Application of Geospatial Data in Cyber Security

Namosha Veerasamy, Yaseen Moolla and Zubeida Dawood
CSIR, Pretoria, South Africa
nveerasamy@csir.co.za
ymoolla@csir.co.za
zdawood@csir.co.za

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.

Keywords: geospatial data, cyber security, geoinformatics, GIS

1. Introduction

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.

The contributions of the paper are summarised as follows:

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

This paper looks at these application areas to the domain of cyber security. The remainder of the paper is structured as follows: the next section provides some background on geospatial data. Thereafter, the framework of application areas is discussed. The researchers then conclude the paper and propose future work.

2. Geospatial data

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) (IBM 2022).

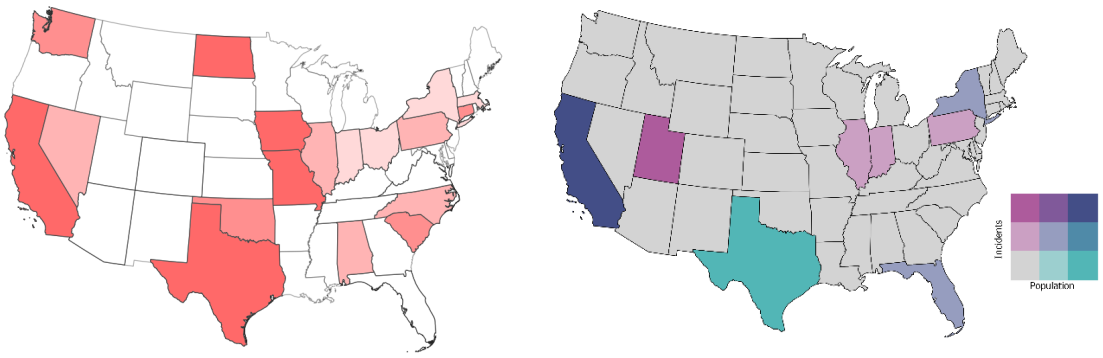
With geospatial analytics, timing and location can be added to common data types to produce useful visualisations. Visualisations can be in the form of maps, graphs, statistics and cartograms that can show changes over a period of time, as well as shifts in development. These visualisations offer more 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.

Examples of geospatial data include (IBM 2022):

- Vectors and attributes: Descriptive information about a location such as points, lines and polygons
- Point clouds: A collection of co-located charted points that can be re-contextured as 3D models
- Raster and satellite imagery: High-resolution images of our world, taken from above
- Census data: Released census data tied to specific geographic areas, for the study of community trends
- Cell phone data: Calls routed by satellite, based on GPS location coordinates
- Drawn images: CAD images of buildings or other structures, delivering geographic information as well as architectural data
- 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).



(a) (b)

Figure 1: Example Choropleth maps. (a) shows a monovariate choropleth map; and (b) shows a bivariate choropleth map, which visualises the correlation between two variables through two overlayed colour scales

The world is advancing at a rapid rate and there are more developments in the technological fields. With the rapid growth of ICT, comes the associated risks of cyber threats. Cyber threats also evolve as attackers adapt their methods of operation. Geospatial data can help better understand the changes that are taking place and

support the defence against threats through data analysis and powerful visualisations. Some questions that can be considered are:

- Where are cyber-attacks taking place?
- What are the locations of targets?
- What are the locations of the sources of attacks?
- What are the locations of intermediary infrastructure in cyber-attacks, e.g., proxy servers, digital post-boxes, and command and control servers?
- What type of cyber-attacks are occurring?
- What are the prime targets?
- What are the main methods used?
- How is the cyber-attack pattern changing over time?

Geospatial data and analytics can provide insight into these important questions by identifying the locations, types, targets, methods, as well performing comparisons.

Previously spatial data was cumbersome to use and required advanced software. However, with advances in processing and ICT, more domains can turn to spatial data to provide better insight and find solutions for problem areas. Smartphones, vehicle tracking, and satellites are helping to unlock the world of spatial and location data for organizations big and small (Safe.com).

Geospatial data now performs the functions that maps, compasses and smoke signals once fulfilled. Tracking people, populations, topography changes, events, storms and traffic can all be performed using geospatial data.

A key application area of geospatial data in the field of cyber security is tracking. Geospatial data can play a very strategic role for data analysis. It can help visualise the impact of a hacking group or see the plot of propaganda in social media feeds. Visualisation of the spread of cyber-attacks can create awareness of the scope and impact of these events. With geospatial data, cyber-attack data can be represented in an impactful manner. Location intelligence can be key to developing cyber intelligence. Connections can be shown, and links found, through the use of maps, descriptions and data fields. Graphical symbology is very useful in conveying critical pieces of information that makes it easier for the viewer to process.

Cybersecurity specialists can now also rely on geospatial data to improve security and build defensive mechanisms. Geospatial data is undervalued. Most organisations embrace the latest technology, but the vital capabilities of geospatial data can be missed. There is scant literature on using GIS for cyber security. Within the Florida University, researchers have mapped cyber-attacks to geospatial data (Zhiyong Baynard, Hongda & Fazio 2015). The geospatial analysis of this data had revealed spatial patterns, and identified countries that were more prone to cyber-attacks. Furthermore, hotspots within the United States were identified. Xui and Li performed some preliminary analysis on mapping IP addresses to a spatial database for geolocating cybercrimes (Xui W 2014). Bhargava et al. developed a framework for defining various types of cybercrimes based on laws in India, and analyse the spatial distribution of cybercrimes across India (Bhargava 2015). In the military domain, German cybersecurity experts integrated GIS with cybersecurity tools to discover patterns from cyber attacks (Conklin B 2022). In the commercial space, Kaspersky (Kaspersky 2021), Bitdefender (Bitdefender 2022), and Fortinet (Fortinet 2022) provide maps to visualise threats that are detected by their respective software suits. It is unclear what further processing and analysis, beyond processing, is performed on their geospatial data.

Geospatial data can the ability to strengthen cyber security by providing a wealth of information. This paper summarises various benefits and application areas for the use of geospatial data in the field of cybersecurity. The proposed framework that discusses the applications are as follows.

3. Framework

The authors were 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):

- Retail: income, housing/rent prices, population, age
- Weather patterns: hurricanes, tornadoes, extreme winter weather
- Site identification: traffic patterns, foot traffic, number of residents, competitor information
- Healthcare: water location, drug users, environmental hazards, vaccines,
- Financial services: visualise real estate, track construction over time, analyse investments without travel
- 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.

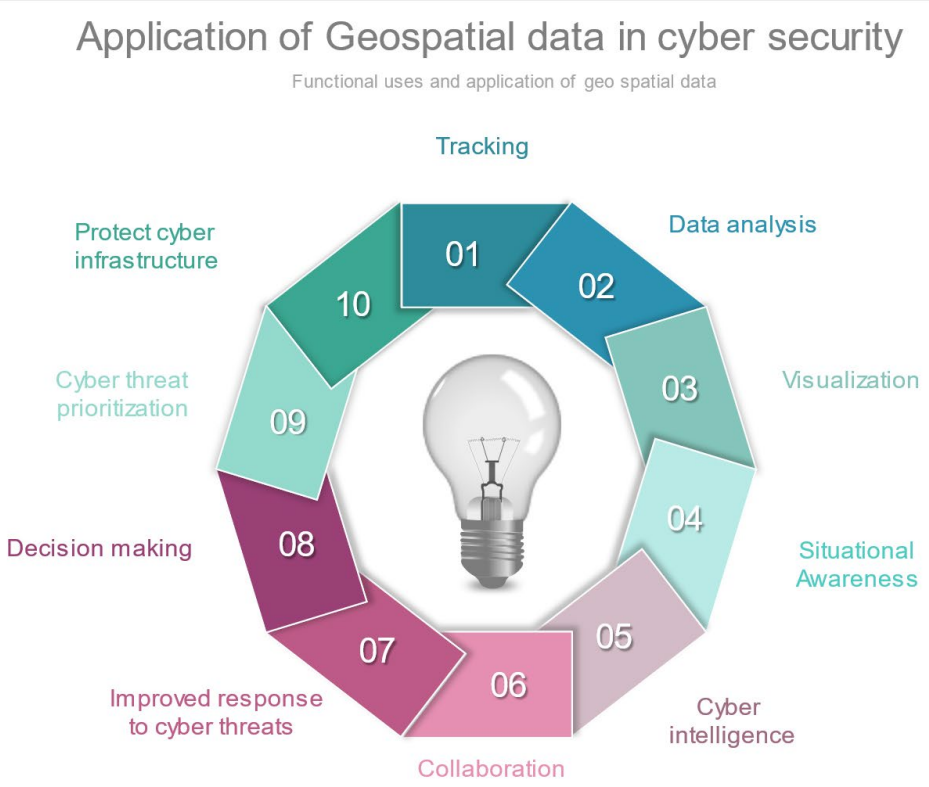


Figure 2: Application of geospatial data to cyber security

The framework summarises 10 principal application areas which are:

- Tracking
- Data analysis
- Visualisation
- Situational awareness

- Cyber intelligence
- Collaboration
- Improved response to cyber threats
- Decision-making
- Cyber threat prioritisation
- Protect cyber infrastructure

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.

3.1 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.

3.2 Data analysis

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.

3.3 Visualisation

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.

3.4 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.

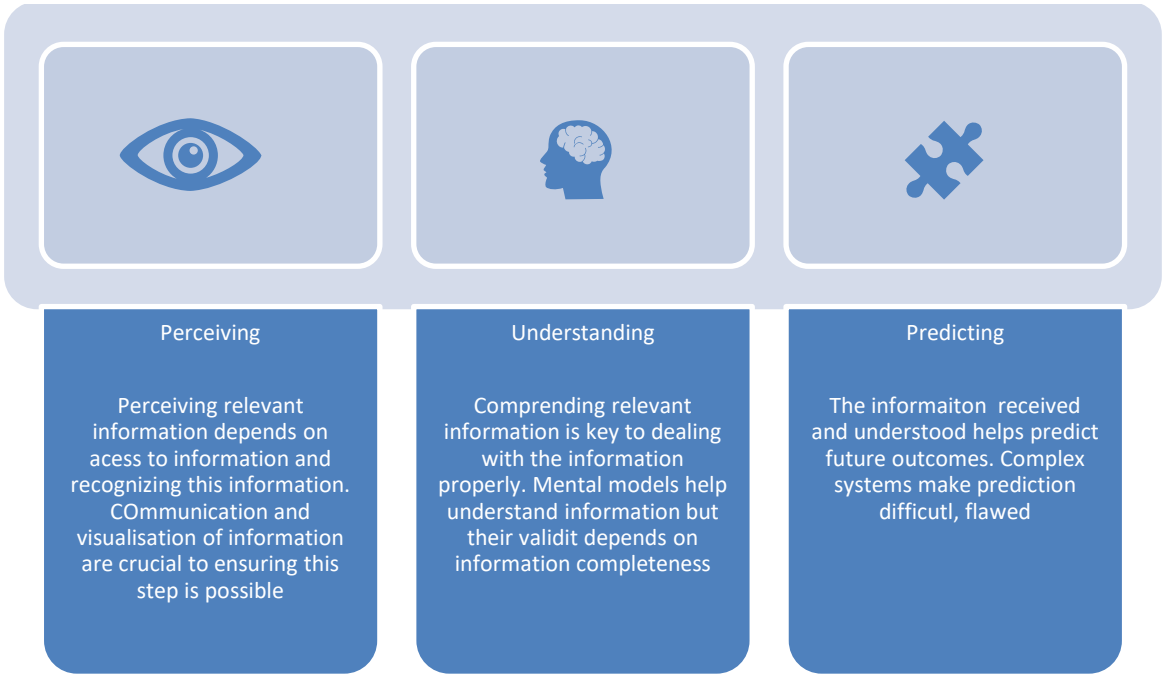


Figure 3: Steps in situational awareness (Endsley 1995)

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 (Shiftelearning, 2021):

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

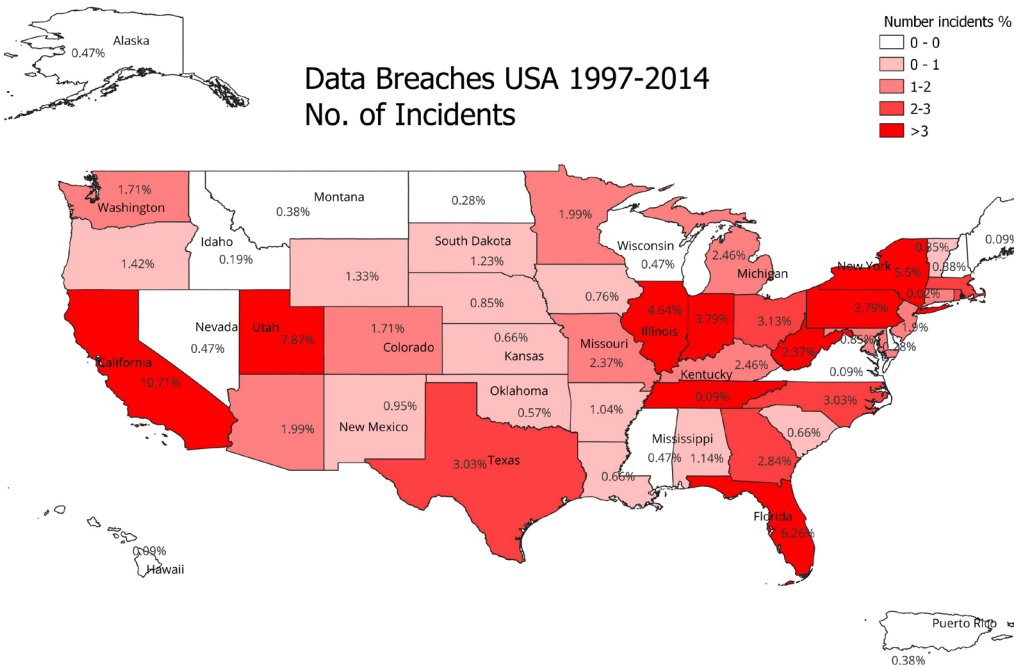


Figure 4: Map to indicate data breaches in states of the USA. Map developed using QGIS

3.5 Cyber intelligence

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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

4. 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 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.

5. Future work

Future work includes applying the framework to various use-cases. For the South African 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 South Africa. 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

Bitdefender, 2022 Cyberthreat Real-time Map, [Online] Available at https://threatmap.bitdefender.com/, Accessed 26 January 2022.

Bhargava, N., Bhargava, R., & Tanwar, P. S. ,2015. Analysing and Implementing Spatial Distribution of Cyber Crime Trends in India. *International Journal of Advanced Research in Computer Science*, *6*(4).

Brode B, 2021, Why cybersecurity experts want more geospatial data, Geospatial World, [Online] Available at https://www.geospatialworld.net/blogs/why-cybersecurity-experts-want-more-geospatial-data/, [Accessed 19 January 2022].

Conklin B, 2022 Cybersecurity: The Geospatial Edge, [Online] Available at https://www.esri.com/about/newsroom/blog/german-cybersecurity-experts-use-gis/ Cybersecurity: The Geospatial Edge, [Accessed 25 January 2022].

CQ Net, 2022, Situational awareness: What it is and why it matters as a management tool, [Online] Available at https://www.ckju.net/en/dossier/situational-awareness-what-it-and-why-it-matters-management-tool, [Accessed 20 January 2022].

Datumize, 2020, The top five advantages of data visualisation, [Online] Available at https://blog.datumize.com/top-five-advantages-of-data-visualization, [Accessed 20 January 2022].

Fortinet, Inc. ,2022, Fortiguard Map, [Online] Available at https://threatmap.fortiguard.com/, [Accessed 26 January 2022].

Endsley, MR , 1995, Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64. Human Factors: The Journal of the Human Factors and Ergonomics Society. 37. 32-64. 10.1518/001872095779049543.

IBM, 2022, What is geospatial data?, [Online] Available https://www.ibm.com/topics/geospatial-data, [Accessed 21 January 2022].

Kaspersky Labs ,2021, Cyberthreat Real-time Map, [Online] Available at https://cybermap.kaspersky.com, Accessed 26 January 2022.

Safe.com, 2022, What is spatial data?, [Online] Available https://www.safe.com/what-is/spatial-data/, [Accessed 21 January 2022].

Shiftelearning, 2021, Studies Confirm the Power of Visuals to Engage Your Audience in eLearning, [Online] Available at https://www.shiftelearning.com/blog/bid/350326/studies-confirm-the-power-of-visuals-in-elearning, [Accessed 20 January 2022].

Trajectory Magazine, 2022 The Past, Present, and Future of Geospatial Data Use, [Online] Available at https://trajectorymagazine.com/past-present-future-geospatial-data-use/, [Accessed 21 January 2022].

Xui W 2014 Xiu, W., & Li, X. (2014, April). The design of cybercrime spatial analysis system. In *2014 4th IEEE International Conference on Information Science and Technology* (pp. 132-135). IEEE.

Zhiyong H, Baynard, CW, Hongda H, Fazio, M , 2015. GIS mapping and spatial analysis of cybersecurity attacks on a Florida university, *IEEE 2015 23rd International Conference on Geoinformatics* , Wuhan, China (2015.6.19-2015.6.21).