Enhancing Cybersecurity through the Integration of Geographic Information Systems Technologies

Georgi Pavlov[1], Nedko Tagarev[2]

[1]UNWE, Sofia, Bulgaria
Email: *gpavlov[at]unwe.bg,*

[2]UNWE, Sofia, Bulgaria
Email: *ntagarev[at]unwe.bg*

Abstract: ***This article explores the integration of Geographic Information Systems GIS with cybersecurity to enhance threat analysis, incident response, and overall network security. Cybersecurity systems can achieve higher efficiency and effectiveness by leveraging GIS data for spatial analysis and real - time monitoring. Integrating SCADA systems further enables comprehensive monitoring and management of external and internal environments. This study also discusses the application of machine learning in automating data analysis for cybersecurity, providing a cyclical improvement in security processes. The article analyses the effect of cybersecurity through GIS technologies.***

Keywords: Cybersecurity, Geographic Information Systems, Threat Analysis, SCADA Systems, Machine Learning

1. Introduction

"The scientific publication is in fulfillment of the objectives of the National Scientific Program "Security and Defense", financed by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the Decision of the Council of Ministers No.731 of October 21, 2021 and according to Agreement No. D01 - 74 /19.05.2022. "

When it comes to cybersecurity, data analysis and output are crucial elements. The output serves as a trigger that activates cybersecurity instruments in the event of an attack or incident. Gathering and analysing additional data from multiple sources can provide a more comprehensive understanding of the system. This, in turn, can enhance the effectiveness and efficiency of security systems such as IDS, IPS, and DMZ, as well as security concepts like Antivirus and Zero trust.

We cannot collect data manually because of millions of IT (Information Technologies) systems, billions of users, and IT components. Manual data collection is very costly due to the vast number of IT systems, users, and components. Therefore, to improve the process's efficiency and make our security sustainable, we must automate the collection and analysis of data. The instruments that are usable for that are GIS and SCADA. Also, if we implement ML (Machine Learning), adding additional data analyses for threats, vulnerabilities, and process effectiveness, we can improve the inclusivity of self - learning.

We should remember that cybersecurity is a cyclical process that improves with each evaluation, regardless of the number of tools we deploy.

We use SCADA and GIS for different purposes. Therefore, SCADA and GIS are utilised in most cases for different purposes. However, we can use them together to provide a more comprehensive cybersecurity strategy. We use SCADA systems to monitor and control industrial processes and operations. SCADA systems collect real - time data from sensors and other devices. We use it to control and optimise operations and processes. We use GIS to manage and analyse spatial and geographic data. GIS systems for different planning applications such as urban planning, environmental management, and disaster response. GIS systems visualise and analyse data to make informed decisions. [1]

Through GIS, we monitor the external environment for cyber security; through SCADA, we monitor the organisation's internal environment. Implementing both systems allows the organisation of cyber security in large networks, for example, at the national level. For each of them, we can visualise a process.

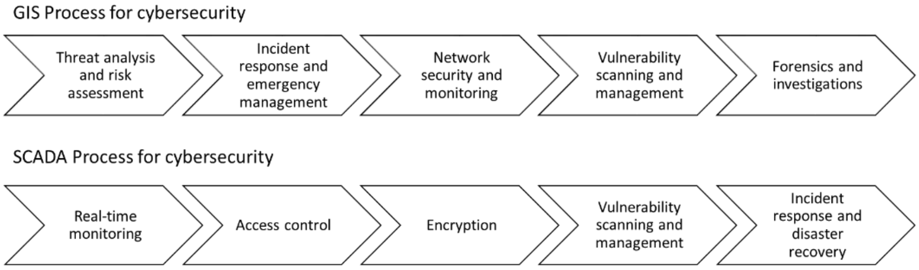

GIS Process for cybersecurity
Threat analysis and risk assessment
Incident response and emergency management
Network security and monitoring
Vulnerability scanning and management
Forensics and investigations
SCADA Process for cybersecurity
Real-time monitoring
Access control
Encryption
Vulnerability scanning and management
Incident response and disaster recovery

Figure 1: GIS and SCADA processes for cybersecurity: [source authors]

- Threat analysis and risk assessment

Map and analyse threats to critical infrastructure, visualise threats and analyse risk factors. Organisations identify vulnerabilities and develop risk mitigation strategies.

- Incident response and emergency management
  Map and track cyber incidents in real - time. Quickly respond to mitigate the impact of cyber attacks. Identify critical infrastructure and assets that may be at risk during emergencies.
- Network security and monitoring
  Map and monitor network activity. We identify potential intrusions and monitor user activity by Visualising network activity. Identify suspicious activity and respond quickly to potential threats.
- Vulnerability scanning and management
  Map and analyse vulnerabilities in networks and infrastructure. We are identifying potential attack vectors and assessing the risk of specific vulnerabilities. Prioritise and manage vulnerabilities to reduce the risk of cyber - attacks.
- Forensics and investigations
  We map and analyse data related to cyber incidents. We identify the source of attacks and track the spread of malware. We visualise relationships between different data points, helping investigators identify patterns and connections.
- Real - time monitoring
  We monitor networks and systems in real - time, detect and alert operators to potential cyber threats, identify potential intrusions, and respond quickly to mitigate the impact of cyberattacks.
- Access control
  We control access to networks and systems. We implement multi - factor authentication and role - based access control to reduce the risk of unauthorised access and limit the potential impact of cyber - attacks.
- Encryption
  Protect sensitive data, including data in transit and at rest. Protect against unauthorised access and ensure that critical data is kept secure.
- Vulnerability scanning and management
  We scan networks and systems for vulnerabilities. We identify potential attack vectors and assess the risk of specific vulnerabilities. We prioritise and manage vulnerabilities.
- Incident response and disaster recovery
  We develop incident response plans and disaster recovery plans. We also identify critical infrastructure and assets that may be at risk.

Th**is article** aims to analyse the integration of Geographic Information Systems GIS with cybersecurity frameworks to enhance the effectiveness of threat analysis, risk management, and incident response.

This *article is significant* as it provides insights into how integrating GIS with cybersecurity can improve monitoring and response capabilities, ultimately enhancing the overall security infrastructure.

2. Literature review

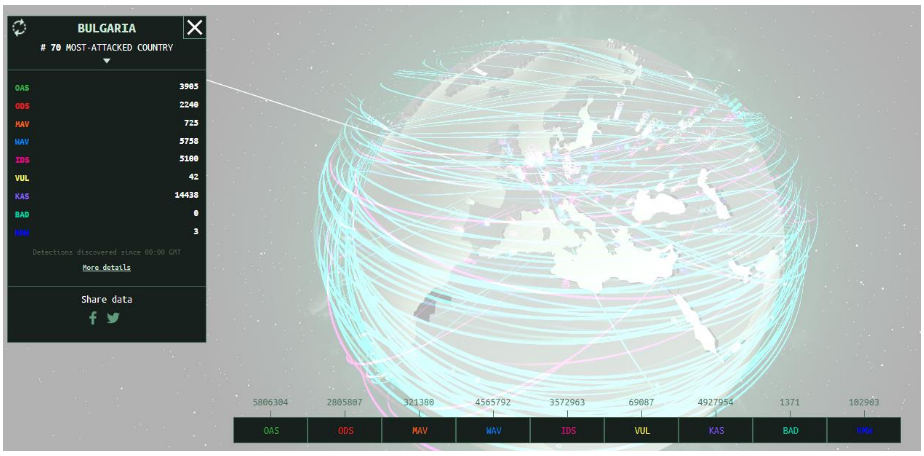
In GIS, the features we use to identify the network connections are - service, protocol, number of login attempts, packets per flow, bytes per flow, source address, destination address, source port, destination port, and others. The model records the feature values, and the anomaly detection engine will mark any deviation in recorded values as anomalous. Techniques in anomaly detection can be categorised into three types - Machine Learning, Statistical Techniques and Finite State Machines. [2] GIS security is a property characterising the resistance to the emergence of hazardous situations, i. e. those in which the need arises to protect the internal values of the GIS system from external threats or threat factors. [3] The primary feature that will assist cybersecurity is GIS - IDs. By this technique, the model establishes relations 1: 1, 1: m, m: 1 and m: n. This model means that multiple elements in the model can share the same GIS ID or represent multiple elements in the GIS. [4]

Geospatial data can assist in identifying and prioritising cyber threats. It can also assist in identifying critical areas of concern. Although discovering patterns or trends in large data sets can be a daunting task, the graphical capabilities of geo - mapping make it easier to present data clearly and concisely. This data can help analysts detect emerging issues, threats, and target areas more efficiently. [5] The geospatial technology in the support of physical security is well - known and understood. It is used for situational awareness, data management, multiple intelligence (multi - INT) fusion, analysis, and information sharing. The goal is to enable early detection and organisation - wide agility when responding to cyber intrusions. [6] GIS can pinpoint and help determine when an attack occurs, providing a layer of cybersecurity through spatial analytics. IP addresses are used to launch malware, with the pattern of attacks used to provide an overall pattern and suggest where the main attack originated [7]. A bird's eye view of all network infrastructure could allow GIS security experts to assess numerous factors and determine where an attack originated. With artificial intelligence and machine learning, better prediction methods can be attained, allowing for pre - emptive defence. [8]

A key application area of geospatial data in cyber security is tracking. Visualising the spread of cyber - attacks can raise awareness of their impact and scope, including the plot of propaganda in social media feeds. Location intelligence can be vital to developing cyber intelligence. Connections can be shown, and links can be found using maps, descriptions, and data fields. Graphical symbology is especially useful in conveying critical information that makes it easier for the viewer to process. [9]

Powerful GIS platforms (e. g., ArcGIS), once integrated with the company's cyber security tools, can enhance the management of data, information sharing, analytics, and fusion. For example, Secure Access Service Edge (SASE) technology can take the integration of cyber and geospatial technologies and data even further. SASE analyses the data and compiles it into the company's context. [10] Government intelligence agencies and private companies rely on individuals with experience in GIS. Cybercriminals are highly attracted to GIS data because GIS systems affect many customers. Most GIS systems are connected through the internet and cluster networks. [11] Cyberspace geography (CG) expands geographical research from physical to virtual spaces. CG research maps relationships between cyberspace and the physical world, redefines geographic concepts, and visually represents cyberspace. It studies the principles governing cyberspace structures and behaviours.

The technical methods of CG involve gathering and integrating data on cyberspace elements, visually representing cyberspace, and conducting situational and behavioural intelligence awareness in cyberspace. [12]



BULGARIA
70 MOST-ATTACKED COUNTRY

OAS	3905
ODS	2240
MAV	725
WAV	5758
IDS	5100
VUL	42
KAS	14438
BAD	0
RMW	3

Detections discovered since 00:00 GMT

More details

Share data

OAS	ODS	MAV	WAV	IDS	VUL	KAS	BAD	RMW
5806304	2805807	321380	4565792	3572963	69087	4927954	1371	102903

Figure 2: Visualisation of the attacks in real - time [source: https: //cybermap. kaspersky. com/ **[13]**]

A new feature type is called Behaviour Change Detector – BCD and it is obtained as follows: during a slot of time, the events which match some conditions are counted; the process is made again in the next slot of time, and its results are compared with the previous value in last time. The BCD feature is the difference between the counted events in the actual period and the last period. It can detect abrupt changes in the network traffic behaviour. [14]

Fortunately, spatial information (*note 4*) can also directly assist security experts in detecting unauthorised activity. GIS promotes situational awareness across multiple departments by providing clear visualisations of the systems involved in an incident. [15]

The role of entities dealing with spatial information is to ensure the security and integrity of data. The first legal act that imposed obligations in data security, obliging them to ensure confidentiality, integrity, availability, and resilience of the systems, was the Regulation on the Protection of Personal Data. [16] Machine learning - based phishing detection is a burgeoning research topic, with deep learning approaches increasingly being used. A method for detecting phishing websites and their targets based on features from URLs and web page links. [17] A study has shown that machine learning algorithms can effectively and efficiently detect and categorise phishing websites as security threats. Machine learning provides simplified and efficient methods for data analysis. Machine learning models can be helpful in phishing because it is a categorisation challenge. Machine learning models swiftly adapt to changes to identify fraudulent transaction patterns, which would aid in developing a learning - based identification system. [18]

Creating Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) counteracts cyberattacks. These systems monitor network activity in real time and retain information for subsequent analysis and reporting on cybersecurity. One well - known and proven practical countermeasure approach that fits into IDS/IPS measures is terminologically known as a honeypot (see Note 1). NGIPS tools have evolved to include application and user control features that enable them to detect a wide range of attacks. In addition, some NGIPS tools offer sandboxing capabilities for automatic and manual inspection of potential malware. Many of these features have also been incorporated into other security solutions, such as Next - Generation Firewalls (NGFW), Unified Threat Management (UTM), and Extended Detection and Response (XDR) tools. Endpoint Detection and Response (EDR) tools can also function as host - based IPS for endpoints to a certain extent. [19] An intrusion detection system (IDS) can effectively identify anomalous behaviours in the network. However, it still has a low detection rate and a high false alarm rate, especially for anomalies with fewer records. [20]

GIS data can be integrated into cybersecurity tools to enhance their effectiveness. An Intrusion Detection System/Intrusion Prevention System (IDS/IPS) is essential for storing data for future analysis and reporting. It is crucial to hire a different company to code and build organisation IDS/IPS instead of relying on the same company that codes and builds an organisation security system. Additionally, it is essential to physically separate the two systems to ensure they are not blind to the same vulnerabilities and exploits. Even if we have an appliance that combines a firewall and an IDS/IPS, it is still necessary to have a separate layer of IDS/IPS protection behind our firewall to have a defence - in - depth strategy. For complete protection, good practice is recommended that we install a network IDS/IPS at every entry point to our organisational network. Additionally, we should place a host IDS/IPS on our most critical servers to prevent intrusion and a wireless IPS to protect our wireless internet connection against potential attacks. This IPS will ensure that we guard our network from all possible threats. [21]

Another instrument for cybersecurity is DMZ (de - militarised Zone). A DMZ is a physical or logical subnet that isolates a LAN from untrusted networks like the public internet. Any service offered on the public internet should be in the DMZ network. We typically locate the external - facing servers, services, and resources in the DMZ. These services include web, DNS, e - mail, proxy servers, FTP, and VoIP. [22]

The third instrument that can be applied is the "honeypot". We base our approach on drawing the attention of attackers to an individual server or network service that is intentionally left not fully protected. Data about the attacker's actions is gathered when attempting to infiltrate an inadequately protected network resource. The collected information is then analysed to identify the techniques used to execute the cyber - attacks, and practical strategies and solutions to counter them are determined. For this reason, we investigated the potential for a standardised set of MoE (measure of effect) related to standard dynamic honeypot features. Twenty articles of primary research served as the foundation for our analysis. Based on this data set, we selected four quantitatively assessable characteristics of honeypots to measure their effectiveness as honeypots and assembled the components into a taxonomy. The proposed model establishes this as fingerprinting, data capture, deception, and intelligence. Collectively, these should be successful in quantitatively assessing dynamic honeypots. [23]

Honeypots can be installed on public servers, in DMZs, behind firewalls, or on user computers to gather data on sophisticated attacks. As a specific implementation, a honeypot can be a separate server configuration, a virtual machine pre - configured for the purpose, or a software solution installed on a user's computer in the network. Another scenario for organising a honeypot in the sense of protecting wireless networks is to attract the attacker to interact with the fake resources of the system, which prevents the attack on valuable resources. [24] It is a security best practice to implement a perimeter network, also known as a de - militarised zone (DMZ) or screened subnetwork, to prevent external users from directly accessing your ArcGIS Server site. A perimeter network is the only exposed point in our network that is accessible to external users. It adds a layer of security to an organisation's network. [25] ArcGIS Server is a software component that functions as a back - end for ArcGIS Enterprise. Its primary purpose is to provide access to our geographical information to other members of our organisation and, optionally, to anyone with an internet connection. GIS services facilitate this by enabling a server computer to receive and process information requests from other devices. [26] We must remember that firewalls and DMZ do not significantly impact security when the applications and OSes have few or too many vulnerabilities. When the operating systems are not vulnerable, but the applications are, the effectiveness of firewalls and DMZs in providing security decreases as the percentage of vulnerable applications increases. [27] A DMZ significantly enhances the security of a network. A DMZ adds an extra layer of protection to the network. It is also used to protect confidential information. A DMZ should be appropriately configured to increase the network's security. This work reviewed DMZ and its importance, design, and effect on network performance. [28]

2. Mutual beneficial model by implementing GIS for cybersecurity

In most cases, GIS and SCADA systems are objects for protection by the cybersecurity system. The first benefit that we can achieve by implementing their resources in cybersecurity is the unification of policy and standards between business processes and goals and, on the other side, security processes and goals. Machine learning plays a considerable role in the implementation of GIS in cybersecurity. Machine learning automates the process of analysing data usable for cybersecurity, which the system collects from internal digital infrastructure by SCADA and the external environment by GIS.

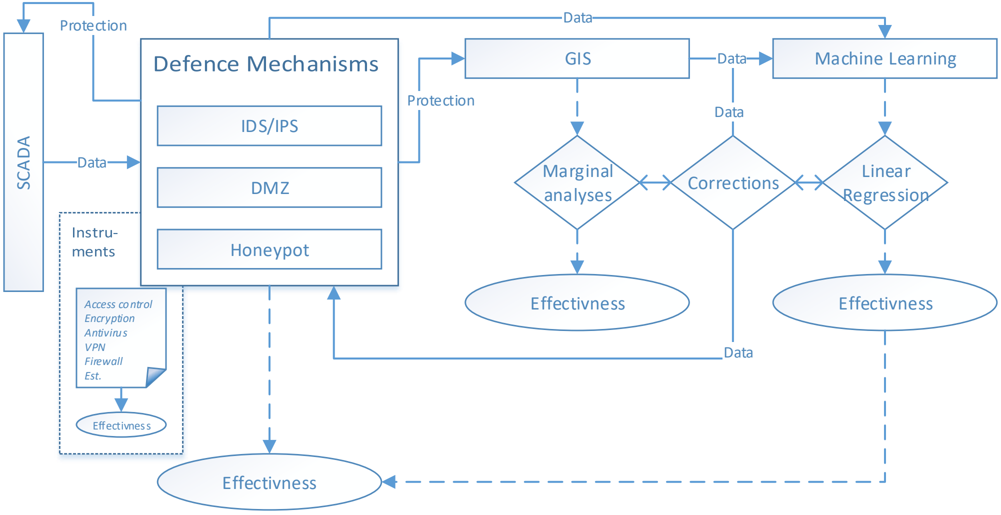


Figure 3: Model for implementing GIS in cybersecurity system [source authors]

The most critical aspect of implementing instruments and products for cybersecurity is their effectiveness. The best solution is to create quantity metrics for measurement. To evaluate the overall effect, we must measure the effects/benefits of each system element. For example, GIS and SCADA alone do not provide protection but need one. GIS provides data. With data quality being a critical factor in managing utility networks, ensuring that both future and existing data meet necessary quality standards is essential. Reviewing and evaluating data quality, examining relationships to other networks, and analysing attribute data are essential to creating reliable networks. [29]

For this data, its usefulness for cybersecurity – its quality and quantity. We achieve quality and quantity by adding to the system marginal analyses and evaluating the marginal utility of the data. For measuring GIS effectiveness is measured by the Capability Maturity Model (CMM). The main objective of this model is to define the characteristics of each 'maturity stage' and to provide a step - by - step approach that enables an organisation to measure its GIS capabilities. Using this model, an organisation can develop a plan to progress from one maturity stage to another. [30]

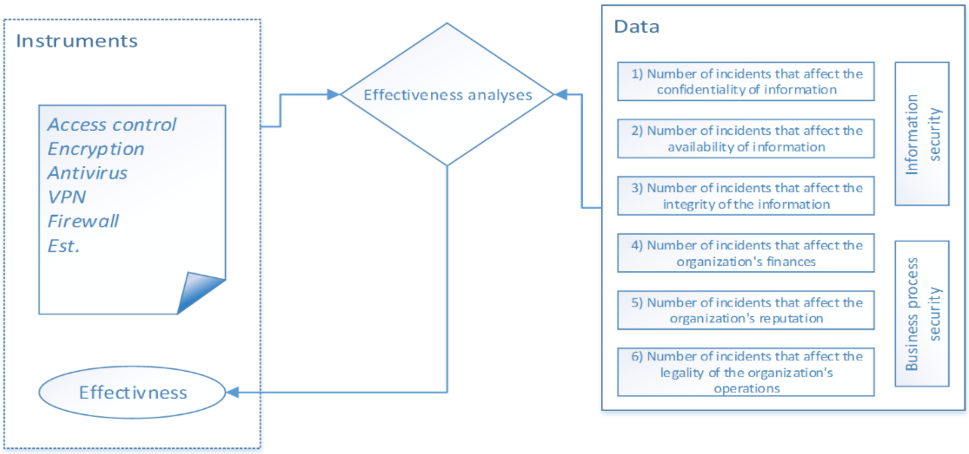

Instruments
Access control
Encryption
Antivirus
VPN
Firewall
Est.
Effectivness
Effectiveness analyses
Data
1) Number of incidents that affect the confidentiality of information
2) Number of incidents that affect the availability of information
3) Number of incidents that affect the integrity of the information
4) Number of incidents that affect the organization's finances
5) Number of incidents that affect the organization's reputation
6) Number of incidents that affect the legality of the organization's operations
Information security
Business process security

Figure 4: Model for the evaluation of the effectiveness of instruments for cybersecurity [source authors]

To improve the effectiveness of the instruments, we can add data from the outside environment by implementing GIS data collection. We can apply this principle to every product, regardless of manufacturer.

3. Example

GIS for network security

In the described case, with the need for cyber protection in a wireless network, a crucial factor is the size of the covered territory. Building a honeypot security network, it is possible to implement Internet of Things (IoT) devices with built - in wireless connectivity capabilities. Data from freely available sources show a typical distance of stable wireless connectivity in the line - of - sight range of up to 70 m using the built - in antenna, up to 600 m using an external antenna, within the legally permitted radio emission power.

When deploying a wireless security network in urban conditions, the effective distance of connectivity decreases due to radio - technical effects caused by the presence of infrastructure objects, buildings, and other built - up areas. In this regard, the availability of a database with three - dimensional models of built - up urban areas is a crucial condition for designing cyber defences with the application of wireless honeypot networks.

In the specification referred to above, building data is maintained with different levels of detail coverage, both in geometry and specific structural features. Generally, the 3D representation of buildings is an extended version of the CityGML standard of the organisation developing GIS technologies - the Open Geospatial Consortium (OGC). Automated data extraction from files in the CityGML format boils down to applying a software tool to analyse the content of the XML (eXtended Markup Structure) structure. The format is suitable for software processing using UML (Unified Modeling Language) modelling.

The other considered variant of a three - dimensional representation of buildings in Google Earth, 3D Imagery, basically uses the principle of stereo photogrammetry [31]. This high - tech approach has made it possible to synthesise and provide for the visualisation of three - dimensional models of built - up areas for extensive territories, including the largest settlements in the Republic of Bulgaria. Third - party software manufacturers offer a solution for extracting a 3D model in a standardised file format; its use is subject to compliance with existing Google Incorporation® license agreements.

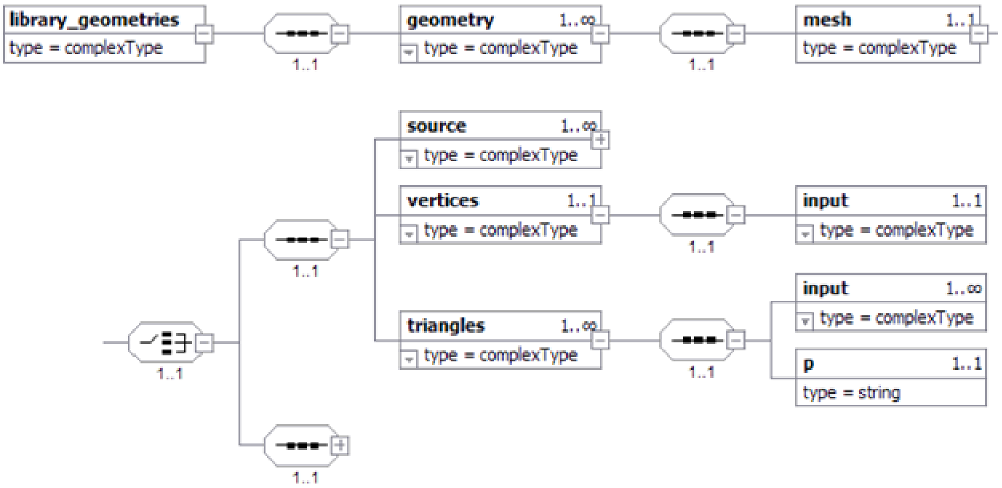


Figure 5: Geometric characteristics using the COLLADA file format when representing Legacy 3D Buildings **[31]**

In Fig.6, Screens from Google Earth show a 3D view of an urban area in different system variants.

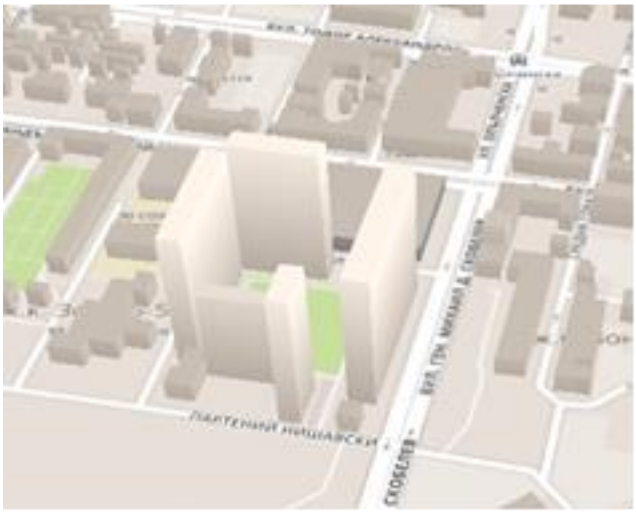
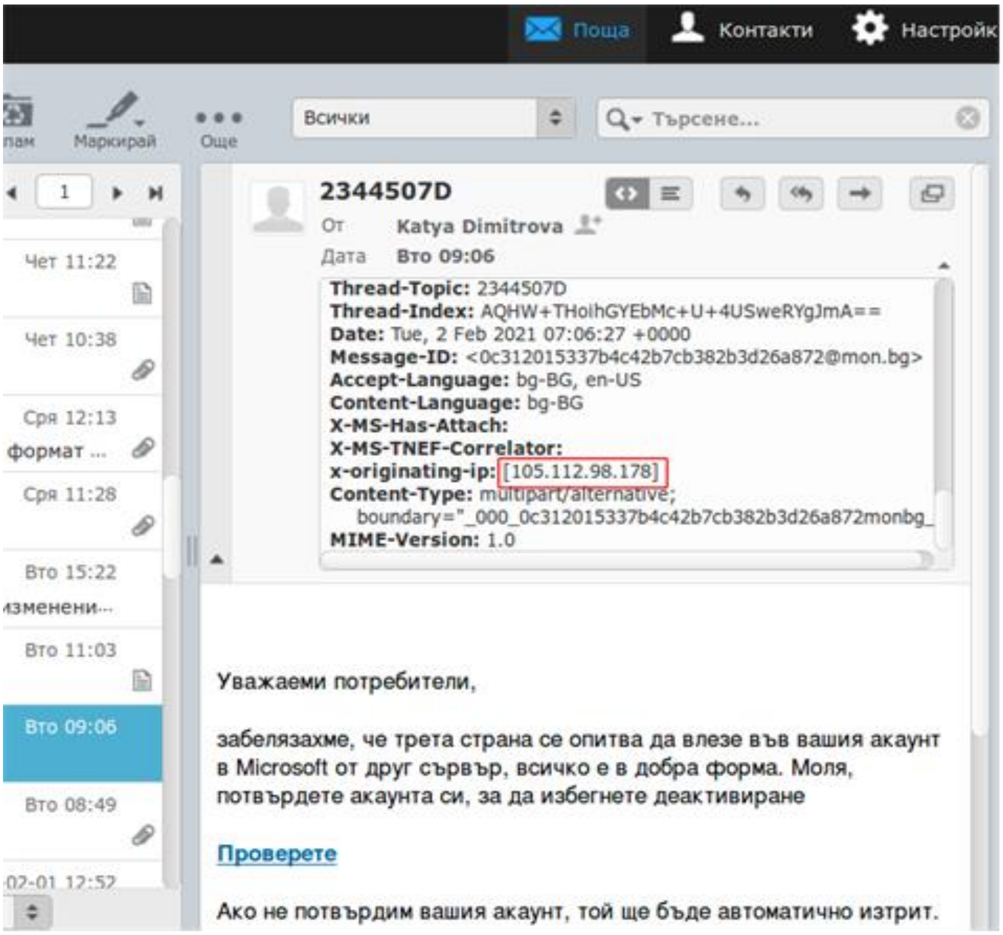


Figure 6: View in Simple 3D Buildings format **[**source: Pavlov. G., Kibersigurnost I geografski informacionni tehnologiiq prilojimi kum pandemiqta COVID - 19”, Modelirane, analiz I optimizirane na socialno - ikonomicheskite merki za namalqvane na negativnite posledici ot pandemiqta Covid - 19, Avangard Prima, 2023**] [33]**

GIS against cyber fraud

Using e - mail is often accompanied by receiving unexpected messages that invite us to perform specific actions. When a user suspects a malicious spoofing or phishing attack (see Notes 2 and 3), a good approach is to verify the source of the e - mail. Fig.4 shows an e - mail screen with an enabled "message details" option.

In essence, the message has been sent by the Bulgarian representative office of the well - known company Microsoft and invites the user to activate a link in the message. The originating IP address of the mail server, 105.112.98.178, is crucial to verifying the message's authenticity.



2344507D
От Katya Dimitrova
Дата Вто 09:06

```
Thread-Topic: 2344507D
Thread-Index: AQHW+THoihGYEbMc+U+4USweRYgJmA==
Date: Tue, 2 Feb 2021 07:06:27 +0000
Message-ID: <0c312015337b4c42b7cb382b3d26a872@mon.bg>
Accept-Language: bg-BG, en-US
Content-Language: bg-BG
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
x-originating-ip: [105.112.98.178]
Content-Type: multipart/alternative;
   boundary="_000_0c312015337b4c42b7cb382b3d26a872monbg_
MIME-Version: 1.0
```

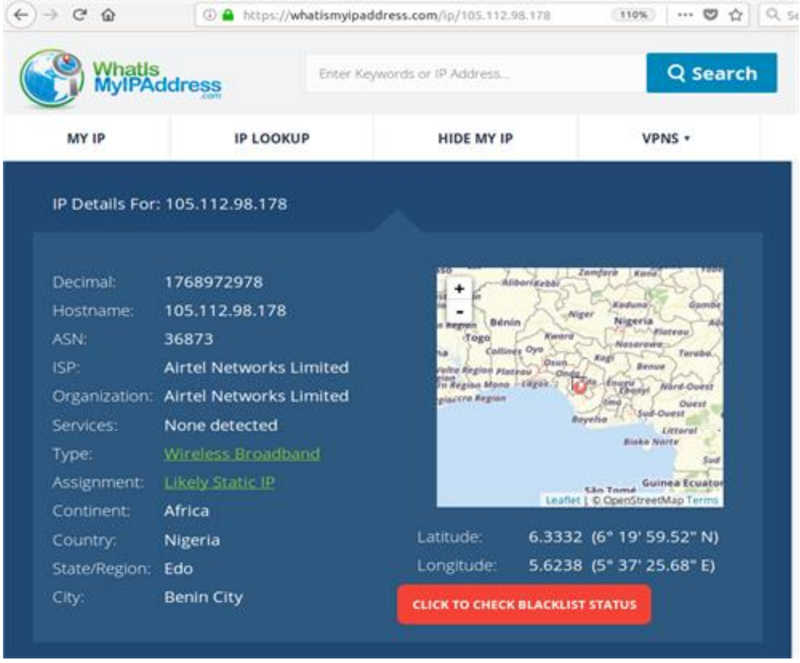
Уважаеми потребители,

забелязахме, че трета страна се опитва да влезе във вашия акаунт в Microsoft от друг сървър, всичко е в добра форма. Моля, потвърдете акаунта си, за да избегнете деактивиране

Проверете

Ако не потвърдим вашия акаунт, той ще бъде автоматично изтрит.

Figure 7: Details of the checked e - mail **[**source: Pavlov. G., Kibersigurnost I geografski informacionni tehnologiiq prilojimi kum pandemiqta COVID - 19”, Modelirane, analiz I optimizirane na socialno - ikonomicheskite merki za namalqvane na negativnite posledici ot pandemiqta Covid - 19, Avangard Prima, 2023**] [33]**


https://whatismyipaddress.com/ip/105.112.98.178
110%
WhatIs MyIPAddress.com
Enter Keywords or IP Address...
Search
MY IP
IP LOOKUP
HIDE MY IP
VPNS ▾
Benin
Nigeria
Togo
Leaflet | © OpenStreetMap Terms
CLICK TO CHECK BLACKLIST STATUS

IP Details For: 105.112.98.178

Decimal: 1768972978
Hostname: 105.112.98.178
ASN: 36873
ISP: Airtel Networks Limited
Organization: Airtel Networks Limited
Services: None detected
Type: Wireless Broadband
Assignment: Likely Static IP
Continent: Africa
Country: Nigeria
State/Region: Edo
City: Benin City

Latitude: 6.3332 (6° 19' 59.52" N)
Longitude: 5.6238 (5° 37' 25.68" E)

Figure 8: Geolocation of checked mail server **[**source: Pavlov. G., Kibersigurnost I geografski informacionni tehnologiiq prilojimi kum pandemiqta COVID - 19", Modelirane, analiz I optimizirane na socialno - ikonomicheskite merki za namalqvane na negativnite posledici ot pandemiqta Covid - 19, Avangard Prima, 2023**] [33]**

GIS against cyber fraud

4. Conclusion

The integration of Geographic Information Systems GIS with cybersecurity frameworks offers significant improvements in threat analysis, incident response, and overall network security. By leveraging spatial data and real - time monitoring, organisations can achieve a comprehensive security strategy. Implementing machine learning techniques further enhances the effectiveness of these systems, ensuring continuous improvement in cybersecurity measures.

By applying web - based GIS functionality, it is possible to verify the geographical location of the mail server of the sender of the electronic message with high reliability. For this purpose, the available Internet service with the common name IP Lookup is used.

Fig.8 shows the result of executing the request https: //whatismyipaddress. com/ip/105.112.98.178. The user sees that the misleading e - mail from the Bulgarian Microsoft representative is from Africa, Nigeria, and Benin.

To prevent this type of cyber fraud attempt, a user interface for automated geolocation verification of a suspicious e - mail server could be created.

The existing WEB resource https: //www.ip2location. com allows registered users to submit a request for geo referencing an IP address using the c URL software tool, available in Windows versions after April 2018. In other cases, when using cURL from a local computer is difficult, a working approach is to address an intermediate server's web page using an asynchronous XMLHttpRequest (City Geography Markup Language) [32].
Integrating SCADA and GIS can provide operators with real - time data and spatial analysis to make informed decisions. This integration can improve operational efficiency, reduce costs, and enhance overall performance. However, it is crucial to implement proper cybersecurity measures to safeguard SCADA and GIS systems from cyber threats.

Notes

1) "honeypot". The practical application of such software systems allows us to perform in - depth analyses of cybersecurity risks and determine potential attacks and their perpetrators based on accurate data. Installing and monitoring a honeypot is helpful and dramatically helps cybersecurity teams and system administrators.
2) Spoofing is a deceptive technique used by criminals to make you believe you are interacting with a trusted source by disguising an e - mail address, sender name, phone number, or website URL. They often change just one letter, symbol, or number to make the victim believe the communication is authentic. The victim may receive an e - mail that appears to be from their boss or even someone in their family, but it is not. The criminals manipulate their victims into believing that these fraudulent communications are genuine, which can lead them to download malware, disclose personal, financial, or other sensitive information, or even send money.
3) Phishing schemes are online frauds that use deceptive tactics to entice people to reveal personal information. Attackers attempt to deceive their targets with seemingly genuine e - mails from reputable organisations requesting them to update or verify personal information via e - mail or link click. The website linked in the e - mail often looks very similar to the company's actual website. After the victim clicks on the link, they are directed to a fake website that fraudulently solicits sensitive information such as passwords, credit card numbers, and bank PIN codes. These fake websites are only designed to steal victim information. It is essential to be cautious of suspicious e - mails and verify the sender's authenticity before taking any action.

4) Spatial data refers to information linked to a specific geographic location, also known as geospatial data or geographic information.

References

[1] M. Goodchild, R. Haining, and S. Wise, 'Integrating GIS and Spatial Data Analysis—Problems and Possibilities', *Int. J. Geogr. Inf. Sci.*, vol.6, pp.407–423, Sep.1992, doi: 10.1080/02693799208901923.

[2] A. Aziz, 'Network Intrusion Detection using Machine Learning - GISPP', *GISPP - Global InfoSec Pakistani Professionals*, Jan.25, 2021. https: //www.gispp. org/2021/01/25/network - intrusion - detection - techniques - using - machine - learning/ (accessed Mar.26, 2023).

[3] J. Stanik and M. K. Kiedrowicz, 'Risk in GIS systems', *eng*, vol.2, no.1, 2022, doi: 10.57599/gisoj.2022.2.1.39.

[4] 'Tips for improving performance of all - pipe models linked to a GIS - OpenFlows | Water Infrastructure Wiki - OpenFlows | Water Infrastructure - Bentley Communities', Oct.14, 2014. https: //communities. bentley. com/products/hydraulics___hydrology/w/hydraulics_and_hydrology__wiki/17388/tips - for - improving - performance - of - all - pipe - models - linked - to - a - gis (accessed Mar.26, 2023).

[5] D. Eastman, 'Application of Geospatial Data in Cyber Security'. Esri Australia National Security Sandbox, Feb.20, 2023. Accessed: Mar.25, 2023. [Online]. Available: https: //gis - and - cyber - security - esriaudefence. hub. arcgis. com/documents/esriaudefence:: application - of - geospatial - data - in - cyber - security/about

[6] 'The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations / An Esri® White Paper'. Esri, 2015. Accessed: Mar.25, 2023. [Online]. Available: https: //www.esri. com/content/dam/esrisites/sitecore - archive/Files/Pdfs/library/whitepapers/implementing - platform - secure - cyber - infrastructure - operations. pdf

[7] Z. Hu, C. W. Baynard, H. Hu, and M. Fazio, 'GIS mapping and spatial analysis of cybersecurity attacks on a Florida university', in *2015 23rd International Conference on Geoinformatics*, Jun.2015, pp.1–5. doi: 10.1109/GEOINFORMATICS.2015.7378714.

[8] A. Kayyali, 'GIS cybersecurity: The geospatial approach and its importance', *Inside Telecom*, Aug.25, 2021. https: //insidetelecom. com/gis - cybersecurity - the - geospatial - approach - and - its - importance/ (accessed Mar.25, 2023).

[9] N. Veerasamy, Y. Moolla, and Z. Dawood, 'Application of Geospatial Data in Cyber security', *Eur. Conf. Cyber Warf. Secur.*, vol.21, no.1, pp.305–313, Jun.2022, doi: 10.34190/eccws.21.1.447.

[10] P. Piletic, 'Applications of Geospatial Data in Cybersecurity', *Geospatial World*, Feb.23, 2023. https: //www.geospatialworld. net/prime/business - and - industry - trends/applications - geospatial - data - cybersecurity/ (accessed Mar.25, 2023).

[11] C. Hayslett and D. J. Muhammad, 'Today's Cyberthreat Landscape and the GIS', 2019.

[12] C. Gao, Q. Guo, D. Jiang, Z. Wang, C. Fang, and M. Hao, 'Theoretical basis and technical methods of cyberspace geography', *J. Geogr. Sci.*, vol.29, no.12, pp.1949–1964, Dec.2019, doi: 10.1007/s11442 - 019 - 1698 - 7.

[13] 'MAP | Kaspersky Cyberthreat real - time map'. https: //cybermap. kaspersky. com/ (accessed Mar.25, 2023).

[14] E. Guillén, J. Rodriguez Parra, and R. V. Páez, 'Improving Network Intrusion Detection with Extended KDD Features', in *Lecture Notes in Electrical Engineering*, 2014, pp.431–445. doi: 10.1007/978 - 94 - 007 - 6818 - 5 - 30.

[15] D. Freeman, 'GIS and Cybersecurity', *USC GIS Online*, Jun.21, 2021. https: //gis. usc. edu/blog/gis - and - cybersecurity/ (accessed Mar.25, 2023).

[16] A. Besiekierska and K. Czaplicki, 'CYBERSECURITY OF SPATIAL INFORMATION', *GIS Odyssey J.*, vol.2, no.2, Art. no.2, Dec.2022, doi: 10.57599/gisoj.2022.2.2.23.

[17] A. K. Jain and B. B. Gupta, 'Phishing Detection: Analysis of Visual Similarity Based Approaches', *Secur. Commun. Netw.*, vol.2017, p. e5421046, Jan.2017, doi: 10.1155/2017/5421046.

[18] M. Sanskar, S. Miss, Maske, and P. Chate, 'THE ADVANCE TECHNIQUES USED IN CYBER SECURITY FOR PHISHING DETECTION', vol.8, Jul.2021.

[19] C. Kime, 'IDS & IPS Remain Important Even as Other Tools Add IDPS Features', *eSecurityPlanet*, May 25, 2022. https: //www.esecurityplanet. com/trends/ids - ips - still - matter/ (accessed Mar.26, 2023).

[20] J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, and H. Jingjing, 'Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms', *Secur. Commun. Netw.*, vol.2019, p. e7130868, Jun.2019, doi: 10.1155/2019/7130868.

[21] 'Protect Your Organization with Managed IDS/IPS', Feb.10, 2017. https: //www.secureworks. com/blog/protect - your - organization - with - managed - ids - ips (accessed Mar.26, 2023).

[22] 'What is a DMZ in Networking and How does it work?', *Intellipaat Blog*, Jan.21, 2022. https: //intellipaat. com/blog/what - is - dmz - network/ (accessed Mar.26, 2023).

[23] J. M. Pittman, K. Hoffpauir, N. Markle, and C. Meadows, 'A Taxonomy for Dynamic Honeypot Measures of Effectiveness'.

[24] A. Колев, 'Определяне на вероятна зона на поражение при задействане на импровизирано взривно устройство в градски условия', *Информационен Бюлетин Година MMXVI Бр 2 „Противодействие На ИВУ"*, no.2, pp.59–70, 2015.

[25] 'Firewalls and ArcGIS Server—ArcGIS Server | Documentation for ArcGIS Enterprise'. https: //enterprise. arcgis. com/en/server/latest/administer/linux/firewalls - and - arcgis - server. htm (accessed Mar.26, 2023).

[26] 'What is ArcGIS Server?—ArcGIS Server | Documentation for ArcGIS Enterprise'. https: //enterprise. arcgis. com/en/server/latest/get - started/windows/what - is - arcgis - for - server - . htm (accessed Mar.26, 2023).

[27] H. Chen, J. - H. Cho, and S. Xu, ‘Quantifying the security effectiveness of firewalls and DMZs’, in *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security*, Raleigh North Carolina: ACM, Apr.2018, pp.1–11. doi: 10.1145/3190619.3190639.

[28] Islamic University in Madinah, Almadina Almonawara, KSA, B. Rababah, S. Zhou, and M. Bader, ‘Evaluation the Performance of DMZ’, *Int. J. Wirel. Microw. Technol.*, vol.8, no.1, pp.1–13, Jan.2018, doi: 10.5815/ijwmt.2018.01.01.

[29] ‘Network Data Quality and Digital Evolution in the Utility Industry’, *VertiGIS*. https: //www.vertigis. com/vertigis_blog/network - data - quality - in - the - utility - industry/ (accessed Mar.26, 2023).

[30] exprodat, ‘Measuring GIS Effectiveness’, *Exprodat*, Mar.04, 2013. https: //www.exprodat. com/blogs/measuring - gis - effectiveness - 4/ (accessed Mar.26, 2023).

[31] М. Ламбева and А. Колев, ‘Съвременни подходи за отдалечен достъп до информационни масиви’, presented at the MT&S Conference of the Defence Institute, pp.205–210.

[32] ‘OGC City Geography Markup Language (CityGML) Encoding Standard, https: //portal. opengeospatial. org/files/?artifact_id=47842’.

[33] [Pavlov. G., Kibersigurnost I geografski informacionni tehnologiiq prilojimi kum pandemiqta COVID - 19”, Modelirane, analiz I optimizirane na socialno - ikonomicheskite merki za namalqvane na negativnite posledici ot pandemiqta Covid - 19, Avangard Prima, 2023**]**