


# OSINTEP: A Tool for Cyber Defense in the Peruvian Army

Luis Flores Méndez, Eng<sup>1</sup>; Manuel Vargas Zubiarte, Eng<sup>1</sup>; Carlos Quinto Huamán, PhD<sup>2</sup>; Sonia Lidia Romero Vela, PhD<sup>1</sup>; and Percy Fortunato Ochoa Castillo, PhD<sup>1</sup>

<sup>1</sup>Grupo de Investigación en Ciberseguridad, IoT e Inteligencia Artificial (GriCIA), Instituto Científico y Tecnológico del Ejército, Lima, Perú, [lfloresm@icte.edu.pe](mailto:lfloresm@icte.edu.pe), [mvargasz@icte.edu.pe](mailto:mvargasz@icte.edu.pe), [sromerov@icte.edu.pe](mailto:sromerov@icte.edu.pe), [pochoac@icte.edu.pe](mailto:pochoac@icte.edu.pe)

<sup>2</sup>Universidad Privada del Norte, Lima, Perú, [carlos.quinto@upn.pe](mailto:carlos.quinto@upn.pe)

**Abstract**– *Open-Source Intelligence (OSINT) plays a crucial role in cybersecurity by enabling the collection and analysis of publicly available information to detect emerging threats. The Peruvian Army (EP) faces a significant challenge in relying on commercial tools that are not fully adapted to its specific operational needs, limiting their effectiveness in addressing the ever-evolving cyber threats. To bridge this gap, this paper proposes the development of OSINT EP, a customized solution designed specifically to enhance the EP's response capabilities to cybersecurity challenges. The OSINT EP tool integrates several APIs, such as X API, IPinfo.io, NewsAPI, and LookupClient, to perform real-time data analysis and detect threats from various sources. The OSINT EP tool enabled the identification of cyber threats through multiple APIs. The X API revealed an increase in mentions regarding vulnerabilities on social media, suggesting a greater public interest. The IP analysis with IPinfo.io detected an address linked to a known attack in Peru, recommending its blocking. NewsAPI identified incidents of cyberattacks on critical infrastructures, which led to alerts being issued to the authorities. Finally, the DNS analysis with LookupClient verified the security of an email server, recommending periodic security audits.*

**Keywords:** *Open-Source Intelligence, Cyber Defense, Information Analysis, Strategic Technology*

## I. INTRODUCTION

In today's digital era, information has become one of the most valuable strategic assets. It is essential for national security, supports critical decision-making processes, and enhances situational awareness. Within this framework, Open-Source Intelligence (OSINT) has emerged as a key discipline that enables organizations to systematically collect, analyze, and interpret publicly available data from a wide range of sources, including the internet, news outlets, public records, and social media platforms. Although OSINT does not rely on classified information, it requires advanced techniques to ensure the accuracy, relevance, and contextual understanding of the data it processes.

Recent studies suggest that around 90 percent of the intelligence used in current security operations is derived from open sources, highlighting the growing significance of OSINT across both civilian and military sectors [1], [2]. This importance is further emphasized by the exponential increase in publicly accessible digital information, which is estimated to double approximately every two years. Such rapid growth

presents both opportunities for enhanced insight and challenges for effective data management and analysis.

One of the most well-known tools supporting OSINT is the OSINT Framework. This resource compiles a wide selection of free tools designed to assist in the various stages of intelligence work. While some tools may offer premium options or require registration, most are freely accessible and serve essential functions in data collection and analysis. Originally created for cybersecurity purposes, the framework has since been adopted in areas such as investigative journalism, law enforcement, humanitarian action, and military operations [1].

The strategic value of OSINT became increasingly evident following the terrorist attacks of September 11, 2001, which led both the United States and NATO to formally incorporate OSINT into their intelligence strategies. Non-state actors such as Al Qaeda, the Taliban, Hezbollah, and Hamas began using the internet extensively for communication, recruitment, and propaganda. In response, OSINT evolved to become a fundamental element of modern intelligence, complementing traditional methods such as Human Intelligence (HUMINT) and Technical Intelligence (TECHINT) [3].

Despite these global developments, many Latin American military institutions still face critical limitations in OSINT capacity. For example, the Peruvian Army currently depends on commercial software tools that are expensive and not fully aligned with its operational requirements. This reliance limits its responsiveness to cyber threats, which have intensified across the region, with an average of 15 daily attacks on critical infrastructure [4]. Furthermore, the use of foreign platforms raises concerns about data security, technological sovereignty, and long-term sustainability.

In response to this strategic gap, the present research proposes the design and development of OSINT-EP, a specialized platform tailored to the specific operational and doctrinal needs of the Peruvian Army. The system aims to enhance the autonomous capability to collect and analyze open data, improve cyber defense readiness, and reduce dependency on foreign technologies. In addition to its technological objectives, the initiative seeks to promote a broader institutional transformation by embedding OSINT into the Army's intelligence structure and contributing to a more resilient and adaptive national defense posture.

This work is structured as follows: Section 1 introduces the topic; Section 2 presents fundamental concepts related to OSINT tools; Section 3 reviews related work; Section 4 outlines the proposed method; Section 5 describes the experiments conducted and analyzes the results obtained; and Section 6 provides conclusions and contributions of the work.

## II. OVERVIEW OF OSINT TOOLS

OSINT tools are a set of techniques and tools used to collect public information, analyze data, and relate them to convert them into useful knowledge. They are used in various fields such as finance, technology, law enforcement, marketing, etc., allowing access to all available information from any public source about a company, individual, or anything we want to investigate.

The history of OSINT dates back to World War II [5], when the governments of the United States and the United Kingdom began collecting publicly available information potentially relevant to national security and defense. The United States pioneered the creation of an autonomous capability to monitor and analyze foreign media with the establishment of the Foreign Broadcast Monitoring Service (FBMS) in 1941. In the United Kingdom, the BBC launched a similar program known as Digest of Foreign Broadcasts. Over time, these initiatives evolved into strategic and complex tools for collecting and interpreting information from public sources. OSINT has continued to evolve with the rise of technology and the information available on the internet, becoming an important field for national security and criminal investigation. With the increase in the use of the internet and social media, OSINT has become increasingly important in information gathering. Today, OSINT professionals use a variety of tools and techniques to collect information from online sources, such as search engines, social networks, and news websites.

### A. OSINT Cycle

The intelligence cycle is what allows us to transform raw data into the knowledge we aim to obtain [6]. According to [7], the intelligence cycle can be divided into 5 stages, as shown in Figure 1.

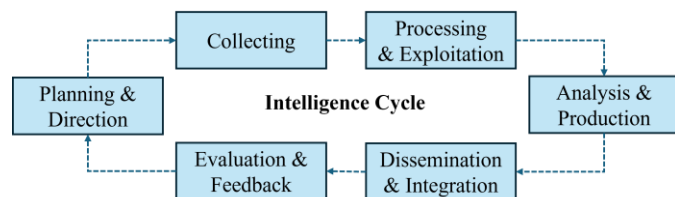


Fig. 1 OSINT Workflow Cycle

*A.1. Planning and Direction:* This initial phase establishes the objectives and intelligence requirements, setting the foundation for the subsequent stages of the cycle. It also appears at the end, as the finalized intelligence informs and

shapes future planning based on the end-user’s evolving needs.

*A.2. Collecting:* This stage involves gathering raw data from a wide variety of sources, such as social media, forums, public documents, and interviews, which serve as the foundation for intelligence production. While actors in the private sector often adopt broad and flexible collection strategies, public agencies usually concentrate on more narrowly defined targets.

*A.3. Processing and Exploitation:* This phase transforms collected data into structured formats suitable for analysis. It includes organizing, categorizing, and, when necessary, digitizing analog information to ensure analytical readiness.

*A.4. Analysis and Production:* Analysts assess the reliability, validity, timeliness, and relevance of the processed data, integrating it into coherent and actionable intelligence products. These outputs provide insights, breakdowns of relevant events, and potential implications for decision-makers.

*A.5. Dissemination and Integration:* Once intelligence has been produced, it must be effectively communicated to the end-users, often in the form of reports, briefings, or presentations. This stage typically triggers feedback, which can serve as the starting point for a new intelligence cycle.

*A.6. Evaluation and Feedback:* Post-delivery, continued engagement with the client is essential. Analysts must assess how well the intelligence met user requirements and identify any gaps or improvements needed. This iterative feedback loop helps enhance analytical processes and user satisfaction over time.

OSINT is used to conduct investigations effectively, focusing these investigations on various objectives such as: (a) identifying and preventing potential threats in the military or national security sectors, (b) locating and tracking individuals, (c) assessing the online reputation of a company or specific user, (d) conducting sociological, psychological, or linguistic studies, (e) performing audits on companies and organizations to evaluate their level of privacy and security, (f) gathering documentation for journalistic use, (g) collecting information for investigative purposes, (h) evaluating market trends, and (i) conducting market analysis for launching marketing campaigns [8].

### B. OSINT Tools

Due to the vast amount of publicly available information, it is often impractical to manually collect, categorize, and analyze OSINT data. Specialized open-source intelligence tools can assist in managing and automating data tasks for various OSINT use cases. According to [8], there are several tools that can be highly useful when conducting OSINT research, offering numerous possibilities, such as: (a) Shodan, (b) Google Dorks, (c) Bing Dorks, (d) Maltego, (e) NexVision, and (f) Social Links. Table 1 describes six tools commonly used in OSINT research.

TABLE I  
DESCRIPTIONS OF COMMON OSINT TOOLS

Tool Level	Description
Shodan	A search engine that helps users identify specific types of devices (e.g., routers, servers) connected to the internet via various filters. It also functions as a banner search engine, retrieving metadata such as server software details, supported options, or welcome messages before server interaction [9].
Google Dorks	Refers to the advanced search technique using Google to find sensitive, unprotected information left online. Known as Google Hacking, it is crucial in military and strategic sectors for uncovering security flaws. It helps locate confidential data like passwords or vulnerable system files that should not be publicly available [10].
Bing Dorks	Similar to Google Dorks, but with different options and features that may yield different search results.
Maltego	An open-source intelligence and forensics tool developed by Paterva. It offers a variety of transformations for discovering and visualizing data from open sources, focusing on analyzing real-world relationships between entities such as people, groups, websites, and networks. It allows custom entity creation for broader data representation [11].
NexVision	An AI-powered tool that delivers real-time insights from across the web, including dark web searches. It helps find valuable information on individuals and organizations, with filtering options to refine results for specific queries [12].

### III. STATE OF THE ART

Open-Source Intelligence is widely used in cybersecurity and defense to analyze public information and detect threats. Various tools have demonstrated their usefulness in military and strategic sectors, establishing the foundations for the development of solutions tailored to specific needs.

The interest in collecting OSINT, building databases, and analyzing social media information is growing. The areas of application for OSINT in gathering information from social networks include the following: (a) Intelligence for collecting OSINT information and secondary analysis of published information is used to understand significant threats to security, terrorism, and cyberterrorism. In OSINT, data mining, statistical analysis, location analysis, network analysis, and time series pattern analysis are important [14]. (b) Background checks on social media and profiles of specific individuals or groups. Recently, activities are mainly carried out in cyberspace, making it more likely to gather information about the characteristics, history, and trends of specific individuals and organizations in the online space than in the offline space [15]. (c) Criminal investigations: This is an online activity used to gather criminal evidence. Unlike digital forensics investigations, it includes information about online witnesses and testimonies [16].

In [17], the authors analyzed the effectiveness of OSINT in dealing with military information leakage through social networks, investigated the collection of OSINT data at the Institute for the Study of Violent Groups (ISVG) and the Study of Terrorism and Responses to Terrorism (START) in

the field of terrorism. Additionally, the characteristics of the Cyber Threat Analysis and Sharing (C-TAS) in Korea were analyzed through a research survey on cyber threat information collected from social networks in response to cyberterrorism.

The ISVG program in the United States is a research project that uses federal research funds to create databases related to terrorism. ISVG is responsible for the College of Criminal Justice at Sam Houston State University. The ISVG program uses OSINT information that can be collected from SNS (Social Networking Services) to create a database of information about terrorist organizations and significant terrorists worldwide. Since 2004, more than 150,000 databases about terrorists have been created. As seen in Figure 2, the ISVG database at Sam Houston State University in the U.S. consists of a series of incident identification numbers that collect OSINT information from various social networks about related events, people, and organizations. Therefore, it is possible to obtain complete information about incidents by searching for specific terrorist events, people, and organizations [18].

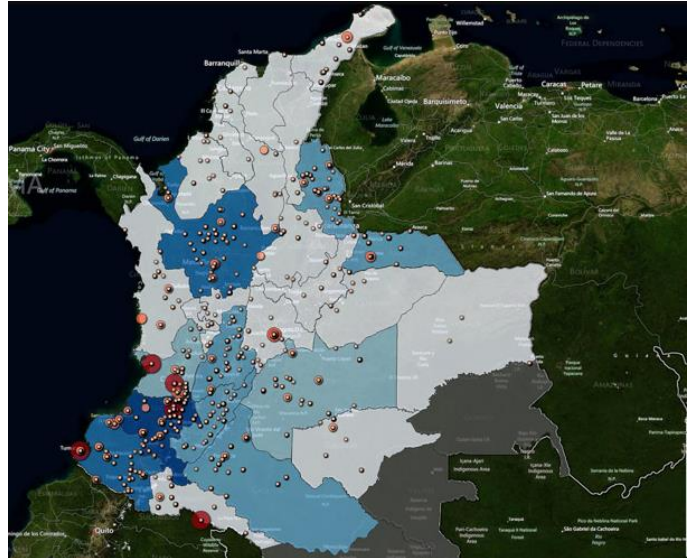


Fig. 2 ISVG database of Sam Houston State University

START is a program supported by the U.S. Department of Homeland Security and is being studied by the University of Maryland to collect and analyze information on terrorism. As shown in Figure 3, START creates a variety of databases, but one of its most notable contributions is the Global Terrorism Database (GTD), which focuses on documenting and analyzing terrorist attacks worldwide. The GTD collects data not only from traditional intelligence sources but also actively monitors social media platforms through Open-Source Intelligence (OSINT) methods, enhancing its ability to capture real-time data and insights from global incidents. This inclusion of social media allows for the rapid identification of emerging threats and trends within the context of terrorism.

The database aggregates comprehensive information on terrorist attacks across the globe, including specifics on the incidents, types of attacks, weapons used, and damages incurred, providing a holistic view of the evolving landscape of global terrorism [19]. Furthermore, the GTD systematically compiles data on terrorist incidents globally and has amassed over 110,000 data entries to date, making it one of the most extensive databases of its kind. For each terrorist event, the GTD offers detailed information such as the date, location, weapons used, the nature of the terrorist group or individual, the number of victims, and additional identifying details related to the perpetrators. This database plays a crucial role in shaping global counterterrorism strategies and policies by providing accessible, open-source data for analysis.

The GTD is publicly accessible on the Internet, providing valuable resources for researchers, policymakers, and organizations involved in counterterrorism efforts. It allows anyone to browse the data, conduct detailed research, and gain insights into the patterns and tactics used in terrorist activities, thereby contributing to a more informed and strategic approach to global security [20].

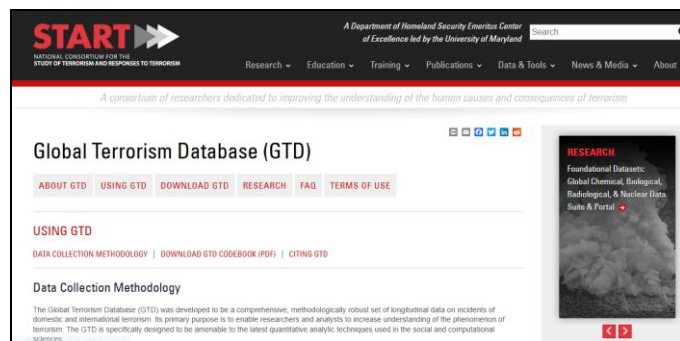


Fig. 3 Global Terrorism Database (GTD)

The Korea Internet and Security Agency (KISA) has rolled out an innovative platform called Cyber Threat Analysis and Sharing (C-TAS) to streamline the exchange of cyber threat intelligence. This solution facilitates the distribution of a wide range of data including IP addresses associated with threats, malware signatures, vulnerabilities, and additional information supplied by certified agencies (see Figure 4). Operating under the umbrella of Cyber Threat Intelligence (CTI), the system is organized into two main segments: Threat Intelligence Service (TIS) and Threat Intelligence Platform (TIP), each available as either an independent service or an integrated platform [21]. FireEye’s iSIGHT Intelligence delivers CTI solutions through multiple layers by harnessing APIs and online data sources. These offerings are critical for tracking cyber adversaries, detailing their profiles, analyzing their development environments, and addressing various security issues [22]. Symantec’s DeepSight™ intelligence contributes by generating vital reputation metrics and providing thorough analyses of major incidents linked to threat indicators. It aggregates essential details such as domain

records, URLs, IP reputation, malware history, regional data, industry-specific insights, ownership information, and behavioral trends [23]. Meanwhile, IBM bolsters cybersecurity efforts by offering threat intelligence services and products via its IBM i2 platform. This service has been further advanced through the integration of Watson technology, thereby enhancing the overall robustness of its cybersecurity operations [24].

Finally, reference [25] presents a state-of-the-art analysis of the challenges and opportunities faced by the Peruvian Army in adopting automated tools, including those based on artificial intelligence. The study highlights the need for systems such as Enhanced Military Intelligence (IMME), aimed at improving the collection, analysis, and processing of intelligence information from various sources. Among the proposed capabilities is the implementation of robust Open-Source Intelligence (OSINT) tools designed exclusively for the Army's Directorate of Intelligence, with interfaces that allow for decentralized data distribution and consumption. Additionally, the study suggests the application of advanced techniques such as Federated Learning. This analysis underscores the importance of developing specialized OSINT tools to strengthen the institutional security of the Peruvian Army.

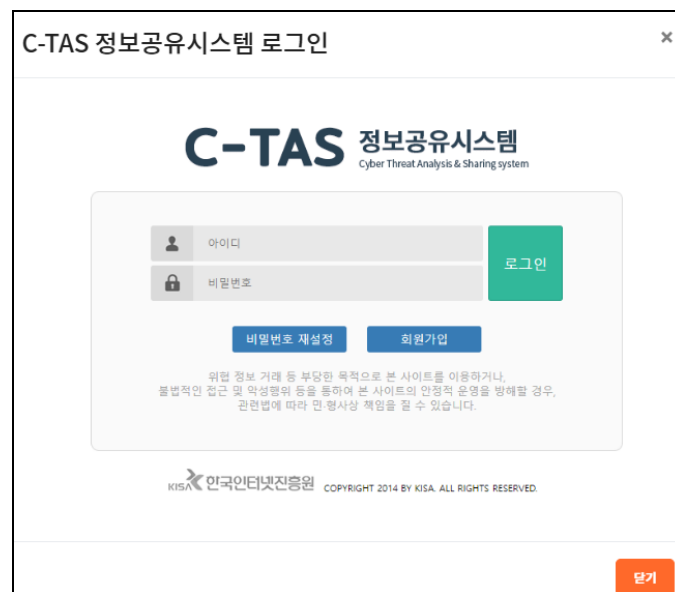


Fig. 4 KISA C-TAS Database of Korea

#### IV. DEVELOPMENT OF THE PROPOSAL

In this work, we present the development of OSINTEP, designed for the Peruvian Army, with the aim of establishing a solid foundation for future improvements and advanced implementations. This tool provides the necessary capabilities for OSINT operations. Defining the minimum software and hardware requirements is crucial to ensure the proper

functioning and scalability of OSINTEP, especially considering the operational needs of the Peruvian Army. These requirements have been carefully selected to guarantee a stable and efficient development environment, meeting the demands of the defense sector and ensuring the ability to process real-time data. Table 2 presents the minimum requirements for the development and deployment of OSINTEP, aligned with the strategic needs of the Army and designed to provide a solid technological foundation for both current and future implementations within the defense sector.

TABLE II  
MINIMUM REQUIREMENTS FOR THE DEVELOPMENT AND DEPLOYMENT OF OSINTEP

Component	Description
Programming Language	C#
Development Environment	Visual Studio .NET 2019 Professional
Framework	.NET Framework 4.7.2
Operating System	Windows 10 or later
Libraries and Components	DevExpress 24.1.7
Hardware Requirements	Processor: i5 or higher RAM: 8 GB or more Disk Space: 10 GB free
Connectivity	Internet connection for updates and external resources

A. Phases for the Development of the OSINTEP Tool

OSINTEP undergoes a structured process consisting of several phases. These allow for the collection, analysis, and presentation of information obtained from various sources in an efficient and organized manner. In Figure 5, the main phases that characterize this scanning system are carried out.

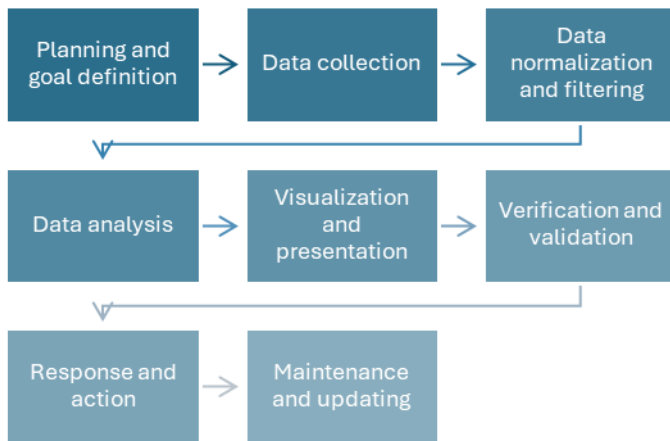


Fig. 5 Phases of OSINTEP

A.1. *Planning and goal definition*: Define what will be searched and from which sources: This phase involves i) objective definition, where the information to be obtained is

established, such as vulnerabilities, IP addresses, information about people or companies; ii) selection of information sources, defining open data sources such as social media, public databases, forums, websites, search engines, third-party APIs; iii) scope of the scan, delimiting the data collection scope.

A.2. *Data Collection*: Obtain data from various open sources defined in the previous phase, performing i) web scraping to extract data, using web scraping tools and techniques, querying public databases, third-party APIs. Some sources may include search engines (e.g., Google, Bing), social media (e.g., X, LinkedIn, Facebook), government portals, and public records, as well as threat databases (e.g., VirusTotal, Shodan, Censys); ii) automation by using scripts and automated tools for efficient, large-scale data collection.

A.3. *Data normalization and filtering*: Once the data has been collected, it is necessary to process it for analysis, ensuring i) information filtering by removing irrelevant or redundant data; ii) data normalization, especially for data extracted from different sources, which may be in disparate formats (JSON, XML, CSV, plain text). In this phase, the data is transformed into a structured format to facilitate subsequent analysis.

A.4. *Data analysis*: The scanning system performs analysis to identify patterns or relevant information, executing i) manual and automated analysis depending on complexity, involving both manual and automated techniques. Automated analysis can include a) pattern analysis to identify behaviors or relationships between data, b) threat recognition in OSINT scans directed at cybersecurity to identify potential vulnerabilities, security exposures, compromised IP addresses, malicious domains, c) data correlation with information obtained from different sources to discover new connections between seemingly unrelated data. Additionally, ii) identification of key actors in cases of investigations about people or entities, their relationships, and their influence.

A.5. *Visualization and presentation*: The visualization and presentation phase focuses on displaying the results clearly and understandably. Interactive dashboards are used to visualize large volumes of data in real-time, facilitating interpretation and effective tracking of information. Additionally, alerts and automatic notifications are configured to inform about detected events or patterns, such as the identification of vulnerabilities or suspicious activity. Integration with social media platforms, using APIs from platforms like X and Facebook, enables the collection and presentation of real-time results related to specific keywords, facilitating active monitoring and analysis of relevant trends and behaviors.

A.6. *Verification and validation*: Ensure the accuracy and reliability of the results by performing i) data verification through a cross-checking process with other sources to validate the findings; ii) validation of conclusions to verify whether the conclusions obtained from the analysis are consistent with the objectives established at the beginning of the process.

*A.7. Response and action:* This phase involves making decisions based on the results of the scan, which may include i) corrective actions by recommending actions to mitigate identified risks (e.g., security patches, configuration changes, etc.); ii) alerting stakeholders, generating alerts for researchers or entities interested in the collected information; iii) feedback, which can be used to adjust parameters for future investigations or scans, such as refining sources or the data collection methodology.

*A.8. Maintenance and updating:* Finally, due to the dynamic nature of OSINT data (websites, social media, public records, etc.), it is important to maintain the system continuously by i) periodic source updates to ensure the system has access to current data; ii) continuous improvement to ensure the system's accuracy and efficiency.

### B. Development of the OSINTEP Tool

The development of the OSINTEP tool was carried out using the Visual Studio .NET 2019 development environment, employing the C# programming language and the .NET Framework 4.7.2. This environment provided a solid platform for code development and debugging, ensuring efficient and scalable system performance. For the user interface, DevExpress 24.1.7 was used, a suite of components that allowed designing a modern and intuitive interface, facilitating user interaction with the system and improving the overall user experience. It is important to mention that the software integrates basic functionality through the consumption of various external APIs:

- X API: Provides access to real-time social media data, allowing the collection of information such as recent posts, mentions, hashtags, user data (name, location, profile picture), and tweet dates. This API is useful for detecting trends, analyzing social interactions, and monitoring relevant activities to identify potential threats or disinformation campaigns.
- IPinfo.io API: Allows detailed IP address searches, providing key information such as hostname, city, region, country, geographic coordinates, associated organization, postal code, and time zone. This tool facilitates the analysis of geospatial patterns and the identification of potentially compromised sources, being essential for risk assessment and strengthening cybersecurity.
- NewsAPI: Collects updated news from multiple online sources, offering data such as the title, description, access URL, and publication date. This enables content analysis to identify relevant topics, detect fake news, and better understand the real-time informational environment, contributing to strategic decision-making based on reliable information.

Additionally, the use of the LookupClient library has been implemented, a tool specialized in DNS queries, to perform MX (Mail Exchange) record validations. This integration

expands the system's analytical capabilities, allowing the processing of key information in open-source intelligence operations. Figure 6 shows the main screen of OSINTEP.

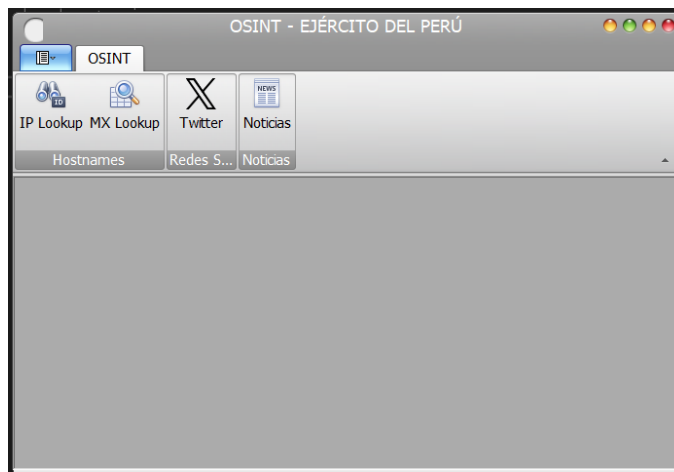


Fig. 6 OSINTEP Main Screen

The modular and extensible design of the software ensures that this initial version can evolve into more advanced implementations. This architecture facilitates the integration of new functionalities and improvements in the future, consolidating the system as a strategic tool for the Peruvian Army. The component diagram shown in Figure 7 describes the architecture used in the software implementation. This model illustrates how the different modules of the system, including the libraries and APIs used, are integrated to provide the basic functionalities of this first version. The diagram highlights the relationships between key components, showcasing the modular approach adopted, which facilitates future expansions and updates based on the strategic needs of the Peruvian Army.

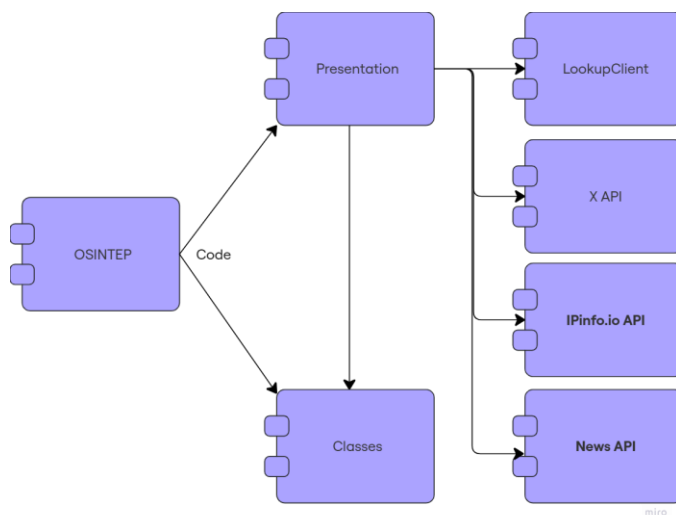


Fig.7 Component Diagram

Algorithm 1 presents the pseudocode that describes the functional structure of the developed software, designed to perform data analysis through multiple selected APIs.

The pseudocode shows the logical flow of the system, starting from a main menu that organizes user interactions and the specific functions of each module. Its purpose is to provide a clear and structured view of how the software works, serving as a foundation for future extensions, optimizations, and integration of advanced technologies. This methodological approach ensures that the system can evolve consistently with the objectives outlined in future research.

---

**Algorithm 1:** Development and Functionality of OSINTEP

---

**Begin**

1. **Create main form**

Add "IP Lookup" button (btnIPLookup)

Add "MX Lookup" button (btnMXLookup)

Add "X API" button (btnXAPI)

Add "NewsAPI" button (btnNewsAPI)

Add "Exit" button (btnExit)

2. **Event btnLookup.Click:**

Show "Enter search term:"

Read searchTerm

result ← ConsultAPI(searchTerm, btnLookup.Tag)

Show "Results:"

Display result in Corresponding Control based on API

3. **Function ConsultAPI(searchTerm, apiType):**

apiFunctions ← {

"IPinfo": CallAPI("IPinfo.io", searchTerm),

"MX": CallAPI("MX Lookup", searchTerm),

"XAPI": CallAPI("X API", searchTerm),

"News": CallAPI("NewsAPI", searchTerm)

} Return

apiFunctions[apiType]

4. **Function CallAPI(apiName, searchTerm):**

If apiName == "IPinfo.io":

    Call IPinfo.io API with searchTerm

Else If apiName == "MX Lookup":

    Call MX Lookup API with searchTerm

Else If apiName == "X API":

    Call X API with searchTerm

Else If apiName == "NewsAPI":

    Call NewsAPI with searchTerm

Receive data from api

Return processed data

**End**

---

*A. Results*

In this section, the results obtained through the use of the OSINTEP tool and the integration of various APIs for the collection and analysis of information related to potential threats, misinformation, and security vulnerabilities are presented. The tools used include X API, IPinfo.io API, NewsAPI, and the LookupClient library for DNS queries.

To perform the analysis, automated scripts within OSINTEP were used. For example, the X API was accessed via HTTP requests to retrieve posts using the hashtag #Ciberseguridad, and the responses were processed to extract mention counts, user data, and timestamps. The IPinfo.io API was queried with the IP address 10.x.x.x, returning location data (Peru, Lima), the associated organization (ICTE), and additional technical identifiers. This information was structured and processed using the OSINTEP tool. NewsAPI was queried with the term "Cyberattack," returning a list of recent articles with metadata such as publication name, title, and URL. These articles were manually reviewed to identify any cases related to critical infrastructure. For DNS analysis, the LookupClient library was used to resolve MX records for icte.edu.pe, confirming the mail exchanger as mail.icte.edu.pe and validating its operational state. These tools allowed for reproducible and automated analysis of all collected data.

The automated workflows in OSINTEP allowed efficient data processing and threat analysis, ensuring consistency in results across the different sources of information.

Table 3 presents the data obtained from the integrated APIs, along with the details of the DNS query performed using LookupClient. This process took place on January 6, 2025, highlighting 53 mentions related to cybersecurity vulnerabilities. Additionally, the information regarding the email servers of the Instituto Científico Tecnológico del Ejército (ICTE) is provided, with the IP address not displayed for security reasons.

In Table 4, the results of the analyses performed on various elements related to cyber threats, collected through different sources, are shown. The analysis of the IP address 10.x.x.x revealed that it was linked to a known attack in Peru, so it was recommended to block the IP and strengthen security measures. Social media mentions identified an increase in discussions related to recent vulnerabilities, suggesting a potential risk, and it was recommended to alert the security teams. Furthermore, news about cyberattacks highlighted an incident targeting critical infrastructure in Peru, which led to the recommendation to notify authorities and take preventive actions. Lastly, the DNS query performed on the domain icte.edu.pe showed that the mail server was secure, with no critical vulnerabilities, but it was advised to carry out periodic security reviews to maintain its protection.

TABLE III  
DATA COLLECTION THROUGH APIs AND DNS QUERIES

Data Source	Search Parameter	Data Obtained	Type of Information
X (Social Media) API	Hashtag: #Ciberseguridad	53 mentions related to cybersecurity vulnerabilities	Mentions, users, locations
IPinfo.io API	IP: 10.x.x.x	Country: Peru, City: Lima, Organization: ICTE	Geolocation, IP details
NewsAPI	Term: "Cyberattack"	10 news articles on cyber incidents in Latin America	Online news, access links
LookupClient (DNS)	Domain: icte.edu.pe	MX Record: mail.icte.edu.pe, associated IP: 10.x.x.x	Email server information

TABLE IV  
DATA ANALYSIS AND THREAT IDENTIFICATION

Analyzed Element	Analysis Description	Identified Result	Recommended Action
IP: 10.x.x.x	Analysis of the IP address in threat databases	IP linked to a known attack in Peru	Block the IP and strengthen security
Mentions on social media	Identification of patterns and trend analysis on social media	Increase in mentions related to recent vulnerabilities	Alert security teams
News on Cyberattacks	Content and context analysis of news on cyberattacks	News about a targeted attack on critical infrastructure in Peru	Notify authorities and take preventive measures
DNS Query on icte.edu.pe	Validation of the MX (Mail Exchange) record for icte.edu.pe	Secure mail server, no critical vulnerabilities	Perform regular security reviews and apply additional protection

## B. Discussion

The results obtained through the OSINTEP tool, and the integration of various APIs have demonstrated the potential of this approach to detect and analyze cyber threats in real time. However, it is important to consider some observations that help understand both the advantages and the limitations of such tools in a military context.

Firstly, the analysis of social media mentions through the X API revealed a significant number of discussions about cybersecurity vulnerabilities, highlighting the growing interest in these topics within society. While this type of data is useful for gaining a preliminary understanding of threats, it also emphasizes the need for a more in-depth and sophisticated

analysis. Social media mentions can be disorganized and difficult to interpret without an adequate filter, which limits their ability to detect specific threats in real time. Additionally, commercial tools specialized in analyzing large volumes of social data often offer a much higher level of accuracy, something that free solutions, like X API, cannot always match.

The geolocated analysis of IPs using the IPinfo.io API revealed an IP address linked to a known attack in Peru. This finding highlights the importance of having monitoring systems that can quickly identify compromised IP addresses. While tools like IPinfo.io provide relevant information, the data provided is basic and does not always allow access to more comprehensive threat databases. This can be a significant limitation in situations where cybersecurity is critical, such as in the military. In these cases, specialized and paid systems can provide more detailed and real-time analysis.

News about cyberattacks, gathered using NewsAPI, evidenced relevant incidents that could jeopardize critical infrastructures. This type of information is essential for decision-making and planning preventive measures. However, the tools used in this study provide only limited access to the available information in the media. More detailed analyses of the impacts of cyberattacks usually require more specialized sources of information, which highlights one of the limitations of open-source and free solutions.

The analysis of mail servers using LookupClient demonstrated that the ICTE mail server was secure at the time, but also pointed out the importance of conducting periodic security audits. Although using DNS queries is an important step in assessing infrastructure security, the available tools cannot predict future vulnerabilities or fully automate the monitoring process. Commercial or paid solutions in this field allow the integration of more advanced detection systems and continuous analysis, which is especially valuable for maintaining protection in critical infrastructures.

Regarding the overall approach of this study, one of the main advantages is that, being accessible and free, OSINT tools allow military institutions to perform basic monitoring and detect threats efficiently without incurring the costs of commercial solutions. However, it is clear that the tools used in this analysis have some limitations, particularly in terms of real-time monitoring capabilities and the depth of analysis. Paid solutions, though expensive, provide much more comprehensive coverage, making them the preferred option for organizations that require exhaustive and continuous monitoring of cyber threats.

What differentiates this work from the approaches presented in the state of the art is its focus on the integration of free and openly accessible tools specifically tailored for military institutions in contexts where access to commercial cybersecurity solutions may be limited. Unlike other studies that rely on high-cost or proprietary systems for cyber threat detection and monitoring, this research demonstrates a practical implementation of OSINT-based tools (such as X API, IPinfo.io API, and NewsAPI) and highlights their

effectiveness and limitations when applied in a military environment. The novelty lies in the adaptation of these tools within the operational framework of the Instituto Científico Tecnológico del Ejército (ICTE), providing a cost-effective model for initial threat detection and situational awareness that can serve as a foundation for more robust cybersecurity infrastructures.

## VI. CONCLUSIONS

In this work, the development of OSINTEP is presented, a tool specifically designed for the Army of Peru with the goal of establishing a solid foundation for future improvements and advanced implementations in the field of open-source intelligence (OSINT) operations. The developed system enables the execution of various phases, such as data collection, analysis, and presentation, from multiple open sources, in order to detect vulnerabilities, threats, and other key aspects in cybersecurity and other relevant domains.

The results obtained from the use of OSINTEP and the integration of various open-source APIs, such as X API, IPinfo.io, NewsAPI, and LookupClient, demonstrated the potential of the tool to detect and analyze cyber threats in real time. In particular, the tool allowed for the identification of critical vulnerabilities, misinformation patterns, and suspicious activities related to cybersecurity, enabling authorities and security teams to make informed and timely decisions.

By analyzing the collected data, it was observed that mentions on social media, obtained through X API, revealed a significant increase in discussions related to cybersecurity vulnerabilities, highlighting the growing social interest in these issues. The geolocated IP address query using the IPinfo.io API allowed the identification of addresses linked to previous attacks, recommending actions such as blocking these IPs and strengthening security measures. Additionally, queries through NewsAPI identified news about cyberattacks affecting critical infrastructure, leading to recommendations for notifying authorities and taking preventive measures.

Furthermore, the analysis of DNS records, performed with LookupClient, validated the security of the Army's Scientific and Technological Institute (ICTE) email server, emphasizing the need for periodic security reviews to maintain system protection.

## ACKNOWLEDGMENTS

The authors extend their gratitude to the Cybersecurity, IoT, and Artificial Intelligence Research Group (GriCIA) of the Army Scientific and Technological Institute (Instituto Científico y Tecnológico del Ejército) and the Directorate of this university for funding the project.

## REFERENCES

[1] OSINT Framework. (2025). Open-Source Intelligence (OSINT) Tools. Retrieved from <https://osintframework.com>.  
 [2] M. Goodman, "Open Source Intelligence in a Networked World,"

Palgrave Macmillan, 2016.  
 [3] C. Ventures, "Data growth projections for 2023-2025," Cybersecurity Statistics, 2023.  
 [4] L. Yong-Joon, P. Se-Joon, and P. Won-Hyung, "Military Information Leak Response Technology through OSINT Information Analysis Using SNSes," Security and Communication Networks, 2022.  
 [5] K. Lab, "Cyberthreats in Latin America: 2024 Overview," Kaspersky Reports, 2024.  
 [6] ODIN, "ODIN," 2024. [Online]. Available: <https://odint.net/osint-y-el-ciclo-dean%C3%A1lisis-de-inteligencia/>  
 [7] Elasticsearch, "Elasticsearch," 2024. [Online]. Available: <https://www.elastic.co/es/what-is/elasticsearch>  
 [8] J. Jimenez, "Plataforma OSINT para el almacenamiento y análisis inteligente de datos de la red social Twitter," Centro Universitario de la Defensa en la Escuela Naval Militar, 2023.  
 [9] B. Talent, "OSINT: que' es y te'cnicas ma's usadas," 2024. [Online]. Available: <https://www.il3.u.edu/blog/osint-que-es-y-tecnicas-mas-usadas/>  
 [10] Shodan, "Shodan," 2024. [Online]. Available: <https://es.wikipedia.org/wiki/Shodan>  
 [11] Keepcoding, "¿Que' es Google Dorks?" 2024. [Online]. Available: <https://keepcoding.io/blog/que-es-google-dorks/>  
 [12] Maltego Web, "Maltego," 2024. [Online]. Available: <https://www.maltego.com/>  
 [13] Aprenderhacking.org, "Entendiendo OSINT," 2024. [Online]. Available: <https://aprenderhacking.org/osint-que-es-software-herramientas-framework/>  
 [14] Keppcoding, "¿Que' es SocialLinks?" 2024. [Online]. Available: <https://keepcoding.io/blog/que-es-sociallinks-ciberseguridad/>  
 [15] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A review." Int. J. Netw. Secur., vol. 19, no. 2, pp. 244–250, 2017.  
 [16] B. Cho, "A system for national intelligence activity based on all kinds of osint (open source intelligence) on the internet," Journal of Information and Security, vol. 3, no. 2, pp. 41–55, 2003.  
 [17] Y.-B. Leau and S. Manickam, "Network security situation prediction: a review and discussion," in Intelligence in the Era of Big Data: 4th International Conference on Soft Computing, Intelligent Systems, and Information Technology, ICSIT 2015, Bali, Indonesia, March 11-14, 2015. Proceedings 4. Springer, 2015, pp. 424–435.  
 [18] J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, "Machine learning techniques applied to cybersecurity," International Journal of Machine Learning and Cybernetics, vol. 10, no. 10, pp. 2823–2836, 2019.  
 [19] N. Badie and A. H. Lashkari, "A new evaluation criteria for effective security awareness in computer risk management based on ahp," Journal of Basic and Applied Scientific Research, vol. 2, no. 9, pp. 9331–9347, 2012.  
 [20] E. Bashier and T. B. Jabeur, "An efficient secure image encryption algorithm based on total shuffling, integer chaotic maps and median filter," 2021.  
 [21] S. Symantec, "Istr internet security threat report," 2019. [Online]. Available: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf>  
 [22] B. Fireeye, "M-Trends," 2021. [Online]. Available: <https://www.fireeye.com/current-threats/annual-threat-report.html>  
 [23] S. Rahmadika, M. Firdaus, S. Jang, and K.-H. Rhee, "Blockchain-enabled 5G edge networks and beyond: An intelligent cross-silo federated learning approach," Security and Communication Networks, vol. 2021, no. 1, p. 5550153, 2021.  
 [24] R. Brown and R. M. Lee, "The evolution of cyber threat intelligence (cti): 2019 sans cti survey," SANS Institute, 2019. [Online]. Available: <https://www.sans.org/white-papers/38790/>  
 [25] Quinto Huamán, C., & Picón Huacarpuma, R. M. (2023). Uso de la Inteligencia Artificial en el Ejército del Perú: Desafíos y Oportunidades. *Revista CITEK*, 6(06). Recuperado a partir de <https://revistas.ictedu.edu.pe/citek/article/view/34>