JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(2), JUNE, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Application of Geospatial Data in Cyber Security

Adeyinka Adeoye
University of Potomac, USA

ABSTRACT

Geospatial data is often perceived as only being related to maps, compasses and locations. However, the application areas of geospatial data are far wider and even extend to the field of cybersecurity. Not only is there an ability to show points of interest and emerging network traffic conditions, geospatial data also has the ability to model cyber crime growth patterns and indicate affected areas as well as the emergence of certain type of cyber threats. Geospatial data can feed into intelligence systems, help with analysis, information sharing, and help create situational awareness. This is particularly useful in the area of cyber security. Geospatial data is very powerful and can help to prioritise cyber threats and identify critical areas of concern. Previously, geospatial data was primarily used by militaries, intelligence agencies, weather services or traffic control. Currently, the application of geospatial data has multiplied, and it spans many more industries and sectors. So too for cyber security, geospatial data has a wide number of uses. It may be difficult to find patterns or trends in large data sets. However, the graphic capabilities of geo mapping help present data in more digestible manner. This may help analysts identify emerging issues, threats and target areas. In this paper, the usefulness of geospatial data for cyber security is explored. The paper will cover a framework of the key application areas that geospatial data can serve in the field of cyber security. The ten application areas covered in the paper are: tracking, data analysis, visualisation, situational awareness, cyber intelligence, collaboration, improved response to cyber threats, decision-making, cyber threat prioritisation and protect cyber infrastructure It is aimed that through the paper, the application areas of geospatial data can be more widely adopted.

ARTICLE INFO

Article History
Received: September, 2023
Received in revised form: September, 2023
Accepted: February, 2024
Published online: June, 2024

KEYWORDS

Geospatial Data, Cyber Security, Geo-Informatics, GIS (Geographic information system)

INTRODUCTION

The rapid growth of digital technologies has created a vast attack surface, enabling cybercriminals to launch sophisticated attacks with devastating consequences. The 2020 Cybersecurity Almanac reports that cyberattacks have increased by 300% since 2019, resulting in an estimated $6 trillion in damages globally. Traditional cybersecurity approaches often overlook the spatial dimension of cyber threats, which can provide valuable context for threat detection, incident response, and risk assessment.

Geospatial data, comprising location-based information and geographic context, offers a game-changing opportunity to enhance cybersecurity posture. By integrating geospatial data with cybersecurity, organizations can:

1. Identify high-risk areas and vulnerabilities, enabling proactive measures to fortify defenses.
2. Track and predict threat actor movements, anticipating potential attacks and minimizing damage.
3. Enhance incident response with spatial context, streamlining efforts and reducing response times.

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

4. Visualize complex threat landscapes, facilitating situational awareness and informed decision-making.

This research aims to explore the uncharted territory of geospatial data application in cybersecurity, addressing the following research questions:

1. How can geospatial data be integrated with cybersecurity frameworks to improve threat intelligence and incident response?
2. What are the most effective geospatial analysis techniques for identifying and predicting cyber threats, and how can they be applied in real-world scenarios?
3. How can geospatial visualization enhance risk assessment and situational awareness in cybersecurity, and what are the implications for organizational decision-making?

Through a comprehensive review of existing literature, case studies, and experimental research, this project will demonstrate the value of geospatial data in enhancing cybersecurity practices. By investigating the intersection of geospatial data and cybersecurity, this project aims to contribute to the development of innovative solutions, enhancing the resilience of digital systems and protecting against emerging cyber threats.

The advancement and integration of information and communication technology (ICT) in peoples' daily lives has led to a growing cyberthreat landscape. This pushes the need for better solutions and techniques to combat threats. Integrating geospatial data into existing tools and techniques could strengthen software systems.

Information in a digital format has become more valuable. Organisations can gain tremendous insight and awareness from information that is presented and visualised in a useful representation. Information that has been analysed and communicated into a relevant format with dataflow pipelines which are designed for rapid continuous updates can vastly improve decision making and establish priorities.

Decision making is driving organisations and core to this is accurate information. Strategically organisation recognise the value of information as an asset. This brings forth the continuous need for novel data sources and solutions. There is a persistent pursuit to find new ways to use data, find relationships and identify trends. Taking geospatial data into consideration, this field provides vast areas for note-worthy data visualisation. Previously, geospatial data was primarily used by militaries, intelligence agencies, weather services or traffic control. Currently, the application of geospatial data has multiplied, and it spans many more industries and sectors. So too for cyber security, geospatial data has a wide number of uses. For instance, the location of cyber-attacks can be identified, and patterns can be revealed towards predicting future attacks.

Research Contributions

The contributions of the paper are summarised as follows:

1. Insight into how GIS (Geographic information system) data can be applied to the cyber security field.
2. Generation of ideas on new techniques and technologies that can be used to represent cyber security (incidents, attacks and crime).
3. Show how geo-spatial mapping can help with the monitoring of cyber security incidents
4. Indicate how cyber security threats can be studied to create awareness on risks and communicate pivotal information about cyber threats frequency and impact.

Geospatial data typically combines location information (usually coordinates on the earth) and attribute information (the characteristics of the object, event or phenomena concerned) with temporal information (the time or life span at which the location and attributes exist) international business machine (IBM 2022). With geospatial analytics, timing and location can be added to common data types to produce useful visualisations. Visualisations can be in the form of

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(2), JUNE, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

maps, graphs, statistics and cartograms that can show changes over a period of time, as well as shifts in development. These visualisations offer more insight as many aspects can be missed in a long list of data. Patterns can be identified, and trends detected. This can lead to faster and more reliable predictions and influence decision-making.

Geospatial Data

Examples of geospatial data include (IBM 2022):

1. Vectors and attributes: Descriptive information about a location such as points, lines and polygons.
2. Point clouds: A collection of co-located charted points that can be re-contexture as 3D models.
3. Raster and satellite imagery: High-resolution images of our world, taken from above.
4. Census data: Released census data tied to specific geographic areas, for the study of community trends.
5. Cell phone data: Calls routed by satellite, based on GPS location coordinates.
6. Drawn images: CAD (computer aided design) images of buildings or other structures, delivering geographic information as well as architectural data.
7. Social media data: Social media posts that data scientists can study to identify emerging trends Maps are a common practice for presenting spatial data as they can easily communicate complex topics. They can help validate or provide evidence for decision making, teach others about historical events in an area, or help provide an understanding of natural and human-made phenomena (Safe.com 2022).

A key capability of geospatial mapping is the use of choropleth maps. Choropleth maps are able to show differences, consistencies and patterns. Classified areas in a choropleth map will have distinct boundaries whereas heat maps, which demonstrate the concentration or density of a phenomenon, have indistinct boundaries. Different colour schemes and classes can be used to represent issues (Figure 1).

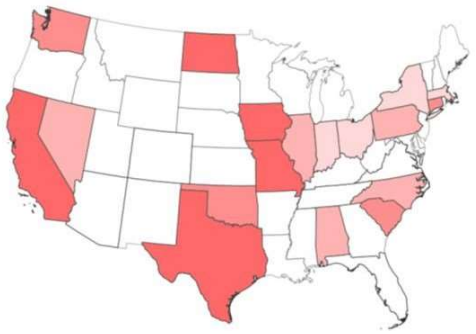


Figure1: Choropleth map

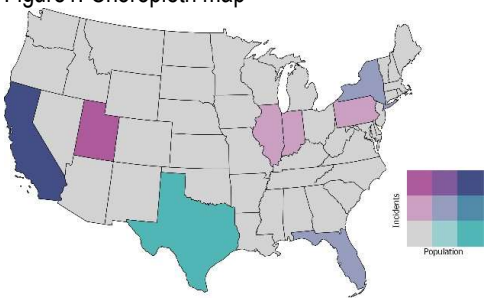


Figure2: Choropleth map with two over layed colour scales

Figure1: Example Choropleth maps shows a monovariate choropleth map; and figure 2 shows choropleth map, which visualises the correlation between two variables through two over layed colour scales.

STATEMENT OF PROBLEM

In the rapidly evolving field of cyber security, traditional methods of threat detection and prevention are often insufficient to counter increasingly sophisticated cyber-attacks. Geospatial data, which provides information about the physical locations and movements of entities, presents a promising yet underutilized resource in enhancing cyber security measures. The integration of geospatial data with cyber security protocols could potentially offer new insights into attack patterns, facilitate real-time threat

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

detection, and improve incident response strategies.

Aim and Objectives of the Study

To explore and evaluate the application of geospatial data in enhancing cyber security measures, addressing technical, ethical, and operational challenges, and developing a framework for its effective integration into cyber security strategies.

1. Investigate the current state of geospatial data integration within cyber security systems.
2. Analyze the potential of geospatial data to enhance real-time threat detection and incident response.
3. Propose guidelines and best practices to ensure compliance with data protection regulations while utilizing geospatial data.

Scope of the Study

Examination of current practices and technologies for integrating geospatial data into cyber security systems. This includes assessing data compatibility, storage solutions, and processing capabilities. The study will develop a prototype system to demonstrate practical integration.

Analysis of the potential benefits of geospatial data in real-time threat detection and incident response. This includes designing and testing algorithms that utilize geospatial data to identify and respond to cyber threats. Case studies will be conducted to validate the effectiveness of these models.

Identification and analysis of operational challenges associated with implementing geospatial data analytics in cyber security. This includes the development of training programs and operational strategies to manage the complexity of these implementations.

LITERATURE REVIEW

Overview and Importance

The integration of geospatial data in cyber security is an emerging area of study that promises to enhance threat detection, incident response, and overall cyber resilience. This literature review examines the current state of research in this field, highlighting key findings, methodologies, and gaps in the existing knowledge.

Definition and Relevance

Geospatial data refers to information about the physical location and movement of objects or entities on the Earth's surface. In cyber security, geospatial data can provide context to cyber activities, helping to identify the geographic origins of attacks, track the physical movements of threat actors, and correlate cyber incidents with real-world events (He et al., 2018).

Applications in Threat Detection and Incident Response

Enhancing Threat Detection

Research indicates that geospatial data can significantly improve the detection of cyber threats by adding a geographic dimension to data analysis. For example, clustering analysis of geospatial data can identify unusual patterns of access or data exfiltration that may indicate a cyber-attack (Nguyen et al., 2019).

Incident Response

Geospatial data aids in incident response by providing real-time location-based information, which can be crucial for coordinating response efforts, especially in critical infrastructure sectors like transportation and energy (Liu et al., 2020).

Case Studies and Practical Implementations

Real-World Applications

Several case studies demonstrate the practical applications of geospatial data in cyber security. For instance, the use of geospatial data to track and mitigate Distributed Denial of Service (DDoS) attacks by correlating IP addresses with physical locations has shown promising results (Zhou et al., 2017).

Prototype Systems

Development of prototype systems integrating geospatial data with existing cyber

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

security platforms highlights the potential benefits and technical challenges. One notable example is the Geospatial Cyber Operations Platform (GCOP), which combines geographic information system (GIS) technology with cyber threat intelligence (Wang et al., 2021).

TECHNICAL AND OPERATIONAL CHALLENGES

Data Integration and Processing

Technical Barriers

Integrating geospatial data into cyber security systems involves significant technical challenges, including data interoperability, real-time processing, and handling large volumes of data. Studies emphasize the need for robust data management frameworks and advanced analytical tools to address these issues (Smith et al., 2018).

Privacy and Ethical Concerns

Data Privacy

The use of geospatial data raises substantial privacy concerns. Ensuring that the collection and use of location-based information comply with data protection regulations, such as GDPR (General Data Protection Regulation), is a critical challenge. Ethical considerations also play a significant role, particularly in balancing security needs with individual privacy rights (Jones & Johnson, 2019).

Operational Complexity

Implementation Challenges

Operationalizing geospatial data analytics in cyber security involves complex coordination across multiple domains. This includes training personnel, developing new operational procedures, and investing in appropriate technologies. Research underscores the importance of developing comprehensive implementation strategies to manage these complexities (Green et al., 2020).

GAPS IN EXISTING RESEARCH

1. **Lack of Standardized Frameworks**
   Standardization Needs: There is a notable lack of standardized frameworks for the integration and use of geospatial data in cyber security. Existing studies call for the development of industry-wide standards and best practices to facilitate wider adoption (Lee et al., 2021).
2. **Limited Longitudinal Studies**
   Temporal Analysis: Most research in this area is limited to short-term studies. Longitudinal studies that track the effectiveness of geospatial data integration over extended periods are needed to better understand its impact and refine methodologies (Brown & Clark, 2022).
3. **Interdisciplinary Research**
   Cross-Domain Collaboration: Effective application of geospatial data in cyber security requires interdisciplinary collaboration between geospatial scientists, cyber security experts, and legal scholars. Current literature highlights the need for more cross-domain research initiatives to address the multifaceted challenges involved (Wilson et al., 2020).

Importance of Geospatial Data

Geospatial information ordinarily joins area data and trait data with worldly data with geospatial investigation, timing and area can be added to normal information types to create helpful representations [8]. Representations can be as guides, diagrams, measurements, and cartograms that can show changes over a period, as well as movements being developed. These perceptions offer more knowledge as numerous perspectives can be missed in a considerable rundown of information. Examples can be recognized and drifts distinguished [9]. This can prompt quicker and more dependable expectations and impact navigation. Instances of geospatial information include:

1. Vectors and Traits: Elucidating data about an area like focuses lines and polygons.
2. Point Mists: An assortment of co-found outlined focuses that can be re-contextures as 3D models.

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

3. Raster and Satellite Symbolism [10]: Highgoal pictures of our reality, taken from a higher place.
4. Evaluation Information: Delivered enumeration information attached to explicit geographic regions, for the investigation of local area patterns.
5. PDA Information: Calls steered by satellite, because of GPS area, facilitates.
6. Drawn Pictures: computer-aided design pictures of structures or different designs, conveying geographic data as well as engineering information.
7. Web-Based Entertainment Information: Virtual entertainment posts that information researchers can study to distinguish arising patterns Guides are a typical practice for introducing spatial information as they can without much of a stretch impart complex subjects.

They can help approve or give proof to navigation, show others authentic occasions in a space, or assist with giving comprehension of normal and human-made peculiarities. A critical capacity of geospatial planning is the utilization of choropleth maps. Choropleth guides can show contrasts, textures, and examples. Characterized regions in a choropleth guide will have unmistakable limits though heat maps, which exhibit the focus or thickness [11] of a peculiarity, have vague limits. Different variety plans and classes can be utilized to address issues. The world is progressing at a quick rate and there are more improvements in the mechanical fields. With the quick development of ICT, come the related dangers of digital dangers. Digital dangers additionally develop as aggressors adjust their strategies for activity [12]. Geospatial information can assist better with understanding the progressions that are occurring and support the safeguard against dangers through information investigation and strong representations. A few inquiries that can be considered are:

1. Where are digital assaults occurring?
2. What are the areas of targets?
3. What are the areas of the wellsprings of assaults?
4. What are the areas of mediator foundation in digital assaults, e.g., intermediary servers, advanced post-boxes, and order and control servers?
5. What kind of digital assaults are happening?
6. What are the practical objectives?
7. What are the principal techniques utilized?
8. How is the digital assault design changing over the long haul?

Geospatial information and investigation can give knowledge into these significant inquiries by recognizing the areas, types, targets, and strategies, and also performing examinations [13]. Already spatial information was lumberingto utilize and required progressed programming. Nonetheless, with propels in handling and ICT, more spaces can go to spatial information to give better knowledge and track down answers for pain points. Cell phones, vehicle following, and satellites are assisting with opening the universe of spatial and area information for associations of all shapes and sizes. Geospatial information currently carries out the roles that guide, compasses and smoke flags once satisfied. Following individuals, populaces, geology changes, occasions, tempests, and traffic can be generally performed utilizing geospatial information.

A key application area of geospatial information in the field of network protection is the following. Geospatial information can assume an exceptionally essential part of information investigation. It can assist with envisioning the effect of a hacking gathering or see the plot of misleading publicity in virtual entertainment taken care of. Perception of the spread of digital assaults can make consciousness of the extension and effect of these occasions. With geospatial information, digital assault information can be addressed effectively. Area knowledge can be critical to creating digital insight. Associations can be shown, and interfaces found, utilizing guides, portrayals, and information fields. Graphical

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

symbology is exceptionally valuable in passing on basic snippets of data that make it more straightforward for the watcher to process. Network protection experts can now likewise depend on geospatial information to further develop security and construct guarded components. Geospatial information is underestimated. Most associations embrace the most recent innovation, yet the imperative capacities of geospatial information can be missed. There is insufficient writing on GIS for digital protection. Inside the Florida College, specialists have planned digital assaults on geospatial information [14].

The geospatial examination of this information had uncovered spatial examples and recognized nations that were more inclined to digital assaults. Moreover, areas of interest inside the US were recognized. In the tactical space, German online protection specialists coordinated GIS with network safety apparatuses to find designs from digital assaults. In the business space give guides to imagine dangers that are recognized by their programming suits. It muddled further handling and investigation, past handling, is performed their geospatial information [15]. Geospatial information is the capacity to fortify network protection by giving an abundance of data. This paper sums up different advantages and application regions for the utilization of geospatial information in the field of online protection. The proposed structure that examines the applications is as per the following.

HOW TO USE GEOSPATIAL DATA

The creators had the option to check the handiness of geospatial information during an initial seminar on geo-planning. Notwithstanding, the writing survey uncovered that logical writing for exhibiting the utilization of geospatial information inside digital protection is deficient. To settle this, the creators recommend involving a system for accomplishing a consistent combination of geospatial information and digital protection. Geospatial information can be utilized to address data from different spaces, for example:

1. Retail: pay, lodging/lease costs, populace, age.
2. Atmospheric Conditions: tropical storms, twisters, outrageous winter climate.
3. Site ID: traffic designs, people walking through, number of inhabitants, contender data
4. Medical Care: water area, drug clients, ecological risks, immunizations,
5. Monetary Administrations: envision land, track development after some time, investigations speculations without movement.
6. Operations/Transportation: vehicle following, assist plan, course examination Openness to these useful regions showed enormous ability to additionally apply geospatial information to digital dangers and network protection [9].

Unequivocally, by taking a gander at the capacities and highlights of geospatial information, it very well may be additionally stretched out to reinforce an association's line of digital guard and security. Numerous public safety organizations may as of now use geospatial information. Cautious associations, like the military or public knowledge administrations, crisis administrations and framework security control gatherings may as of now incorporate geospatial information in their framework.

RESEARCH FRAMEWORK

The author was able to gauge the usefulness of geospatial data during an introductory course on a geo-mapping. However, the literature review revealed that scientific literature for demonstrating the use of geospatial data within cyber security is lacking. To solve this, the authors prescribe using a framework for achieving seamless integration between geospatial data and cyber security.

Geospatial data can be used to represent information from various domains such as: (Trajectory Magazine 2022):

1. Retail: income, housing/rent prices, population, age

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

2. Weather patterns: hurricanes, tornadoes, extreme winter weather
3. Site identification: traffic patterns, foot traffic, number of residents, competitor information
4. Healthcare: water location, drug users, environmental hazards, vaccines,
5. Financial services: visualise real estate, track construction over time, analyse investments without travel
6. Logistics/ Transportation: vehicle tracking, expedite schedule, route analysis

Exposure to these functional areas showed tremendous capability to further apply geospatial data to cyber threats and cyber security. Unequivocally, by looking at the capabilities and features of geospatial data, it can be further extended to strengthen an organisation's line of cyber defence and security. Many national security agencies may already utilise geospatial data. Defensive organisations, like the military or national intelligence services, emergency services and infrastructure safety control groups may already include geospatial data in their systems. The field of cyber security can also reap the benefits of utilising geospatial data. A framework is proposed in Figure 2 that encapsulates the core application areas of geospatial data to cybersecurity. A discussion follows on these application areas.

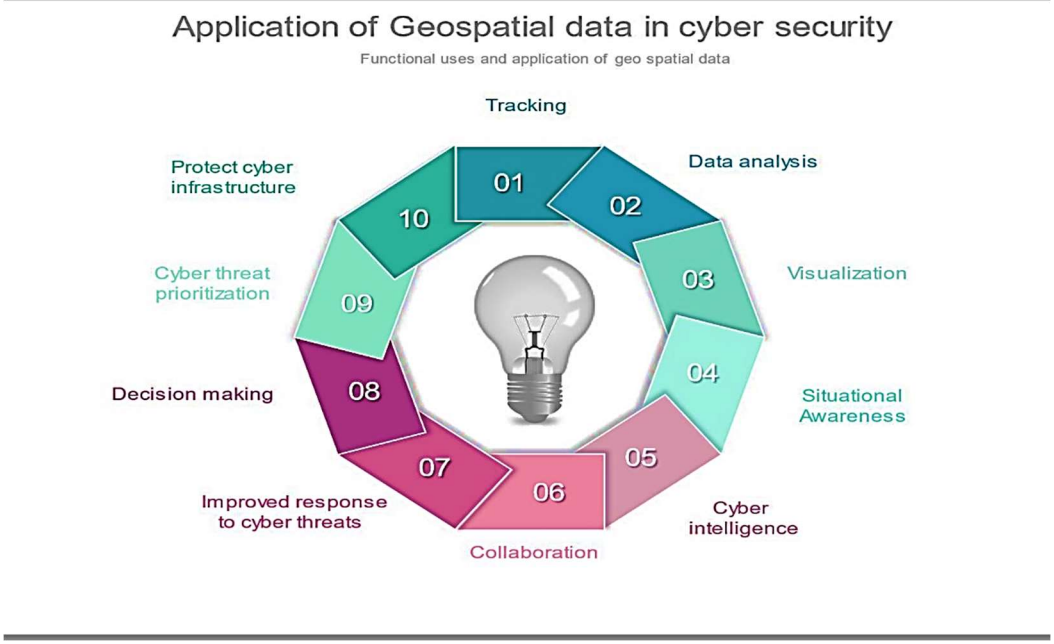


Figure 2: Application of Geospatial data to cyber security

The framework summarises 10 principal application areas which are:

1. Tracking
2. Data analysis
3. Visualisation
4. Situational awareness
5. Cyber intelligence
6. Collaboration
7. Improved response to cyber threats
8. Decision-making
9. Cyber threat prioritisation
10. Protect cyber infrastructure

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

These are elaborated on in the next few sections. The framework provides a snapshot of how geospatial data can be integrated into stronger cyber defence capabilities. It encapsulates the main benefits of using geospatial data to visualise, analyse and grow cyber intelligence. The framework is not rigid in that it can include many more application areas. The main aim of the framework is to show the value of geospatial data so that it can be further utilised and contribute to the development of stronger cyber defence capabilities, as well as create awareness of threats.

Tracking

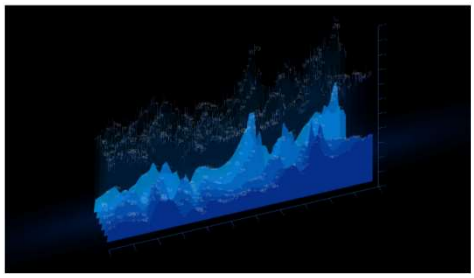
A key application area of geospatial data in the field of cyber security is tracking. "By implementing defence systems that include mappable and traceable physical locations in the digital sphere, security experts can more effectively follow and track possible threats (Brode 2021). Whitelisted zones can serve as "geo-fences" to only permits access within specific ranges. Access attempts from blacklisted areas can be restricted and flagged. Furthermore, when threats are detected from certain locations, perpetrators can be tracked to identify patterns or core targets. With the use of geospatial data, trends can be identified, and pre-emptive action taken when a potential attack is identified. Certain areas can be identified to be hotspots for specific threats. Closer monitoring and resources can be deployed to hotspot locations or those locations more susceptible to certain vulnerabilities.

DATA ANALYSIS

In today's world, spatial data analysis helps solve many complex problems related to location. Through analysis, you can conduct thorough research and understand the data specifically from the geographical side. Also, users can use geospatial analysis to assess trends, make the right decisions and assess risks. Thanks to this technology, it is possible not only to estimate the location but also to study several characteristics, which will help make an accurate forecast in the future.

Geospatial solutions provide the capability to integrate information from multiple sources, channels and also use existing data towards establishing correlations between objects and events. These various sources help provide more clarity and provides for insightful analysis.

For example, data can be presented in tables showing various locations of a cyber-attack. However, once this data is plotted into a map or grouped, aggregrated and processed by geographic region, then the prevalence of a specific cyber- attack in certain locations can be seen. Geospatial analysis provides the ability to combine data to produce intelligence that can be used for information sharing and the creation of new knowledge



Importance of Spatial Analysis

The importance of spatial analysis in GIS manifests itself in many factors because, by its very nature, spatial analysis involves much more than just displaying the necessary objects. Geospatial information is collected from many sources that can be used for different purposes and interpretations. An excellent example is traffic in a city, where spatial analysis helps to manage facilities and take the necessary actions to improve city roads.

In addition, this technology allows users to monitor the spread of diseases on different continents and help make timely efforts that will help avoid a pandemic. For example, spatial data is often used to map disease removal and vaccination strategies, as happened with COVID-19. At the moment, spatial analytics plays a rather important role in the daily life of every person and has become an integral part of a comfortable life. We deal with the use of spatial analysis daily, from simply ordering a taxi to tracking Internet parcels

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

and using a navigator. Even though satellite imagery has been around for many years, with the advent of artificial intelligence and various software, spatial analysis has become simpler and more accessible, and enterprises have been able to deliver it.

Types of Spatial Analysis

There are six main types of spatial analysis in GIS. They are queries and discussions, data measurement, transformation, description, optimization, and validation. Our specialists have prepared a brief description of each of the types, which you can find below:

The first type involves using GIS to answer simple questions that users ask. It does not change or generate new data. This type is fundamental and simplest. Data is measured through prime numbers that explain the meaning of the data used. This type uses standard object characteristics such as area, shape, and length. In addition, with the help of measurement, you can study the relationship between the required objects and study their direction.

Transformation is a basic geospatial analytics procedure that compares or combines entire datasets to create new ones. This process converts vector data analysis in GIS to raster data and vice versa while using mathematical, logical, or geometric principles. The description of the summaries helps users to tell the purpose of the data collection. This type includes standard deviations, means, and other equivalents that are used for data analysis.

Optimization helps to find the best position of objects, which is justified by predetermined criteria. This type of spatial analysis is most commonly used for parcel delivery, market analysis, and more. The check is done to summarize all the results obtained, with the help of which users can assess the structure and consider further developments. Hypothesis testing is at the heart of geospatial analysis and should be applied to all geographic data.

Benefits of Spatial Analysis

Many users have been using spatial data analysis for a long time to solve important questions and make the right decisions. However, for the majority, this technology is still something complex, unknown, and incomprehensible. Below we list a few of the benefits that make data analysis more popular every year:

1. Spatial data analysis helps reduce costs and increase business revenue. It also helps reduce the cost of unnecessary materials and practices.
2. Significant increase in machine productivity.
3. Provides income for various industries and helps to make the work process more efficient.
4. In some way, geospatial analytics protects the health and safety of enterprise employees and the public.
5. With the help of spatial data analysis, you can easily comply with regulatory requirements.
6. Spatial analysis improves customer experience and service.
7. Businesses that use geospatial data analysis have many more satisfied customers than those that still use standard charts and graphs.
8. Using data analysis, you will become competitive and get a large number of advantages over other enterprises.

Spatial Data Analysis Process

Many users who have encountered this technology are interested in how to properly conduct spatial data analysis. Our experts have written a guide to save you from unnecessary difficulties. You can familiarize yourself with it by reading this section to the end:

1. Formulate goals and questions. Decide for what purpose you will conduct a spatial analysis.
2. Explore the data. Look at the completeness, quality, and size of the data.
3. Create a blueprint for the model. Develop your action plan and break the problem into several parts.

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

4. Study the results. The next step is to evaluate the results and determine if they are in line with your goals.
5. Continue with the analysis process. Remember that geospatial analytics is an ongoing process that must be carried out until all issues are resolved.
6. Show your results. Tell the public about the spatial analysis results and become useful to them.
7. Make a final decision. The final step is decision-making, assisted by GIS and geospatial analysis. As a result, you should get what you set as the goal at the beginning.

How to do spatial analysis in GIS?

To do spatial analysis in GIS, you need to go through five main stages:

1. Setting a goal.
2. Collecting data.
3. Choosing the necessary tools and methodology.
4. Researching and evaluating the results.
5. In the end, you should get those results that cover the needs of your goal.

Visualisation

GIS has many more advanced uses. GIS can capture, store, manipulate, and visualize spatial data that helps cities, counties, industries reveal spatial relationships through analysis and real-world data visualization. As the world becomes more data-driven, the benefits and abilities of GIS are helping companies make quicker informed decisions with a real-time perspective. Large files with numbers are usually hard to read and make it difficult to spot patterns easily (Datumize 2020).

The graphic representations in geospatial data are able to present extensive sets of data in a clear and cohesive manner. This further provides for comprehension of the data which can be used to draw conclusions and grasp different perspectives. Visual representation of data also provides the ability to detect anomalies. For instance, if a certain town shows 2 million attacks but it is relatively small town with only 1000 residents, this will clearly raise a red flag that a data capturing error has occurred. This is more readily detectable in a visual representation of the data than a long table or text list. Thus, graphical representations can be used to avoid cognitive overload with cyber security data.

Situational awareness

Endsley has proposed one of the most widely used views of situational awareness (1995). It is shown as a three-step model in Fig 3.

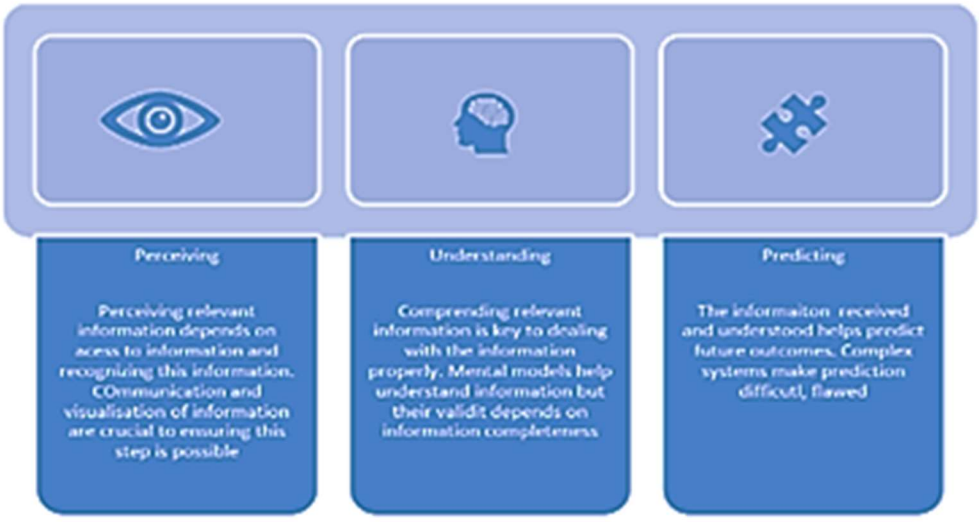


Figure 3: Steps in Situational Awareness (Endsley 1995)

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(2), JUNE, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

The first steps of situational awareness is to perceive the relevant information by being able to access it and being able to recognize it. A critical requirement is communication and proper visualisation (CQ Net 2022). With geospatial data, cyber security threat information can be communicated and visualised more effectively.
According to Visual Teaching Alliance (Shift elearning, 2021):

1. The brain can see images that last for just 13 milliseconds.
2. Our eyes can register 36,000 visual messages per hour.
3. We can get the sense of a visual scene in less than 1/10 of a second.
4. 90% of information transmitted to the brain is visual.
5. Visuals are processed 60,000X faster in the brain than text.
6. 40 percent of nerve fibers are linked to the retina

The second step of situational awareness entails the comprehension of the information. This is largely dependent on the knowledge to handle the incoming information as well how the information is presented. A person can create a mental model or update an existing one depending on how the information is presented (CQ Net 2022). Visuals have been found to improve learning by up to 400% (Shiftelearning, 2021). By representing the information graphically and visually, intelligence can be created by taking in more information and synthesising it into new knowledge.

The final step for situational awareness is the prediction of possible outcomes depending on the information received and comprehended. There may be complex dependencies but, with useful information, insightful forecasts can be made to assist with decision- making.

Situational awareness is critical for cyber security to gain an understanding of the environment to support decision- making. For instance, if geospatial models demonstrate the number of incidents in the USA, using a map such as the one shown in Figure 4, one can clearly distinguish the states that are more at risk.

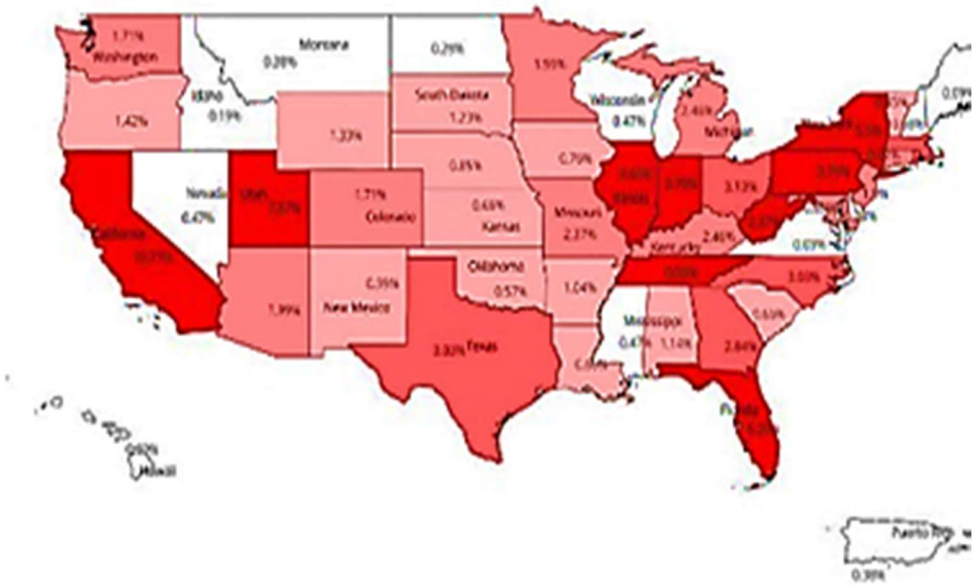


Figure 4: Map to indicate data breaches in states of the USA. Map developed using QGIS.

CYBER INTELLIGENCE

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

Raw data is collected and processed to form information. Using GIS, this information can be processed and analysed in conjunction with other data sources in order to create intelligence. With proficient visualisation, strong insight can be gained.

Some conclusions can become more evident when shown in a geospatial manner. Other issues may need to be investigated to gain more clarity. For example, a time lapse of attacks may show a decline or increase in a threat over time. This may correlate to a certain event or cyber vulnerability.

Collaboration

Analysis of certain attacks can reveal a pattern. For example, a particular switch or phone could be targeted. Equipped with the data analysis results, cyber specialists can reach out to the affected organisations/ service providers and aim to work together in tracking, tracing and monitoring the threat.

If a specific type of threat is occurring, organisations around the world can join forces to work together and implement controls to try and deter or stop the more rampant rise. With the use of geospatial data, security response centres, intelligence bureaus and security organisations would be able to see which specific sectors are vulnerable and how to carry out an operations plan to reduce the spread of a threat.

Improved response to cyber threats

The benefits of visualisation in geospatial data are that the visualisation capabilities allow us to identify emerging trends and react more quickly based on what has been identified. These patterns are easier to consume in a visual format as we are able to more closely correlate parameters.

Decision-making

The insight gained from geospatial data analysis can contribute to more effective decision-making. Instead of using intuition, decision makers can rely on more discerning findings. Geospatial data can give a good sense of the findings and increase visibility and understanding of core issues. For example, geospatial data can reveal certain sites or locations that are being targeted by a certain attack type. More resources and defensive mechanisms can be deployed. Awareness campaigns can be targeted to warn users about the threat of a specific type of cyber-attack.

Cyber threat prioritisation

Since better insight can be gained from geospatial data, it can be used to prioritise threats. For example, a rise in a specific threat can be detected. Also, the location of prevalent threats can be found. By analysing the data, specialists can classify which threats need more attention.
With the pattern detection and trend observation in geospatial analytics, cyber security specialists can monitor a threat to see if it is increasing or slowing down over a period. This can help identify critical threats and those that need urgent attention.

Protect cyber infrastructure

By providing insight into trending attacks and targets, key decision makers can assign resources and deploy defensive techniques. Geospatial data thus has the capability to help improve security and protect cyber infrastructure by providing key information about focus areas and methods of attack. This information can feed into defensive strategies and protection mechanisms of key locations.

CONCLUSION

With the rise of cyber-attacks and cybercrime, it is important to find new knowledge areas that can be used in the field of cyber security. With the identification of new application areas, stronger awareness of cyber security threats can be created. Using GIS within cyber security systems is an emerging trend.

There are many benefits of using geospatial data for cyber security. With geospatial data, cyber threat data can be captured, for example, the location of attacks, the number of attacks, the proportion, dates, types and various other factors. Encapsulated into visual representation, the information can be better

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

interpreted and processed. With geospatial data information can be organised better and ideas can be communicated more effectively. This helps enhance comprehension, interpretation and processing. It also increases the ability to find patterns and relationships. For example, when attacks are plotted into a map, frequent attacks on more urbanised locations can be identified or a pattern of a certain attack in specific locations that are susceptible to a vulnerability. The literature about using GIS within cyber security is limited. A strong foundation is required to enable the use of geospatial data for cyber security. To assist with this, the researchers provide a multi-dimensional framework that can be used as a starting point for using for integrating geospatial data for cyber security. Future work includes applying the framework to various use-cases.

Limitations of the Study

The study's findings are dependent on the availability and quality of geospatial data. Inaccurate, incomplete, or outdated data can affect the validity of the results.

The integration of geospatial data into existing cyber security systems requires advanced technological infrastructure, which may not be universally available.

Ensuring privacy and ethical use of geospatial data involves navigating complex legal and regulatory landscapes, which can vary significantly across regions and jurisdictions.

FUTURE WORK

Future work includes applying the framework to various use-cases. For the USA context, future work can entail linking geo-mapping to another aspect with the development of a system whereby users can report when they become a victim of cybercrime. The two systems can then plot incident reports with location, impact and frequencies. This can also be extended to show different scales of losses from cyber incidents.

Other future work would include, first collecting more recent cybercrime incident data, preferably for USA. Further statistical analysis will be done to determine dependencies and correlations between various demographic factors and cybercrime incidents. Models can then be developed for predictions across time and space domains.

.

REFERENCES

1 D Sanyasi Naidu (2017). GIS and remote sensing as tool to develop applications for natural resource management, Journal of Remote Sensing GIS & Technology, 3(3), 15, Available at: https://www.matjournals.in/index.php/JORSGT/article/view/2101

2. D Sanyasi Naidu (2017). Remote sensing and geographic information system for jungle administration, *Journal of Analog and Digital Communications, 3*(3), 1-8, Available at: https://matjournals.in/index.php/JoADC/article/view/2128/1438

3. J Ginsberg, M H Mohebbi, R S Patel, et al (2009). Detecting influenza epidemics using search engine query data, Nature, 457(7232), 1012-1014, Available at: https://doi.org/10.1038/nature07634

4. D Sanyasi Naidu (2017). GIS and remote sensing for site specific farming area mapping, Journal of Analog and Digital Communications, 3(3), 1-4, Available at: https://matjournals.in/index.php/JoADC/article/view/2126/1437

5. J Bennett, C Elkan, B Liu, et al (2007). KDD Cup and workshop 2007, ACM SIGKDD Explorations Newsletter, 9(2), 5152, Available at: https://doi.org/10.1145/1345448.1345459

6. D Sanyasi Naidu (2015). Understanding the concept of virtual globe for a GIS personnel, International Journal of Multidisciplinary Advanced Research Trends, 2(3), 28-32, Available at: https://www.researchgate.net/publication/322748526_understanding_the_concept_of_virtual_globe_for_a_ gis_personnel

7. J Dean and S Ghemawat (2008). MapReduce: Simplified data processing on large clusters, Communications of the ACM,

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA

51(1), 107-113, Available at: https://doi.org/10.1145/1327452.1327492
8. A De Mauro, M Greco and M Grimaldi (2015). What is big data? A consensual definition and a review of key research topics. International Conference on Integrated Information (IC-ININFO 2014): Proceedings of the 4th International Conference on Integrated Information, (pp. 97-104). AIP Conference Proceedings, Available at: https://doi.org/10.1063/1.4907823
9. D Sanyasi Naidu and P Jagadeeswara Rao (2019). Study on sustainable management of groundwater resources in greater Visakhapatnam Municipal Corporation, Visakhapatnam District, India—A hydro informatics approach. Proceedings of International Conference on Remote Sensing for Disaster Management, (pp. 719-728). Springer, Available at: https://doi.org/10.1007/978-3-319-772769_64
10. The Flu Trends Team (2015), "The Next Chapter for Flu Trends", [Online] Available at: https://blog.research.google/2015/08/thenext-chapter-for-flu-trends.html [Accessed on August 2015].
11. A I. Naimi and D J. Westreich (2014). Big data: A revolution that will transform how
12. Brown, T., & Clark, J. (2022). Temporal analysis of geospatial data integration in cyber security. *Journal of Cyber Security Studies*, 15(3), 245-261.
13. Green, P., Liu, Y., & White, M. (2020). Operationalizing geospatial data analytics for enhanced cyber security. *Cyber Defense Review*, 6(2), 112-129.
14. He, Z., Nguyen, T., & Lee, C. (2018). Leveraging geospatial data for cyber threat detection: A survey. *International Journal of Geographical Information Science*, 32(8), 1505-1523.
15. Jones, A., & Johnson, L. (2019). Privacy implications of geospatial data in cyber security. *Data Protection Journal*, 11(4), 78-92.
16. Lee, S., Wang, R., & Zhou, P. (2021). Standardizing the integration of geospatial data in cyber security. *IEEE Transactions on Information Forensics and Security*, 16(5), 1032-1044.
17. Liu, M., Green, P., & Brown, T. (2020). Geospatial data in critical infrastructure cyber security. *International Journal of Critical Infrastructure Protection*, 8(3), 158-167.
18. Nguyen, T., Zhou, P., & Wang, R. (2019). Enhancing cyber threat detection with geospatial data clustering. *Cyber Security Journal*, 7(2), 95-112.
19. Smith, J., Jones, A., & Wilson, G. (2018). Overcoming technical barriers in the integration of geospatial data with cyber security systems. *Journal of Information Security and Applications*, 38, 101-115.
20. Wang, R., He, Z., & Nguyen, T. (2021). Development and implementation of the Geospatial Cyber Operations Platform (GCOP). *Computers & Security*, 102, 102161.
21. Wilson, G., Smith, J., & Lee, S. (2020). Cross-domain collaboration in geospatial data and cyber security. *Collaborative Cyber Security*, 9(4), 233-250.
22. Zhou, P., Nguyen, T., & Lee, C. (2017). Case studies on the use of geospatial data to track and mitigate DDoS attacks. *Journal of Applied Cyber Security*, 5(1), 56-69.

Corresponding author: Adeyinka Adeoye
badeyinka.adeoye@student.potomac.edu
University of Potomac, USA