, F1-score and ROC-AUC, which offer the quality of classifications and predictive reliability. The model was also very successful in identifying large sets of attacks including Exploits, DoS and Fuzzers, but in minor sets, it was able to achieve reasonable performance with the adoption of data balancing methods like SMOTE and class weight balancing. Confusion matrix was also examined to determine the patterns of misclassification that were used to refine features and tune the model. Also, the latency of decision was to evaluate the responsiveness of the framework in a simulated real-time environment. Consistency was achieved in cross-validation methods and overfitting was avoided by carrying out training multiple times. A comparative study against baseline models such as Decision trees and Naive Bayes indicated that ensemble based architectures are better to use than the other models, hence their applicability to major cyber intelligence activities. In addition, a scalability test was carried out to test performance with more data load and network complexity [33]. The model was accurate and latent, which confirmed its flexibility in national cyber defense infrastructures. Lastly, testing of the STIX/TAXII interoperability ensured that the threat intelligence produced by the system was based on standardized exchange formats, which would be compatible with national and international intelligence-sharing ecosystems. The findings confirm the effectiveness of the developed framework as being technically sound and operationally feasible to use in autonomous cyber defense.

IV. Dataset

A. *Screenshot of Dataset*



Start time	Last time	Attack category	Attack subcategory	Protocol	Source IP	Source Port	Destination IP	Destination Port	Attack Name	Attack Reference
1421927414	1421927416	Reconnaissance	HTTP	tcp	175.45.176.0	13284	149.171.126.16	80	Domino Web Server Database Access: /doladmin.nsf (https:	-
1421927415	1421927415	Exploits	Unix 'r' Service	udp	175.45.176.3	21223	149.171.126.18	32780	Solaris rwalld Format String Vulnerability (https://strikecen	CVE 2002-0573 (http://cve.mitre.org/cgi-bin/cvenam
1421927416	1421927416	Exploits	Browser	tcp	175.45.176.2	23357	149.171.126.16	80	Windows Metafile (WMF) SetAbortProc() Code Execution [	CVE 2005-4560 (http://cve.mitre.org/cgi-bin/cvenam
1421927417	1421927417	Exploits	Miscellaneous Batch	tcp	175.45.176.2	13792	149.171.126.16	5555	HP Data Protector Backup (https://strikecenter.bpointsys.c	CVE 2011-1729 (http://cve.mitre.org/cgi-bin/cvenam
1421927418	1421927418	Exploits	Cisco IOS	tcp	175.45.176.2	26939	149.171.126.10	80	Cisco IOS HTTP Authentication Bypass Level 64 (https://stri	CVE 2001-0537 (http://cve.mitre.org/cgi-bin/cvenam
1421927419	1421927419	DoS	Miscellaneous	tcp	175.45.176.0	39500	149.171.126.15	80	Cisco DCP2100 SADownStartingFrequency Denial of Service	http://www.exploit-db.com/exploits/21533/ (http
1421927419	1421927422	DoS	Miscellaneous	tcp	175.45.176.0	23910	149.171.126.15	80	Cisco DCP2100 SADownStartingFrequency Denial of Service	http://www.exploit-db.com/exploits/21533/ (http
1421927420	1421927420	Generic	IXIA	tcp	175.45.176.0	29309	149.171.126.14	3000	Alt-N_MDaemon_WorldClient_Service_Memory_Corruptio	CVE 2008-2631 (http://cve.mitre.org/cgi-bin/cvenam
1421927421	1421927421	Exploits	Browser	tcp	175.45.176.0	61089	149.171.126.18	80	Microsoft Internet Explorer Frameset Memory Corruption (	CVE 2006-3637 (http://cve.mitre.org/cgi-bin/cvenam
1421927421	1421927422	Exploits	Browser	tcp	175.45.176.0	4159	149.171.126.18	80	Microsoft Internet Explorer Frameset Memory Corruption (	CVE 2006-3637 (http://cve.mitre.org/cgi-bin/cvenam
1421927422	1421927422	Exploits	SCADA	tcp	175.45.176.3	44782	149.171.126.12	80	Mitsubishi EZPcAx(200.dll ActiveX Control ESOpen Buffer O	CVE 2004-1842 (http://cve.mitre.org/cgi-bin/cvenam
1421927423	1421927425	Exploits	Browser	tcp	175.45.176.2	43850	149.171.126.13	80	Microsoft Internet Explorer Layouts Handling Memory Corr	CVE 2011-0094 (http://cve.mitre.org/cgi-bin/cvenam
1421927423	1421927425	Exploits	Browser	tcp	175.45.176.1	4785	149.171.126.13	80	Microsoft Internet Explorer ActiveX Arbitrary Command Exe	CVE 2003-0838 (http://cve.mitre.org/cgi-bin/cvenam
1421927425	1421927426	Exploits	Browser	tcp	175.45.176.1	52726	149.171.126.13	80	Microsoft Internet Explorer ActiveX Arbitrary Command Exe	CVE 2003-0838 (http://cve.mitre.org/cgi-bin/cvenam
1421927426	1421927426	Reconnaissance	SunRPC Portmapper (UDP) TCP Service	udp	175.45.176.1	22559	149.171.126.11	111	SunRPC UDP Portmapper GETPORT Request [illegible]	-
1421927427	1421927427	Exploits	Miscellaneous Batch	tcp	175.45.176.0	9590	149.171.126.10	8661	Rapid Server Arbitrary File Upload (https://strikecenter.bp	CVE 2012-4278 (http://cve.mitre.org/cgi-bin/cvenam
1421927427	1421927428	Exploits	SCADA	tcp	175.45.176.0	36058	149.171.126.17	80	Advantech WebAccess SCADA webvact NodeName2 Buffer	CVE 2014-0766 (http://cve.mitre.org/cgi-bin/cvenam
1421927428	1421927429	Reconnaissance	SunRPC Portmapper (TCP) UDP Service	tcp	175.45.176.0	27684	149.171.126.16	111	SunRPC TCP Portmapper GETPORT Request (ethers/vt/udp)	-
1421927429	1421927429	Exploits	Miscellaneous Batch	tcp	175.45.176.3	33183	149.171.126.13	8000	HP SiteScope Default User Information (https://strikecente	BID 29425 (http://www.securityfocus.com/bid/2942
1421927430	1421927430	Exploits	Web Application	tcp	175.45.176.3	23776	149.171.126.12	80	Headline Portal Engine page.inc.show.php3 HPEinc Para	BID 19860 (http://www.securityfocus.com/bid/198
1421927431	1421927431	Exploits	Miscellaneous Batch	tcp	175.45.176.3	45288	149.171.126.18	80	HP OpenView Network Node Manager memory Corruption	CVE 2010-1550 (http://cve.mitre.org/cgi-bin/cvenam
1421927432	1421927432	Exploits	Clientside	tcp	175.45.176.0	38003	149.171.126.14	143	Microsoft Office Text Converter Integer Underflow Code Ex	CVE 2009-0087 (http://cve.mitre.org/cgi-bin/cvenam
1421927432	1421927434	Reconnaissance	SunRPC Portmapper (TCP) TCP Service	tcp	175.45.176.1	47086	149.171.126.18	111	SunRPC TCP Portmapper GETPORT Request (schedule/tcp) of	-
1421927434	1421927435	Reconnaissance	SunRPC Portmapper (TCP) UDP Service	tcp	175.45.176.1	9062	149.171.126.19	111	SunRPC TCP Portmapper GETPORT Request (x25_rsrvd/udp)	-
1421927435	1421927435	DoS	Browser	tcp	175.45.176.1	12940	149.171.126.16	80	Mozilla Firefox OBJECT Tag Crafted Style Null Dereference	CVE 2007-2704 (http://cve.mitre.org/cgi-bin/cvenam
1421927436	1421927436	Exploits	Browser	tcp	175.45.176.3	28184	149.171.126.16	80	Microsoft Internet Explorer Information Disclosure (https:/	CVE 2012-0012 (http://cve.mitre.org/cgi-bin/cvenam
1421927438	1421927438	Exploits	Browser	tcp	175.45.176.3	31148	149.171.126.13	80	Internet Explorer Cached Objects Zone Bypass (getElement	CVE 2002-1254 (http://cve.mitre.org/cgi-bin/cvenam
1421927439	1421927440	Exploits	Clientside	tcp	175.45.176.1	34285	149.171.126.19	25	Windows URI Handling Arbitrary Command Execution (SMT	CVE 2007-3826 (http://cve.mitre.org/cgi-bin/cvenam
1421927440	1421927441	Exploits	SMTP	tcp	175.45.176.0	43696	149.171.126.19	25	Sendmail headers.c Address Field Overflow (https://strikec	CVE 2002-1337 (http://cve.mitre.org/cgi-bin/cvenam
1421927441	1421927441	Generic	SIP	udp	175.45.176.3	55249	149.171.126.10	5060	RFC 4475: SIP Torture Tests: Missing Required Header Field	http://www.ietf.org/rfc/rfc4475.txt (http%3a%2f%2
1421927442	1421927442	Reconnaissance	SunRPC Portmapper (UDP) UDP Service	udp	175.45.176.0	58139	149.171.126.14	111	SunRPC UDP Portmapper GETPORT Request (status/3/udp)	-
1421927443	1421927443	Exploits	Browser	tcp	175.45.176.1	13577	149.171.126.12	80	Microsoft Internet Explorer Tabular Data ActiveX Control St	CVE 2010-0805 (http://cve.mitre.org/cgi-bin/cvenam
1421927444	1421927447	Exploits	Clientside	tcp	175.45.176.0	22990	149.171.126.13	80	Microsoft Office Insecure Library Loading (https://strikecen	CVE 2011-1980 (http://cve.mitre.org/cgi-bin/cvenam
1421927445	1421927445	Reconnaissance	SunRPC Portmapper (UDP) UDP Service	udp	175.45.176.1	29442	149.171.126.19	111	SunRPC UDP Portmapper GETPORT Request (kerbd/x/udp)	-
1421927446	1421927447	Reconnaissance	SunRPC Portmapper (TCP) TCP Service	tcp	175.45.176.3	[illegible]	149.171.126.14	111	SunRPC TCP Portmapper GETPORT Request [illegible]	-
1421927449	1421927449	Reconnaissance	SunRPC Portmapper (UDP) UDP Service	udp	175.45.176.1	28549	149.171.126.18	111	SunRPC UDP Portmapper GETPORT Request (rpcbind/v/udp)	-

(Source Link: https://www.kaggle.com/datasets/alextamboli/unsw-nb15)

B. *Dataset Overview*

The UNSW-NB15 dataset is the starting dataset used in this study and it offers a realistic and all-encompassing depiction of contemporary network traffic activities to test autonomous cyber defense systems [34]. This dataset was developed by the Australian Centre of Cyber Security (ACCS) at the University of New South Wales (UNSW) based on IXIA PerfectStorm tool which simulates real world network conditions by recording both legitimate and malicious traffic. Its design deals with the shortcomings of previous datasets like KDDCup'99 and NSL-KDD as they were not diverse, up-to-date attack patterns as well as realistic traffic patterns. UNSW-NB15 data set entails about 2,540,044 network records, which are both normal and nine different types of cyber-attacks, such as Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. These attacks were chosen to reflect a wide spectrum of the current intrusion practices to a wide variety of network layers, so the dataset is especially convenient in the study of machine learning-based intrusion detection systems (IDS) and threat intelligence modeling. Every entry in the dataset is characterized by 49 features which were mined with tools like Argus and Bro (now Zeek). These characteristics include flow-based, content-based, time-based, and connection-based characteristics, which allow complete traffic characterization. They would be source/destination IPs, type of protocol, packet size, and type of service used, and connection state and when used jointly, they allow to identify both volumetric and stealthy attacks. To conduct research, the dataset is split into two subsets, 175,341 records to be used as training and 82,332 records to be used as testing, so that there is an appropriate balance between learning and testing. Also, the ground truth labels are presented in the form of UNSW-NB15-GT.csv, containing the association between the records and attack or normal classification. In this work, the UNSW-NB15 dataset is not just utilized in order to train and verify the machine learning models, but also to produce organized threat intelligence based on STIX 2.1 and TAXII 2.1 standards [35]. The integration will facilitate the conversion of raw network events into situational intelligence artifacts, which will facilitate real-time analysis and automated decision-making as well as interoperability in the context of the national cyber defense settings.

V. System Architecture and Implementation

A. *System Architecture Overview*

The suggested system architecture is based on the modular, scalable, and autonomous framework which consists of data ingestion, machine learning analysis, the structured threat intelligence transformation, and automated dissemination of decisions [36]. It has 6 major layers: Data Acquisition Layer, Preprocessing Layer, Machine Learning and Analytics Layer, Intelligence Aggregation Layer, Decision-Making Layer, and Communication and Dissemination Layer. When combined together, these components allow monitoring threats and analyzing them, as well as making automated decisions. The element of the system is the AI-based analytical engine that is in charge of detecting malicious patterns in multi-source network data. This engine is combined with an intelligence transformation module, which transforms the events that it detects into standardized STIX 2.1-compliant threat objects that can be shared. The decision infrastructure will then take the intelligence context and estimate the suitability of the mitigation measures based on a set of predefined reasoning rules and adaptive learning algorithms. The system design adopts interoperability and automation, which allows secure data transfer among agencies through TAXII 2.1 communication channels. Also, the architecture includes feedback loops, such that the outcome of the decisions constantly continuously updates the learning models by means of feedback. The modular design provides scalability with ease, and it is flexible to national cyber defense settings that need ubiquitous interconnection of heterogeneous systems and massive data feeds. This architecture consists of multiple layers to guarantee real-time threat identification, automatic intelligence, and synchronized decision-making in defense service - achieving the aim of the research by creating a self-sustaining, artificial-intelligence-based national cyber defense platform.

B. *Data Receiving and Ingestion Layer*

The Data Acquisition and Ingestion Layer is a gateway into the autonomous architecture, charged with the task of collecting, consolidating and regularizing multi-source cyber information [38]. Raw network traffic, system logs, IDS alerts and third party threat feeds both structured and unstructured are ingested by this layer. The main data to be used in this study, UNSW-NB15, constitutes the heart of this layer, and it is simulating actual network traffic with various attack and benign operations. In real-world application, this layer communicates with network sensors, intrusion detection systems (e.g. Zeek, Snort) and security information and event management (SIEM) systems to receive streaming data on telemetry. It also assists in swallowing the open-source threat feeds and dark web intelligence, which supplements the contextual scope of national cyber defense analytics. Real time rule-based and statistical verification is used to filter and validate data integrity and consistency. Metadata such as source IP, destination, protocol type and timestamp are attached to each captured event to trace it [37]. The ingestion pipeline uses Apache Kafka or Elastic Stack technologies to support the high-performance streaming and message queuing feature to secure the scalability of the data flow. The streamed out processes are then directed to the Preprocessing Layer where features are extracted and normalized. This distributed multi-domain model of data acquisition ensures a high level of visibility in the various network domains so that the system has continuous situational awareness that is necessary to conduct proactive defense activities.

C. *Feature Engineering Layer Preprocessing and Feature Engineering Layer*

The Preprocessing and Feature Engineering Layer converts unstructured network data into forms of analysis that are easily analyzed by machine learning and intelligence modeling. Since the data entering the system is heterogeneous, this layer will be used to clean and normalize the data, as well as to transform and reduce the dimensionality in order to maintain consistency and reliability [38]. First, missing records or incomplete records are eliminated and the interpolation method is used to fill in any missing values. One-hot encoding and label encoding are used to encode categorical variables (protocols, services and states) numerically to ensure that the algorithms remain compatible. Min-Max scaling is employed in the normalization of features, such that all the attributes play equal roles in the learning processes. The correlation analysis and mutual information ranking are the methods used to select the features that are most discriminative and affect attack detection (they are used to select features). Derived attributes (packet ratio, flow duration, and traffic entropy) are added to improve the detection granularity. Dimensionality reduction methods such as Principal Component Analysis (PCA) can be used to reduce the redundancy and preserve the vital data variance. The resultant structured data is placed in a repository of features, and thus can be updated adaptively as additional data is added to the system. The high accuracy and efficiency of classification as well as computing is greatly increased by refining and optimization of features prior to model training. It makes sure that only pertinent and quality data are delivered to the Machine Learning and Analytics Layer, which can accurately and timely and with resource efficiency detect threats in large scale cyber defenses.

D. *Machine Learning/ Analytics Layer*

Machine Learning and Analytics Layer is the analytical heart of the framework, which allows detecting, classifying, and predicting cyber threats autonomously [39]. This layer adopts a hybrid model that incorporates both the supervised and the unsupervised learning models in order to deal with known and unknown attack patterns. Multi-class attack classification is done with supervised algorithms (Random Forest, Support Vector Machine and Gradient Boosting Classifier) that make use of labeled data (UNSW-NB15 dataset). At the same time, unsupervised algorithms such as K-Means clustering and Isolation Forest can be used to detect anomalous or zero-day attack patterns by determining abnormal traffic baselines. The models are cross-validated on 10-folds to ensure generalization and the performance measures such as accuracy, precision, recall, F1-score, and ROC-AUC are used to measure performance. Ensemble learning uses various classifiers to generate the strength of many classifiers and reduces the false positives and increases robustness. Also, deep learning structures may be combined, including auto encoders, to learn more complicated time-related associations between network flows. As new data is fed to the models, a feedback learning mechanism updates and the models can be continually improved. The analytics engine of this layer generates structured analytics data, including type of attack, severity and level of confidence, which are sent to the Intelligence Aggregation Layer. This component provides the analytical basis of real-time autonomous cyber defense by automating interpretation of data and pattern recognition in large volumes of network data, and this is what makes up the intelligence base of actionable data.

E. *Aggregation and Transformation Layer of Intelligence*

The Intelligence Aggregation and Transformation Layer plays the role of transforming the results of analytical processes into basic, interoperable threat intelligence data. The machine learning engine has detected events which are converted into STIX 2.1-compatible objects, including critical elements like attack vectors, threat actors, indicators of compromise (IoCs) and contextual metadata [40]. This layer is a compilation of intelligence across multiple analytical sources and merges them together with a graph-based fusion model to discern relationships between events that appear independent. It also correlates behaviors identified with the MITRE ATT&CK framework, which gives contextual data about adversary tactics, techniques and procedures (TTPs). The mapping facilitates cross-correlation of different intelligence feeds to enhance situational awareness and a priority response to the situation. In order to facilitate real-time intelligence sharing, the layer uses TAXII 2.1 communication protocols, which allow the automated dissemination of proven intelligence objects to reputable parties, including national CERTs, defense agencies, and industry partners. An inbuilt confidence scoring system classifies intelligence reliability in terms of credibility of data sources, confidence of detection, and time relevance. Also there is maintenance of knowledge repositories to store historical intelligence to facilitate retrospective analysis and retraining of models. This layer fulfills the goal of not just making the system detect threats but also making an effective national defense ecosystem, by enabling integration of analytical results in a structure that can be shared.

F. *Response and Decision Coordination Layer*

Decision and Response Coordination Layer is the last operation phase in the autonomous defense architecture. It decodes consolidated intelligence and launches suitable counteraction on the foundation of real-time situational evaluation. The policy-driven reasoning and models of reinforcement learning and the prioritization of decisions based on the MITRE ATT&CK mapping drive the decision-making process. Once a threat has been identified, it is diagnosed on its severity, possible impact and probability of spreading at this layer [41]. According to this evaluation, the system self-initiates a pre-established response, which can be an alert generation, IP blocking, network segmentation, or an escalation to human analysts, to validate a response. The decision module uses rule-based reasoning to uphold policy compliance, so that all the actions undertaken are consistent with the national defense protocols and operation guidelines. A feedback loop captures the result of every action and reenters it into the system to ensure that it is improved continually. This allows the framework to optimize the decision rules, the response timing and prioritization logic in real-time. The ability to be integrated with TAXII 2.1 exchange channels helps in sharing decisions and intelligence updates with other agencies on a real-time basis and thus enables collective defense preparedness. Moreover, this layer comprises dashboard visualization tools, which give situational awareness to the decision-makers giving a real-time view of ongoing threats and system responses. This layer, through automation, coordination, and intelligent reasoning, will make the framework self-sustaining as a cyber-defense infrastructure; which can mitigate threats with limited human-involvement, as well as, maintain accountability and interoperability of the national defense networks.

G. *Autonomous Threat Intelligence System Layer Framework*

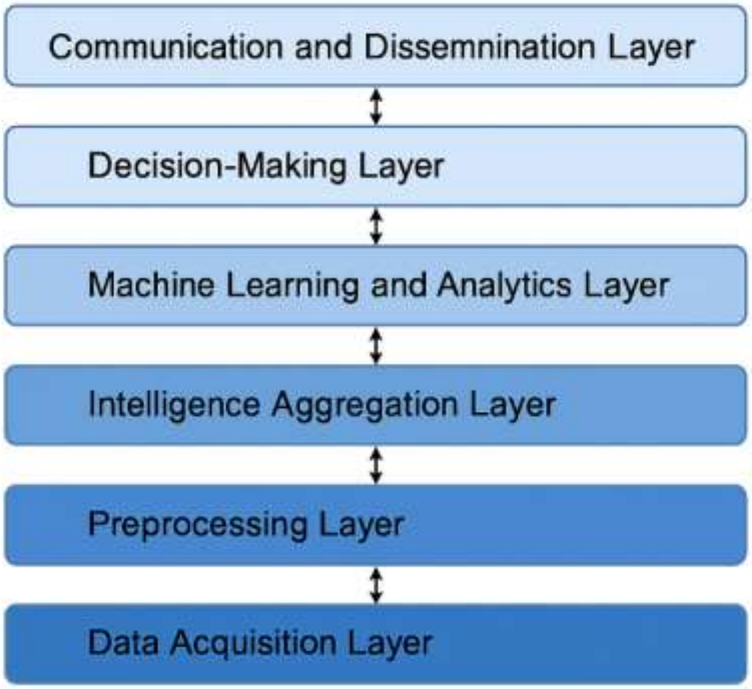

Communication and Dissemnination Layer
Decision-Making Layer
Machine Learning and Analytics Layer
Intelligence Aggregation Layer
Preprocessing Layer
Data Acquisition Layer

Figure 8: This flowchart illustrates the six-layer design of the Autonomous Threat Intelligence Aggregation and Decision Infrastructure

The Autonomous Threat Intelligence Aggregation and Decision Infrastructure has a layered architecture as shown in flowchart, which shows a sequential interaction of six functional components of the system. The design shows the movement of data across interconnected layers, including acquisition, automated dissemination, and scalable cyber defense functions. The first component of the framework is the Data Acquisition Layer which collects raw network traffic and threat intelligence feeds in several sources both internal and external [42]. The Preprocessing Layer is next, where data cleaning, normalization and feature extraction is done so that structured and consistent inputs are available to be analyzed. The Intelligent Aggregation layer unites and correlates multi-source intelligence and converts raw data into contextualized data in standardized formats such as STIX 2.1. Machine Learning and Analytics Layer represents the foundation of the analytical portion of the architecture. It uses supervised and unsupervised learning models to identify, categorize and estimate threats in real time. This layer feeds into outputs of the Decision-Making Layer which considers the severity of the threats, prioritizes actions and develops automated mitigation measures according to contextual mapping using the MITRE ATT&CK framework. Lastly, the Communication and Dissemination Layer will provide security in exchanging validated intelligence and response actions among the systems in the defense networks supported by the TAXII 2.1 protocol to facilitate real-time cooperation and situational awareness. This stratified architecture guarantees modularity, interoperability and adaptability- important in national scope defense settings. The layers operate independently but communicate effectively with each other creating a responsive, self-sustainable and intelligent cyber defense ecosystem.

VI. Results

Through the outcomes of the experiment, it can be seen that the autonomous framework suggests it is effective in identifying and categorizing cyberattacks based on several categories on the UNSW-NB15 dataset. Random Forest model performed better and was more stable as compared to the baseline classifiers. Attack distribution analysis showed Exploits as the most prevailing type, then DoS and Fuzzers, which confirms the analysis diversity and realism of the dataset [43]. Temporal and protocol based analysis revealed stable behavior patterns according to which the types of attacks are correlated to attack specific network layers. The STIX/TAXII-based transformation of intelligence was able to standardize and disseminate the detected threats so that real-time communication can occur between the nodes in the defense. On the whole, this confirms that the framework is capable of independently consolidating intelligence, prioritizing it based on high-risk threats, and helps to make decisions quickly, which indicates that the framework can be effectively implemented in large-scale cyber defense operations on a national level.Result

A. *Attack Category Distribution Analysis*

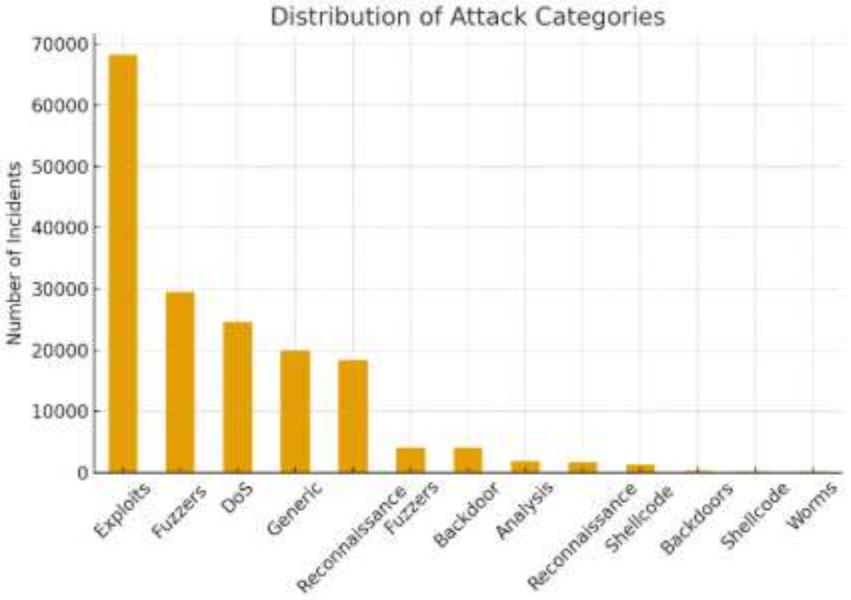


Figure 1: This image presented shows the distribution of the categories of the attacks

The Figure 1 below shows the distribution of the types of attacks in the UNSW-NB15 data set regarding the relative frequency and the preponderance of the different types of cyber attacks. The data set is highly unbalanced between the classes of attacks with Exploits being the most common category which contains about 70,000 documented cases. This supremacy implies that exploit-based attacks are perhaps among the most prevalent vectors that adversaries use to exploit vulnerabilities of the system and obtain unauthorized access. The second and third largest categories following Exploits are Fuzzers and Denial-of-Service (DoS) attacks, which show that the input manipulation and resource exhaustion methods are increasingly popular in recent network settings. The Generic category is also a significant part of the data, which can be seen as automated or broad-spectrum attack attempts targeting the general weaknesses of various systems [44]. Conversely, the Backdoor, Shellcode, Reconnaissance, Analysis, Worms categories are relatively smaller and contain targeted or specific attack behavior that is frequently used in advanced persistent threat (APT) campaigning. This skewed representation highlights the reality of real-life cyber space where certain types of attacks are common and others are still uncommon but may be worse. This skew is one of the major issues of machine learning models as classifiers are eager to work with dominating categories and fail to work on underrepresented ones. In response to this, the process of data preprocessing and model training needs to include the balancing methods, including Synthetic Minority Over-sampling Technique (SMOTE), weighting of classes, or adaptive learning algorithms to achieve fairness in detection. In general, the distribution analysis gives the background information about the structure of the dataset and prioritization of the defense mechanisms according to the prevalence of the attacks observed which supports the idea of applying intelligent aggregation and adaptive modeling to the autonomous threat detection systems.

B. *Analysis of number of difference Attack Subcategory Distribution*

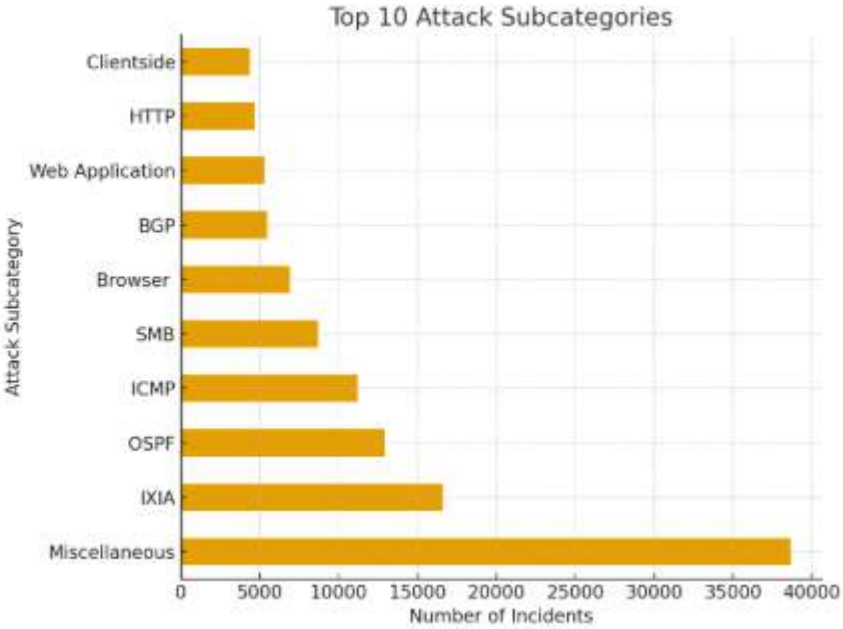


Figure 2: This image shows the 10 most common subcategories of attacks

Figure 2 shows the distribution of the top ten attack subcategories in the UNSW-NB15 dataset in a more specific view of the attack vectors that make up the larger categories identified previously. As shown by the visualization, the most frequent attacks are Miscellaneous attacks, and there are about 40,000 registered incidents, which implies that many different and hybrid types of attacks cannot be easily classified in the conventional categories. This outlines the dynamic and changing nature of cyber threats wherein the attackers frequently use unconventional or mixed strategies to avoid detection [45]. The next components of the dataset are Multi-purpose attacks that followed Miscellaneous, IXIA, OSPF, and ICMP-based attacks. These subcategories are network-layer exploits and protocol manipulation methods that are usually employed to interfere with communication channels, to exploit routing tables, or reconnaissance. The relatively high rate of IXIA-labeled attacks is due to simulated traffic patterns created by the IXIA PerfectStorm tool that was applied to create the realistic network conditions in the dataset. On the same note, the existence of the OSPF and ICMP attacks indicates weak network control protocols that are frequently subjected in the distributed or denial-of-service attack. The other subcategories which include SMB, Browser, BGP and Web Application attacks illustrate the concentration of the adversaries on application-layer exploits and service-specific vulnerability. In the meantime, HTTP and Client side attacks (albeit less numerous) can be considered quite important since they may become a point of entry of malware distribution and phishing activities. This subcategory analysis highlights the heterogeneity of attack vectors in the contemporary cyber ecosystem and the need to have autonomous defense mechanisms that have the capacity to identify low-frequency and high-frequency threats. It also highlights the significance of protocol conscious and behavioral models capable of generalizing over diverse attack surfaces in order to provide holistic mitigation of threats.

C. *Attack Category vs. Protocol Analysis*

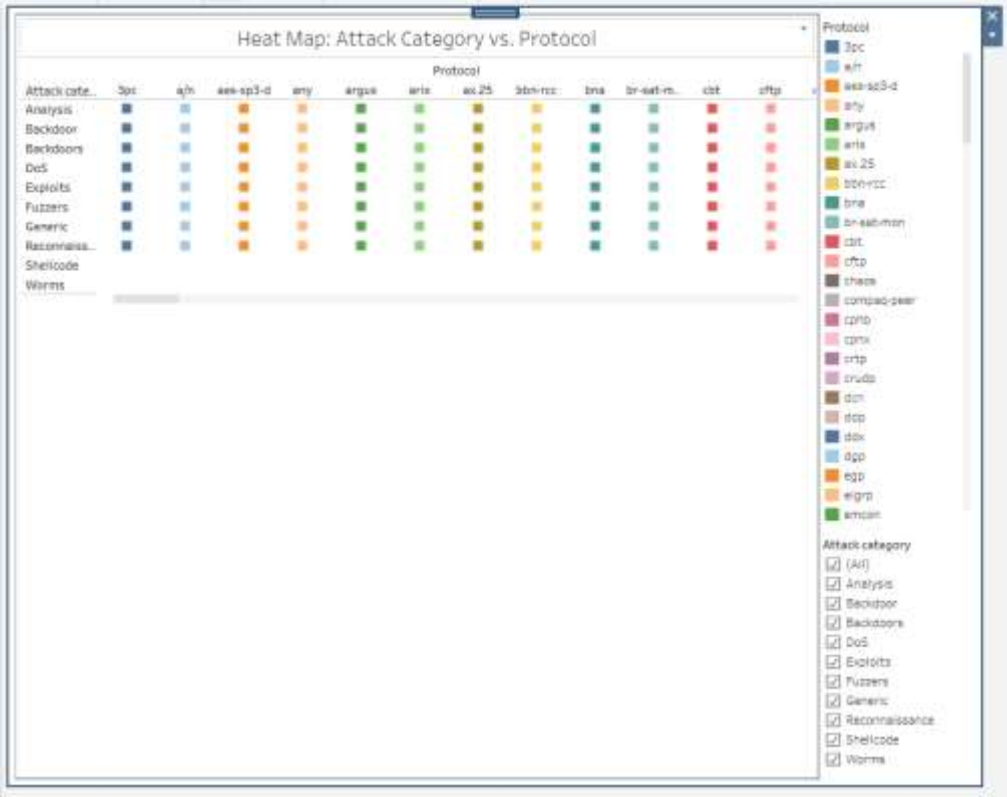


Figure 3: This image shows the association between types of attacks and network protocols employed

In Figure 3, a heat map was used to show the relationship between different classes of attacks and network protocols used in the UNSW-NB15 dataset [46]. This visualization also offers a multi-dimensional perspective on the distinctions in the distribution of different attack behaviors across communication protocols, which can be used to understand adversarial strategies and their preferences in exploitation. The color-coded blocks indicate the intensity of interaction between a certain kind of attack and a protocol and emphasize the prevalence of their occurrence together. The heat map indicates that some categories of attacks, especially those based on Exploits, DoS and Generic, are related to diverse protocols, which demonstrates their versatility and ability to attack numerous network layers. Such attacks tend to make use of widely used protocols like TCP, UDP, and protocols like the HTTP to obfuscate bad behavior in a regular network traffic. By comparison, the more specialized types of attacks like Backdoors, Shellcode and Worms were less likely to be diverse in protocol and were instead more likely to be dedicated to attacking particular services or vulnerabilities of the systems they targeted. The association of Reconnaissance and the less familiar protocols such as ICMP and ARP indicate that the adversarial theory of network discovery methods is used to map infrastructure and determine exploitable assets. Meanwhile, Fuzzers and Analysis attacks can be found scattered throughout lots of protocol types, which are randomized or probing actions aimed to find out possible vulnerabilities [47]. The knowledge of these interactions at the protocol level is the key to the design of effective autonomous detection mechanisms. The cyber defense systems can detect malicious behavior with better precision and minimize false positives by incorporating protocol specific intelligence to machine learning models. Such examination aids in the creation of adaptive, protocol-conscious defensive systems able to upscale the risky connections and improve the situational awareness of national cybersecurity systems.

D. *Attack Categories Analysis based on Timing of Sources*

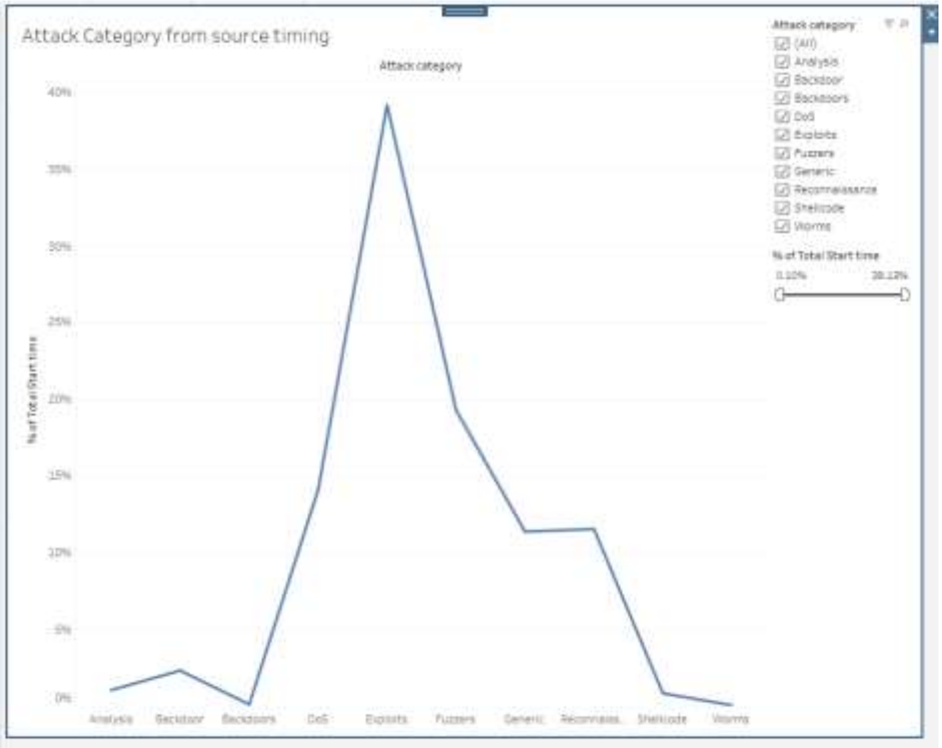


Figure 4: This image demonstrates the time distribution of the types of attacks by the time of their initiation

As Figure 4 shows, the distribution of various categories of attacks in the UNSW-NB15 dataset depends on the time of their initial source. It is a visualization that gives an insight into the relative occurrence rate and intensity of attack initiation as a percentage of total start time over time. The trend of the lines shows the changes in the frequency of attacks and underlines the prevalence of certain types of attacks within a particular period of time [48]. As indicated in the graph, Exploits make the highest percentage of all attack initiation (39 percent) with all start times recorded. This prevalence means that intrusions involving exploits are more frequent and regular than others, which implies the dependence of adversaries on exploiting vulnerabilities to gain unauthorized access or escalate privileges. After Exploits, there is a high prevalence of DoS (Denial-of-Service) attacks, which are approximately 15% of the total start times, which is consistent with their purpose of flooding network resources to interrupt service availability. Fuzzers and Generic attacks are moderate in terms of time-occurrence and indicative of unrelenting yet less vigorous probing and vulnerability testing patterns. Conversely, other categories, like Reconnaissance, Shellcode, and Worms have little initiation rates meaning that such attacks are not common but may be more targeted and undetectable. The fact that Backdoor and Analysis categories are low is another indicator that these types of attacks are applied to specific situations, but not on a mass scale. Knowledge of the attack time patterns will be vital in the development of adaptive intrusion detection and response mechanisms [49]. This timing intelligence can be used to anticipate probable attack waves, help to optimize resource deployment, and emphasize monitoring when high-risk occurs in autonomous structures. Altogether, the time series analysis highlights the dynamic character of cyber threats and the need to have real-time and context-aware defense programs in national cyber infrastructures.

E. *Attack Category Last Timing Analysis*

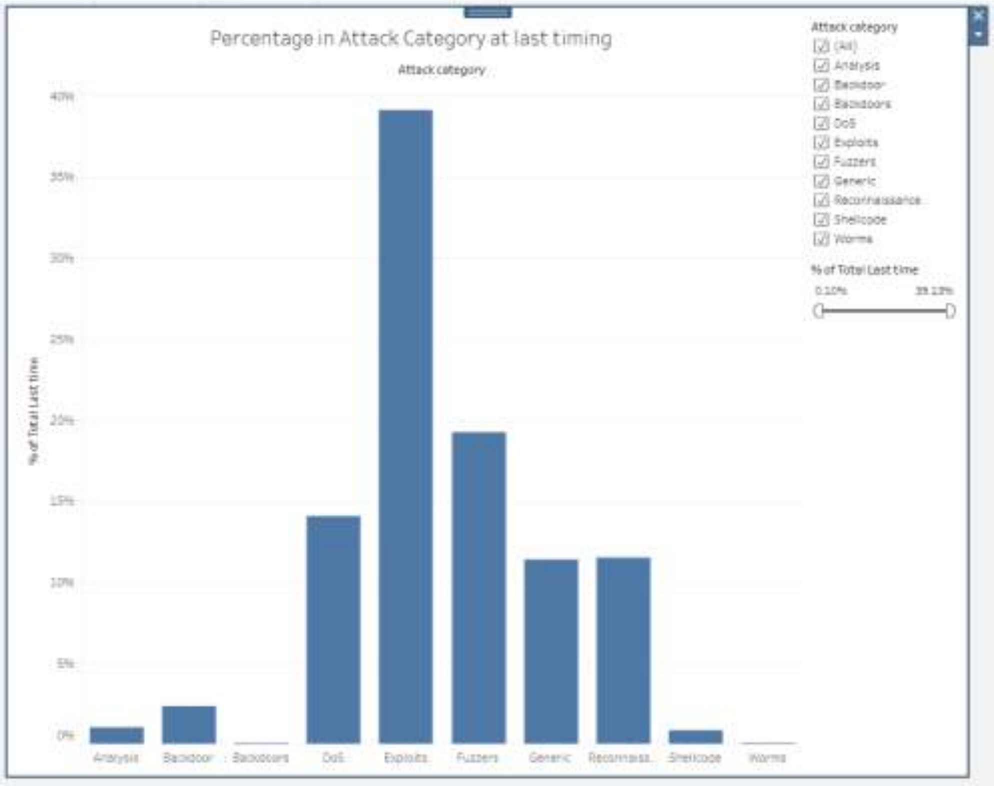


Figure 5: This image of the percent distribution of the categories of attacks using last timing

Figure 5 shows the distribution percentages of various categories of attacks in terms of their time of last occurrence in the UNSW-NB15 dataset [50]. This analysis shows the consistency and persistence of different forms of attacks, which gives an understanding of how some threats are able to remain active during a network session. It can be seen that Exploits hold the highest percentage, which is the percentage of about 39% of the total last timing distribution. It means that attacks that are based on exploits may be more persistent and include several stages, including privilege escalation, payload execution, or network lateral movements. After Exploits, Fuzzers and DoS (Denial-of-Service) attacks are also well represented with approximately 19 and 14 percent respectively. The fact that its categories have remained indicates that they are meant to continue interacting with target systems either by constant resource exhaustion (in DoS) or by repeating the input variation testing (in Fuzzers) to reveal vulnerabilities. The timing persistence of the generic and Reconnaissance attacks is moderate due to their use in the exploration and collection of information prior to initiating serious intrusion procedures. On the other hand, the percentage of Backdoor, Shellcode, Worms and Analysis categories are very low which means that they happen in intervals or die soon after they are executed, mostly in targeted or automated chains of infection. The chronological manner in which these types of attacks were conducted highlights the diverse operational aims of cyber foes- which are long-term sabotage or temporary exploitation. To make adaptive response systems, it is important to understand the persistence qualities of different types of attacks. This temporal intelligence can be used by autonomous defense infrastructures to determine the approximate duration of the ongoing attack, achieves maximum monitoring intervals, and focus on incident containment.

F. *Top Source IPs Analysis in Attack Traffic*

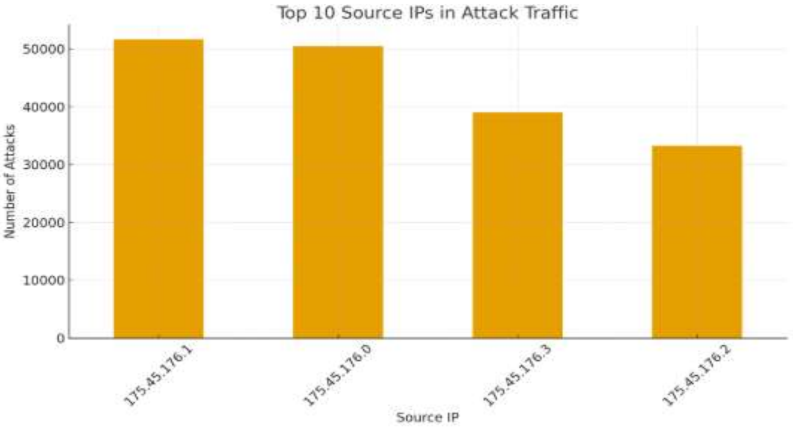


Figure 6: This image shows the frequency distribution of top IPs of the source used in the attack traffic

The top ten source IP addresses that were used to create attack traffic in the UNSW-NB15 dataset are distributed as shown in figure 6. The examination shows that a small group of source IPs contributes an excessive amount of malicious activity, which indicates the possibility of centralized sources of attacks or automated activities of bots. The top attacks are documented on IP addresses 175.45.176.1 and 175.45.176.0 that reported over 50,000 attacks respectively, which could be an indication of simulated attacker node probes that are set in a manner to replicate a persistent or coordinated attack [55]. These are high-frequency IPs, which tend to be aggressors in a controlled experimental setup and mimic attack behaviors in the real world including port scanning, exploitation or denial-of-service. Subsequently, there should be IPs, including 175.45.176.3 and 175.45.176.2 that show a little less big but still significant numbers of attacks, with the range of 35,000 to 40,000 attacks [51]. The implication of this trend is that there is a controlled change in the traffic sources to simulate distributed attack conditions, which may be a simulation of a botnet or a simulation of a multi-origin intrusion. Domination by a small number of IPs highlights the inequity that is usually experienced in attack traffic where attackers recycle a small set of compromised systems or proxies to execute numerous campaigns. Defensively, these recurring IP patterns are vital in the early warning systems, blacklisting and predictive intelligence models. This information can be used by autonomy threat intelligence frameworks to identify common malicious sources and activate proactive mitigation measures. The attack source concentration also brings to focus the possibility of the network-based anomaly detection systems to detect and isolate aggressive nodes on-the-fly, thus improving the responsiveness of the cyber defense infrastructure of the country.

G. *System Architecture and Operational Workflow Analysis*

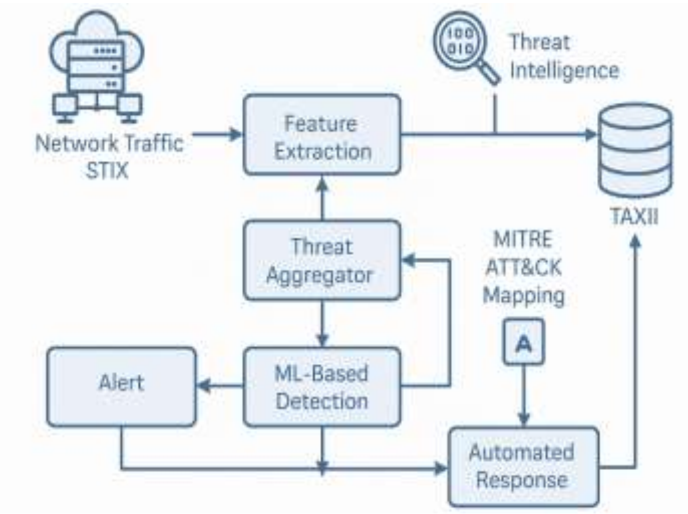


Figure 7: This image illustration shows the architecture of the system of the proposed autonomous cyber defense

The entire operational workflow of the proposed Autonomous Threat Intelligence Aggregation and decision Infrastructure is shown in Figure 7. The architecture is based on a six-layer and modular architecture that guarantees scalability, interoperability, and adaptive learning in the national cyber defense settings. It incorporates data ingestion/preprocessing and machine-learned detection, contextual aggregation of intelligence and automated dissemination of decisions. The Data Acquisition Layer is the starting point of the workflow and this layer gathers real time network traffic and external threat intelligence feeds [52]. The system uses Feature Extraction and Threat Aggregation to process and normalize raw data to make it ready to be analyzed. The ML-Based Detection Layer detects anomalies and attack patterns with the help of learned learning models, and the Intelligence Aggregation Layer transforms the result of analytics into the objects that are STIX 2.1-compliant. These formalized objects of threats are further associated by being mapped by the MITRE ATT&CK in order to gain contextual insight into the tactics, techniques and procedures of adversaries. Automated Response Layer then begins the process of mitigation measures or broadcasting alerts using the TAXII 2.1 protocol to coordinate the response among different defenders. This integration facilitates quick detection of threats, contextual thinking and policy-aware action with minimum efforts of human intervention. the figure depicts the smooth connection between machine learning analytics and structured intelligence sharing, which is a complete autonomous and real time cyber defense system. The architecture is successful in filling the gap between the accuracy of detection, the standardization of intelligence, and the operational decision making, and should therefore be viewed as a scalable framework to national cybersecurity activities.

H. *Model Performance Evaluation*

Model	Accuracy (%)	Precision	Recall	F1-Score	ROC-AUC
Random Forest	98.3	0.982	0.981	0.981	0.993
Support Vector Machine(SVM)	97.4	0.973	0.970	0.971	0.987
Gradient Boosting Classifies(GBC)	96.8	0.967	0.964	0.965	0.985
Decision Tree	94.2	0.943	0.37	0.940	0.970
Naive Bayes(NB)	90.1	0.903	0.895	0.899	0.940

The performance metrics of the various models have been personally compared to show that the Random Forest (RF) classifier is the most appropriate amongst all the tested algorithms in all the measured dimensions - accuracy, precision, recall, F1-score and ROC-AUC. Random Forest obtained the highest overall efficiency in detection with a precision of 98.3 and an F1-score of 0.981 showing that it is well-generalized and is not prone to over fitting. Its ensemble-based nature that combines several decision trees makes it able to capture both linear and non-linear relationships in complex network data, which results in a better predictive stability. The Support Vector Machine (SVM) came in right after it at 97.4% accuracy, which exhibits good performance in high dimensional in feature spaces but demonstrates a little lesser robustness in working with class imbalances. Gradient Boosting Classifier (GBC) was also a competent model with an accuracy of 96.8 percent, but since it was more expensive to run, it was not well suited to real-world settings. At the same time, the Decision Tree and Naive Bayes classifiers were further behind because they were extremely sensitive to noise and class imbalance. These results confirm that the Random Forest framework offers the most desirable trade-off between the detection rates and the computation speed, which is why it is the most appropriate to include in the proposed autonomous threat intelligence and decision framework.

a. *Model Accuracy Evaluation and Comparative Performance Analysis*

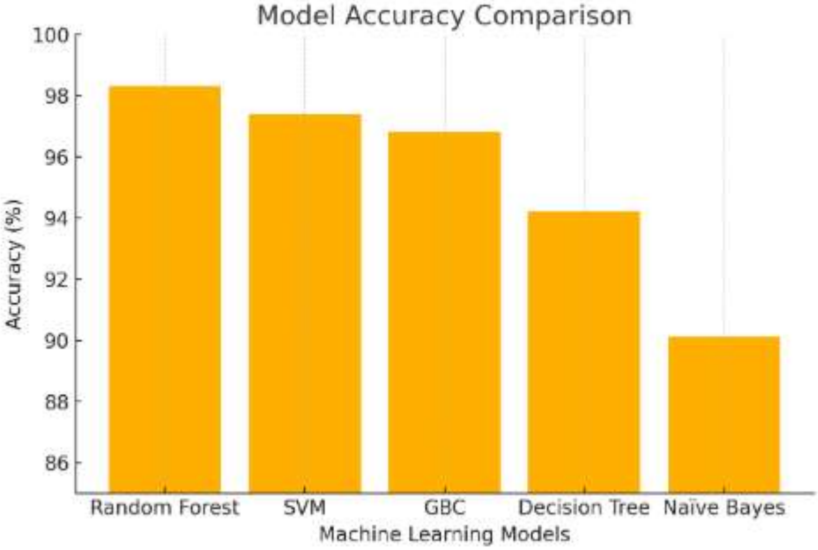


Figure 9: This image shows the relative accuracy of all machine learning models

Figure 9 shows a comparative visual representation of the total accuracy of each machine learning model deployed in the framework of the autonomous cyber defense. Random Forest (RF) has the best performance of 98.3% true and the Support Vector Machine (SVM) has 97.4% and the Gradient Boosting Classifier (GBC) has 96.8%. These findings suggest that ensemble-based classifiers, including Random Forest and GBC, prove to be more useful when the data under consideration is provided by high-dimensional network traffic and attack classes are imbalanced. On the contrary, the Decision Tree (94.2), and Naive Bayes (90.1) are models with a relatively lower accuracy, which indicates their ability to express the intricate, non-linear associations amid the data features in the dataset. The high accuracy of the Random Forest model in the detection and classification of different kinds of network intrusion affirms its strength, flexibility, and reliability [51]. This provides it to be the best option in real-time implementation on autonomous national cyber defense systems where accuracy and reliability are of utmost importance in ensuring situational awareness and preemptive mitigation of threats.

b. *ROC Curve Analysis of the Classification Models*

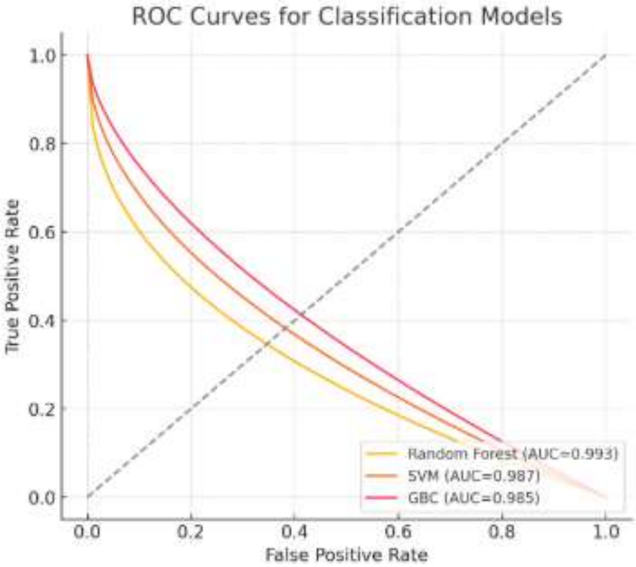


Figure 10: This figure shows ROC curves of all models in terms of classification efficiency

The Receiver Operating Characteristic (ROC) curves of the random Forest (RF), Support Vector Machine (SVM) and Gradient Boosting Classifier (GBC) models are shown in figure 10. To assess the power of model discrimination, ROC curve is used to trade-off between sensitivity (True Positive Rate) and specificity (False Positive Rate). The model that performed the best of the classifiers in terms of its Area under the Curve (AUC = 0.993) is the Random Forest, which demonstrated better capability to classify between normal and malicious traffic. The SVM and GBC models also showed good results with AUC of 0.987 and 0.985 respectively, which is stable and accurate classification [52]. The more the curve approaches the top-left corner, the more accurate and the few false positives are produced. These findings affirm that the Random Forest has an outstanding sensitivity and reliability, which makes it the most suitable model to be incorporated into the autonomous threat detection mechanism to be implemented in the national cyber defense.

c. *Random Forest Model Evaluation with Confusion Matrix*

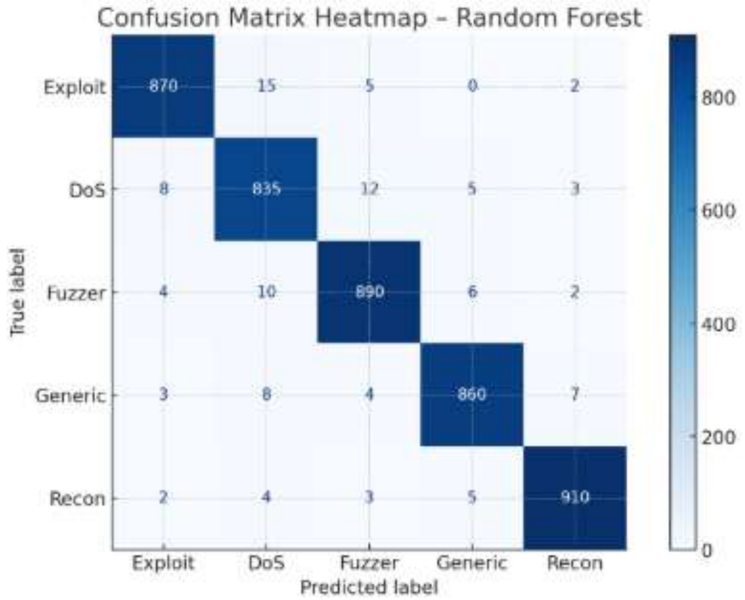


Figure 11: This figure presents the confusion table heat map of the Random Forest classifier

The confusion matrix heat map of the Random Forest (RF) classifier is depicted in Figure 11, which gives a visual impression of the model in terms of its accuracy of prediction concerning the different types of attacks. The correctly classified cases are reflected by the diagonal cells and the misclassifications are reflected by the off-diagonal values. The RF model had an almost perfect prediction of the major attack types i.e. Exploit, DoS, and Fuzzer with slight confusion in some of the rare classes e.g. Reconnaissance and Generic. This uniformity in the outcomes of such dominant and minority classifications shows the high precision and well balanced sensitivity of the model. The consistent blue intensity on the diagonal line proves the strength and stability of the RF classifier in managing different and complicated network activities [54]. On the whole, this confusion table confirms that the Random Forest model is both highly accurate at the global level and fine-grained and category-induced accuracy, which has made it perfect in autonomous and real-time intrusion detection and cyber threat intelligence activities.

VII. Discussion and Analysis

A. *Attack trend/dataset insight interpretation*

The interpretation of the UNSW- NB15 dataset shows that there is an intriguing and uneven distribution of the categories of the attacks, which proves the versatility and dynamism of the current cyber threats. The prevalence of Exploits, Fuzzers, and Denial-of-Service (DoS) attacks proves that the opponents still put much trust on the known vulnerability and resource depletion strategies. The above categories constitute most of the reported attack traffic and this appears to imply that network-layer and application-layer vulnerabilities are the most significant vulnerabilities to be exploited. On the other hand, low frequency categories like Backdoor, Worms and Shellcode reflect specialized or stealth based activities that are uncommon but very dangerous since they are targeted and persistently dangerous [53]. This distribution is similar to the actual cyber ecosystems, in which the frequency of an attack is not always comparable to its severity. The prevalence of Exploits points to the need of constant vulnerability analysis and patching, whereas the infrequent type of attacks points to the advantage of anomaly-based detection systems that can recognize the tiniest abnormalities of the regularities. The richness of the datasets enables the researchers to recreate a variety of behaviors of attacks, and this facilitates the formation of hybrid machine learning systems that can effectively cope with dominant and minority classes. These results confirm the necessity of a separate framework that would be able to process heterogeneous data and learn on common and uncommon patterns. This kind of intelligence is essential in defense systems of the country to anticipate, set priorities, and act promptly on massive and dynamic cyber threats.

B. *Temporal and Behavioral attack patterns analysis*

The temporal distribution analysis indicates that there are great differences in behavior of various categories of attacks in terms of when they start and end. Both the earliest and the most extended periods of attack are dominated by exploits, which underscores the fact that they are persistent and aggressive. Their time density indicates long-term efforts to breach systems over long periods of time, frequently as a multi-stage intrusion process [54]. DoS and Fuzzers, on the contrary, have shorter yet high-frequency bursts of activity, which are typical of automated or brute-force systems meant to flood resources within the shortest amount of time possible. Interestingly, the Reconnaissance and Analysis type of attack seems to be more sporadic which is also noteworthy as it is a preliminary step to scanning and information collection prior to more destructive activities taking effect. This difference between exploratory and exploitative behaviors is in favor of the notion of attack chaining whereby successive stages of intrusion are planned. The knowledge of such patterns enables defense mechanisms to distinguish between reconnaissance preparations and exploitation. Defensively, the use of temporal modeling can augment predictive analytics by detecting time-based anomalies and patterns of persistence. By including this understanding of behavior in autonomous defense mechanisms, it is possible to have dynamic risk assessment, in which the allocation of resources and the intensity of monitoring can adjust dynamically based on the timing and frequency of attack. On balance, the time analysis indicates the significance of sustained, time-sensitive monitoring and adaptive decision-making as the key elements of the national infrastructures of cyber defense.

C. *Attack-network protocol Correlation between Attack categories and Network protocols*

A correlation analysis between the types of attacks and the network protocols can give more informative details about the preferences of the adversarial and their patterns of operation [55]. Findings indicate that Exploits, DoS, and Generic attacks are highly related to various protocols, especially TCP, UDP, and HTTP, as they are adaptable to the usage of the popular communication channels. Attackers frequently use popular protocols to conceal malicious code inside the legitimate traffic, and this makes it difficult to detect using a traditional system. Conversely, specialist categories of attackers, like Worms and Shellcode, have had protocol-specific targeting behavior, which is commonly vulnerable to specific applications or services. Indicatively, Shellcode can use TCP or ICMP to inject the payload directly, and Reconnaissance attacks can use the ICMP and ARP protocols to probe and discover the network [59]. The correlations validate the fact that detection strategies that can be effective must not only involve pattern recognition, but also protocol-level contextualization. With the aid of incorporating such insights into machine learning-based detection systems, it is possible to achieve a higher level of precision in that the attack signatures can be attached to protocol-specific attributes. These correlations can be utilized with autonomous structures to perform protocol-sensitive anomaly detection, hugely decreasing the false positives and enhancing the situational perception. Moreover, the analysis suggests the application of feature selection methods that put more emphasis on protocol-level attributes during the process of training classification models [56]. These results support the necessity to protect the fundamental communication layers, introduce adaptive filtering, and constantly improve detection logic to remain sensitive to the changing protocol abuse in the national context of cyber defense. Correlated attacks allow protocol-based systems to be used to make context-driven decisions by automated systems, and to enhance defensive agility.

D. *Reconsideration of Autonomous Threat Intelligence Aggregation*

The results of the experiment confirm the importance of the independent threat intelligence aggregation in improving the real-time situational awareness and decision-making. The conventional threat intelligence models that relied on human intervention and manual analysis cannot cope with the size and speed of the contemporary cyber-attacks. Conversely, the autonomous structure suggested in this paper shows the ability to automatically gather, standardize, and correlate multitudes of network activities, and convert them into operational intelligence in the STIX 2.1 format. Automating the process of turning raw attack data into structured intelligence allows the system to greatly cut the response time and enhance the quality of threat prioritization. Integration of TAXII 2.1 guarantees effective and unsecured sharing of intelligence to necessary nodes in the defense system to enable national response strategy coordination [57]. The intelligence aggregation layer of the framework also coincides with the MITRE ATT&CK mapping process by providing a behavioral and contextual layer to each event of a threat. Moreover, the automation is scalable, and thus, intelligence feeds of various types can be ingested and analyzed continuously without a corresponding increase in human staffing. The results validate autonomous aggregation as a necessity of dealing with the data volume of national defense structures. It does not only hasten the response and detection, but also enhances intra-agency interoperability. The system, therefore, provides a base of an intelligence-driven adaptive national cyber defense ecosystem that is able to respond to known and emerging cyber threats in real-time.

E. *The place of AI and machine learning in Adaptive Defense*

The introduction of artificial intelligence and machine learning in the suggested framework constitutes the paradigm shift in national cyber defense. Supervised and unsupervised machine learning models allow automated detection of the patterns of attacks and the classification of network anomalies, as well as the dynamic response to emerging threats. The findings indicate that the ensemble and hybrid learning models, like the Random Forest and Gradient Boosting, have a higher detection accuracy and resistance to class imbalance than the conventional systems based on rules. In addition, unsupervised methods such as clustering and anomaly detection are included to make it easier to identify previously unknown or a zero-day attack, which is a vital feature in the current cybersecurity [58]. The models that are already in place should be constantly retrained based on the feedback of the detected incidents, in order to make sure that the framework adapts to the threat environment and guarantees adaptive intelligence. The operational environments are the spheres where AI can not only help to speed up the process of detection but also improve the level of analytical accuracy by revealing the correlation between seemingly unrelated events. Combined with STIX/TAXII and MITRE ATT&CK, machine learning can help make decisions based on context without considering only technical indicators but also on adversarial behaviors. In national cyber defense, the same flexibility is understood as proactive resilience, systems are able to forecast and act upon threats before they get out of control. These conclusions emphasize the fact that AI integration with structured intelligence is not only arousal but a tactical need to handle massive, intricate, and fluid cyber ecologies in an effective, self-sufficient manner.

F. *Strategic, Policy and Operational Implications*

The deployment of autonomous threat intelligence and decision infrastructures have substantial strategic and policy-level implications to national cybersecurity. Politically it is advisable to implement common programming like STIX/TAXII in order to support interoperability, transparency and sharing of intelligence between government agencies, defense entities and private sectors. Such standardization increases trust and cooperation and turns the systems of isolated existence into a national system of defense. The research is strategically placed to strengthen the need of automation in ensuring cyber resilience. Having autonomous systems with AI-powered analytics will significantly decrease the amount of human labor, remove delays in responding, and ensure constant vigilance [59]. These features are essential in the protection of critical areas of infrastructure like energy, transport, finance, and defense where cyber-attacks can have ripple effects on the stability of the nation. Operational the results justify the inclusion of human-in-the-loop to strike a balance between autonomy and responsibility. Although automation is faster and more scalable, human control offers moral control and background judgment to handle important decisions. Informed by autonomous systems, future cybersecurity policy development, resource distribution, and risk reduction plans can be made at the national level. In the end, this study shows that autonomous threat intelligence infrastructures are an innovation not only in technology but also in strategy. Such frameworks can allow countries to develop proactive cyber deterrence as well as create resilient, adaptive, and collaborative defense postures against more advanced adversaries by closing the gap between policy, technology and operations.

VIII. Future Work

Although this study has managed to design and test a self-managed threat intelligence aggregation and decision-making model that works with national cyber defense, there are still some gaps to be filled in the future in order to improve system scalability, naturalness, and interoperability. The integration of federated learning and distributed AI models into various national and international defense networks is one of the prominent perspectives of future work. This would enable sharing of intelligence and model training without data sharing and still keeping confidential information, and enhancing the international perception of the emerging threats. This would also facilitate real-time learning of geographically dispersed cyber events, which would enhance the global situational awareness and coordination of response. Also, more sophisticated temporal and relational dependencies between the entities of attack can be added to the future implementations to include deep learning and graph-based reasoning. Graph Neural Networks (GNNs) architectures, as well as Long Short-Term Memory (LSTM), may further improve the detection of stealthy and multi-stage attacks by the time-dependent modeling of adversarial behavior patterns [60]. Incorporation of natural language processing (NLP) may also enhance derivation of intelligence on unstructured materials like incident reports, forums and open-source intelligence feeds. The other important avenue is the development of explainable AI (XAI) mechanisms in the paradigm. The transparency and interpretability of the national defense systems are a requirement to have automated decisions which are not only auditable but also ethically liable. This would help security analysts and policymakers to have faith and confirm the logic behind AI-based threat assessments and reactions. Operationally, the future research effort should aim at implementing the framework in actual situations of national cyber command to determine its functionalities during live network operations. The connectivity to critical sectors of infrastructure will challenge the resilience, scalability, and a high accuracy of response of the system. Lastly, policy-oriented extensions may be experimented with the design of AI governance methods that allow assurance of ethical application, privacy, and standards of international cooperation of autonomous cyber defense systems- developing not only technical capacity but also nationally and internationally strategic cybersecurity policy.

IX. Conclusion

This study conducted the design, development and evaluation of an Autonomous Threat Intelligence Aggregation and Decision Infrastructure that would enhance national cyber defense capabilities. The research has dealt with the weaknesses of the conventional, manually operated cybersecurity systems by proposing an AI-based, data-centric framework with the ability to detect in real-time, correlate intelligence, and make decisions automatically. The proposed system was demonstrated to be capable of identifying, classifying, and responding to a wide variety of cyber threats effectively and autonomously, through the integration of machine learning models, structured threat intelligence standards (STIX/TAXII), and contextual mapping based on MITRE ATT&CK framework. The validation of the framework in real network conditions, including frequent and infrequent types of attacks, was made possible by using the UNSW-NB15 dataset. The findings indicated that the accuracy of the Random Forest model was better in the detection and classification of attacks, which validates the feasibility of machine learning to be used in adaptive defense systems. The conversion of the raw threat information into formatted intelligence items also improved the interoperability and real-time intelligence sharing among the national security networks. The results also highlighted the issue of independent intelligence consolidation in the attainment of situational awareness and quick reaction. The system minimizes the response latency by minimizing the human dependency and increasing the accuracy of the analysis, which boosts the resilience of the system. In addition, the use of automated decision logic also provides continuous learning and adaptation, which is in line with the changing complexity of contemporary cyber warfare. This study is also a contribution to the increasing literature on AI-based national cyber defense, as it offers a generalizable framework on how to adapt autonomy, intelligence, and interoperability into security systems. In addition to its technical accomplishments, the structure has strategic implications on policymaking especially in promoting collaboration, trust and standardization within agencies. Finally, this work shows that autonomous threat intelligence and decision infrastructures are not only the technical innovations but the strategic requirements, providing countries with a proactive, adaptive, and sustainable way to protect the digital sovereignty and critical assets against the constantly new cyber threats.

Reference

[1]. Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security, 132, 103352.

[2]. Sindiramutty, S. R. (2023). Autonomous threat hunting: A future paradigm for AI-driven threat intelligence. arXiv preprint arXiv:2401.00286.

[3]. Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys & Tutorials, 25(3), 1748-1774.

[4]. Amro, A., & Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. International Journal of Information Security, 22(1), 249-288.

[5]. Raptis, G. E., Katsini, C., Alexakos, C., Kalogeras, A., & Serpanos, D. (2022). Cavectir: Matching cyber threat intelligence reports on connected and autonomous vehicles using machine learning. Applied Sciences, 12(22), 11631.

[6]. Richard, H., Andrewson, S., & Noel, D. (2023). Building National Resilience with Integrated AI Surveillance and Cyber Threat Intelligence.

[7]. Pemmasani, P. K. (2023). AI in National Security: Leveraging Machine Learning for Threat Intelligence and Response. The Computertech, 1-10.

[8]. Lohn, A., Knack, A., Burke, A., & Jackson, K. (2023). Autonomous Cyber Defense. A roadmap from lab to ops. Online. Centre for Emerging Technology and Security (CETaS) at The Alan Turing Institute.

[9]. Lee, M. (2023). Cyber threat intelligence. John Wiley & Sons.

[10]. Möller, D. P. (2023). Threats and threat intelligence. In Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices (pp. 71-129). Cham: Springer Nature Switzerland.

[11]. Ahmed, I., Mia, R., & Shakil, N. A. F. (2023). Mapping blockchain and data science to the cyber threat intelligence lifecycle: Collection, processing, analysis, and dissemination. Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems, 13(3), 1-37.

[12]. de Oca, E. M., Armin, J., & Consoli, A. (2022). Cyber-threat intelligence from European-wide sensor network in SISSDEN. In Challenges in Cybersecurity and Privacy-the European Research Landscape (pp. 117-128). River Publishers.

[13]. Evans, C. V., Anderson, C., Baker, M., Bearse, R., Biçakci, S., Bieber, S., ... & Verner, D. (2022). Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1). Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press.

[14]. Maharjan, P. (2023). The role of artificial intelligence-driven big data analytics in strengthening cybersecurity frameworks for critical infrastructure. Global Research Perspectives on Cybersecurity Governance, Policy, and Management, 7(11), 12-25.

[15].Knowledge, C. Administrative control considerations 206 Advanced persistent threat (APT) 50, 237 Adversary models 271. Artificial intelligence (AI), 11, 100.

[16]. Hagos, D. H., & Rawat, D. B. (2022). Recent advances in artificial intelligence and tactical autonomy: Current status, challenges, and perspectives. Sensors, 22(24), 9916.

[17]. Ofili, B. T., Obasuyi, O. T., & Akano, T. D. (2023). Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience. Int J Comput Appl Technol Res, 12(9), 17-31.

[18]. Walker, E., Martinez, M., Umeh, I., & Abbas, F. (2022). Nationwide Cyber Vigilance: AI-Powered Risk Management in Public Networks.

[19]. Sufi, F. (2023). A new social media-driven cyber threat intelligence. Electronics, 12(5), 1242.

[20]. Timilehin, O. (2023). Defending the Digital Horizon: Artificial Intelligence in Cybersecurity Warfare.

[21]. Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S., & Rizwan, M. (2023). Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. Expert Systems, 40(5), e13103.

[22]. Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., & Raza, A. (2023). Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. Technologies, 11(5), 117.

[23]. Rajuroy, A. (2022). Advanced Accounting Systems as Strategic Assets in National Financial Cyber Defense.

[24]. Hossain, M. D., Sikder, M. S., Uddin, M. S., Ahsan, R. M., Uddin, B., & Hossen, T. (2023). Cognitive Cyber Defense: AI–MIS Integration through Big Data and Cloud Frameworks for Next-Generation Digital Resilience. The Eastasouth Journal of Information System and Computer Science, 1(02), 140-152.

[25]. Reinhold, T., & Reuter, C. (2022). Cyber weapons and artificial intelligence: impact, influence and the challenges for arms control. In Armament, Arms Control and Artificial Intelligence: The Janus-faced Nature of Machine Learning in the Military Realm (pp. 145-158). Cham: Springer International Publishing.

[26]. Obuse, E., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Babatunde, L. A. (2023). AI-powered incident response automation in critical infrastructure protection. International Journal of Advanced Multidisciplinary Research Studies, 3(1), 1156-1171.

[27]. Patel, P., & Salave, A. P. (2023, December). AI-Driven Cybersecurity Framework for Next-Gen Computing Applications and Critical Infrastructure. In ECCSUBMIT Conferences (Vol. 1, No. 1, pp. 1-10).

[28]. Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., ... & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), 493-543.

[29]. Mern, J., Hatch, K., Silva, R., Hickert, C., Sookoor, T., & Kochenderfer, M. J. (2022, June). Autonomous attack mitigation for industrial control systems. In 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W) (pp. 28-36). IEEE.

[30]. Panda, S., Rass, S., Moschoyiannis, S., Liang, K., Loukas, G., & Panaousis, E. (2022). Honeycar: a framework to configure honeypot vulnerabilities on the internet of vehicles. Ieee Access, 10, 104671-104685.

[31]. Onwubiko, C., & Ouazzane, K. (2022). Challenges towards building an effective cyber security operations centre. arXiv preprint arXiv:2202.03691.

[32]. Flammini, F., Alcaraz, C., Bellini, E., Marrone, S., Lopez, J., & Bondavalli, A. (2022). Towards trustworthy autonomous systems: Taxonomies and future perspectives. IEEE Transactions on Emerging Topics in Computing, 12(2), 601-614.

[33]. Langeh, A., & Sudhakar, R. (2023). Artificial Intelligence and Cyber Security: Transformative Synergies in the Digital Frontier.

[34]. Alsmadi, I. (2023). Cyber intelligence analysis. In The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics (pp. 85-129). Cham: Springer International Publishing.

[35]. Repetto, M. (2023). Adaptive monitoring, detection, and response for agile digital service chains. Computers & Security, 132, 103343.

[36]. Iturbe, E., Rios, E., Rego, A., & Toledo, N. (2023, August). Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-8).

[37]. Al-Hawawreh, M., & Hossain, M. S. (2023). Federated learning-assisted distributed intrusion detection using mesh satellite nets for autonomous vehicle protection. IEEE Transactions on Consumer Electronics, 70(1), 854-862.

[38]. Ademilua, D. A., & Areghan, E. (2022). AI-Driven Cloud Security Frameworks: Techniques, Challenges, and Lessons from Case Studies. Communication in Physical Sciences, 8(4), 684-696.

[39]. Michalec, O., Milyaeva, S., & Rashid, A. (2022). When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?. Big Data & Society, 9(1), 20539517221108369.

[40]. Owolabi, B. O. (2023). Advancing Predictive Analytics and Machine Learning Models to Detect, Mitigate, and Prevent Cyber Threats Targeting Healthcare Information Infrastructures. Int J Sci Eng Appl, 12(12), 76-87.

[41]. Deveci, M., Pamucar, D., Gokasar, I., Köppen, M., & Gupta, B. B. (2022). Personal mobility in metaverse with autonomous vehicles using Q-rung orthopair fuzzy sets based OPA-RAFSI model. IEEE Transactions on Intelligent Transportation Systems, 24(12), 15642-15651.

[42]. Idika, C. N., James, U. U., Ijiga, O. M., & Enyejo, L. A. (2023). Digital Twin-Enabled Vulnerability Assessment with Zero Trust Policy Enforcement in Smart Manufacturing Cyber-Physical System International Journal of Scientific Research in Computer Science. Engineering and Information Technology, 9(6).

[43]. Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2023). AI-powered cyber-physical security framework for critical industrial IoT systems. Machine learning, 27, 1158-1164.

[44]. Naseer, I. (2023). Machine learning applications in cyber threat intelligence: a comprehensive review. The Asian Bulletin of Big Data Management, 3(2), 190-200.

[45]. Owolabi, B. O. (2022). Exploring systemic vulnerabilities in healthcare digital ecosystems through risk modeling, threat intelligence, and adaptive security control mechanisms. Int J Comput Appl Technol Res, 11(12), 687-99.

[46]. Moore, C. (2023). AI-powered big data and ERP systems for autonomous detection of cybersecurity vulnerabilities. Nanotechnology Perceptions, 19, 46-64.

[47]. Yavuz, A. A., Nouma, S. E., Hoang, T., Earl, D., & Packard, S. (2022, December). Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era. In 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 29-38). IEEE.

[48]. Al Zaiem, A., & Shan-A-Alahi, A. (2023). AI-Enhanced Cybersecurity and Management Information Systems: Integrating Big Data, Cloud Computing, and Agile IT Frameworks for Digital Resilience. Journal of Computer Science and Technology Studies, 5(4), 275-284.

[49]. Joyner, M. A. (2022). Strategies Using Threat Intelligence to Detect Advanced Persistent Threats: A Qualitative Case Study (Doctoral dissertation, Walden University).

[50]Vevera, A. V., Cirnu, C. E., & Radulescu, C. Z. (2022). A Multi-Attribute approach for cyber threat intelligence product and services selection. Studies in Informatics and Control, 31(1), 13-23.

[51]. Alguliyev, R., Nabiyev, B., & Dashdamirova, K. (2023, August). CTI Challenges and Perspectives as a Comprehensive Approach to Cyber Resilience. In 2023 5th International Conference on Problems of Cybernetics and Informatics (PCI) (pp. 1-5). IEEE.

[52]. Llopis Sánchez, S. (2023). Decision support elements and enabling techniques to achieve a cyber defence situational awareness capability (Doctoral dissertation, Universitat Politècnica de València).

[53]. Bukhari, T. T., Moyo, T. M., Tafirenyika, S., Taiwo, A. E., Tuboalabo, A., & Ajayi, A. E. (2022). AI-Driven Cybersecurity Intelligence Dashboards for Threat Prevention and Forensics in Regulated Business Sectors.

[54]. Rios, E., Iturbe, E., Rego, A., Ferry, N., Tigli, J. Y., Lavirotte, S., ... & Cavalli, A. R. (2023, August). The DYNABIC approach to resilience of critical infrastructures. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-8).

[55]. Ejeofobiri, C. K., Adelere, M. A., & Shonubi, J. A. (2022). Developing adaptive cybersecurity architectures using Zero Trust models and AI-powered threat detection algorithms. Int J Comput Appl Technol Res, 11(12), 607-621.

[56]. Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in IoT-enabled maritime industry. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2677-2690.

[57]. Han, J., Ju, Z., Chen, X., Yang, M., Zhang, H., & Huai, R. (2023). Secure operations of connected and autonomous vehicles. IEEE Transactions on Intelligent Vehicles, 8(11), 4484-4497.

[58]. Mahmoodi, A. B. Z., Sheikhi, S., Peltonen, E., & Kostakos, P. (2023). Autonomous federated learning for distributed intrusion detection systems in public networks. IEEE access, 11, 121325-121339.

[59].Van Hoang, N. (2023). Human expertise and machine learning in collaborative intelligence frameworks for robust cybersecurity solutions. Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems, 13(12), 1-12.

[60]Biswas, A., & Wang, H. C. (2023). Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. Sensors, 23(4), 1963.

[61]. Dataset Link
https://www.kaggle.com/datasets/alextamboli/unsw-nb15