Alessandra Galassi

Cybersecurity risks of GIS technology for smart communities. A case study

Abstract: Digital Transformation (DT) is changing the city-citizen relationship, pushing to rethink urban development models to make them consistent with new socio-economic needs, particularly related to land livability and social inclusion. This article aims to provide an overview of digital security issues related to Geographical Information Systems (GIS) useful for rethinking cities in smart terms. In this specific case, a special Public Administration (PA) called the Special Office for the Reconstruction of the Municipalities of the Seismic Crater (USRC) adopts GIS as a tool to support its efforts in post-earthquake reconstruction by creating attractive smart communities. Briefly, the objective is to explore the cybersecurity aspects of GIS and how these should be considered as part of risk management, vulnerabilities of GIS related to information security, and suggest recommendations. The synergy of GIS with other technologies is also discussed, reflecting how technological innovation has pros and cons for an organization.

Keywords: GIS, Cybersecurity, Smart Communities, Information Security, Innovation Technology.

1. Introduction

Putting the welfare of citizens at the forefront by adopting a people-centered approach is a key objective for the European Union and has gained prominence on the social policy agenda over the past decade. It is necessary to rethink cities, including small towns, redesigning services and sub-services with a sustainable approach by combining competitiveness and conservation strategies. Cities-and likewise small towns-can become hubs of resources, investment, and innovation, and from their digitization can pass that of the whole of Italy, which to date does not have an adequate digital culture as mercilessly photographed by the European Commission's Digital Economy and Society Index (DESI)[1].

1 https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760147

Security is the basis for the decisions of any PA, big or small or special as in this case. And Information Security (InfoSec) becomes an essential aspect of any digital initiative. The application of Information and Communication Technologies (ICT) is not accidental but responds to a strategic design that starts from the specific needs of the context.

Here the focus is on the experience of the USRC mission structure of the Presidency of the Council of Ministers, created ad hoc by Law 134/2012[2], established to coordinate the process of reconstruction (of residential/non-residential buildings) and development of the 56 municipalities located in the so-called "seismic crater" hit by the April 6, 2009 earthquake that struck the Abruzzo Region (Italy), and in particular the city of L'Aquila and its province (see Figure 1) (Fico et al., 2017). The reconstruction is scheduled for completion in 2026. The seismic event had devastating consequences (more than 300 people killed), causing widespread damage to infrastructure, displacement of populations and disruption of essential services. Fifteen years later in the aftermath of this natural calamity, trying to look on the bright side, the area has proposed itself as an open space lab and scientific initiatives have blossomed such as INCIPICT project[3], which envisions the implementation of an experimental optical network to build a Metropolitan Area Network consisting in an Optical Ring to connect the main and the most important sites of L'Aquila city; "SICURA – House of Emerging Technologies"[4] as a technology transfer center to support businesses funded by Ministry of Enterprises and Made in Italy; VITALITY Foundation[5], an ecosystem of Innovation, Digitization and Sustainability for the diffuse economy of Central Italy involving universities, research institutions and private entities from Abruzzo, Marche and Umbria Regions.

2 Legge 7 agosto 2012, n. 134, *Conversione in legge, con modificazioni, del decreto legge 22 giugno 2012, n. 83, recante misure urgenti per la crescita del Paese.*

3 http://incipict.univaq.it/.

4 http://www.ctesicuralaquila.it.

5 https://fondazionevitality.it/.

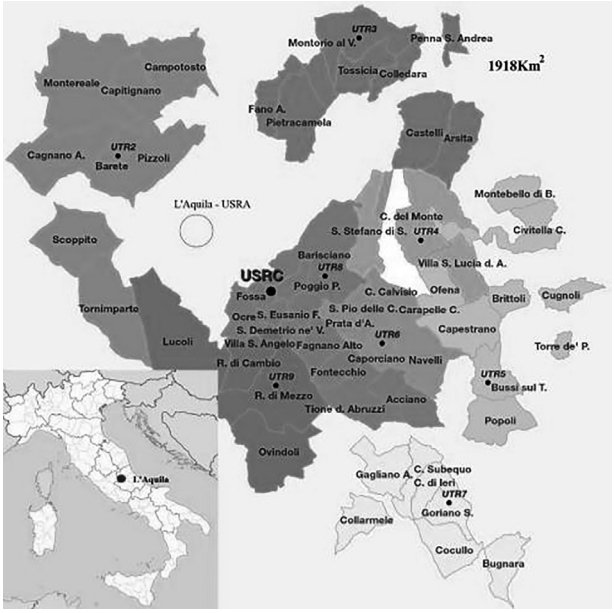

Figure 1: 56 municipalities making up the "seismic crater", divided into 8 homogeneous areas with 8 relevant reconstruction offices, UTRs, dependent on the USRC.

The USRC comprises multidisciplinary teams responsible for different aspects of physical and socioeconomic reconstruction, including engineering, urban planning and community involvement. To restore affected municipalities, the Office undertakes a range of activities, including GIS-based spatial analysis, stakeholder consultations, capacity-building and working groups, and infrastructure investments. The Office also collaborates with several academic institutions to leverage innovative best practices in reconstruction efforts. Hence the partnership with the Department of Telecommunications Engineering at the University of L'Aquila for land development and smart resource management, fostering the DT of these territories, that have characteristics in common, namely low population density, significant historical and environmental heritage. DT can make them attractive, avoid depopulation, promote local economy, counteracting isolation, in line with the National Recovery and Resilience Plan (NRRP)[6] too. From there, the need to develop an ICT platform (which is the core in a smart community) to support the USRC for information management (specifically geodata) useful to re-create more efficient communities.

Thus, GIS technology can play a role in supporting the USRC in both its activities and its DT journey. Whether it is infrastructure planning or resource alloca-

6 https://www.italiadomani.gov.it/content/sogei-ng/it/it/home.html.

tion, by leveraging geodata and analytical capabilities, GIS provides a framework for making informed data-driven decisions, gaining insights, providing innovative services to citizens, and optimizing operations (Fedra & Reitsma, 1990). Through a common platform for mapping and sharing geodata, GIS promotes collaboration and communication within the institution and among stakeholders (Franchi et al., 2024a).

Nevertheless, as institutions embrace DT to optimize operations and enhance services, they face growing cybersecurity risks. Indeed, this introduces potential vulnerabilities and increases the attack surface. Technology is vulnerable to many security issues, such as information theft, communication delays, data manipulation, jamming, remote exploitation, unauthorized access, human factor, etc. According to all 2024 reports released by ACN (National Agency for Cybersecurity)[7], DIS (Department of Information for the Security of the Italian Republic)[8], CLUSIT (Italian Association for Information Security)[9], in 2023 in Italy there was an increase in cyber-attacks against companies, organizations and people, with PA among the main targets of attackers. A successful cyber-attack against PA can lead to disruption of services, financial losses, exposure of private data, erosion of public trust in systems, and even physical damage.

Therefore, cybersecurity has never been more essential than it is now, as organizations have more valuable digital assets than ever before. The increasingly used hybrid cloud architecture and the pervasive use of mobile devices by employees means that enterprise IT must manage the security of many more devices and with a new approach.

2. Geographical Information Systems

Increasingly we hear about the "Science of Where" with geography as a relevant aspect of understanding our world (National Research Council, 2005). And the choice of GIS technology was not accidental but meets the needs of the context and the stakeholder. GIS is an evolving practice that enables organizations to get the most business value by helping multidisciplinary teams work together to make data-driven spending decisions (Chourabi et al., 2012; Franchi et al., 2024a). The literature review suggests that GIS can help understand where, why, and how things happen (Longley et al., 2005; Sui & Elwood, 2015).

Specifically, the USRC has equipped itself with a GIS over these years, but now, given the large volume of data and terminals-so we say big geodata-it needs to move from an on-premises and stand-alone solution to a cloud-edge one, increasing the level of risk of losing security of data. Data not only allow signification, knowledge, or understanding, but they also enable social action. In particular,

7 https://www.acn.gov.it/portale/documents/20119/446882/ACN_Relazione_2023.pdf.

8 https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true.

9 https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2024_web.pdf.

geodata (or geospatial data) are data relating to a location on Earth consisting in information about geographic locations stored in a format (e.g., geodatabase, shapefile, raster image, or even Microsoft Excel spreadsheet) that can be used with a GIS which combines location data (where things are) with descriptive data (how things are like in that location)-this ability distinguishes GIS from other information systems-helping users to discover relationships, enhance situational awareness and understand dynamics to model future scenarios (Worboys & Duckham, 2004).

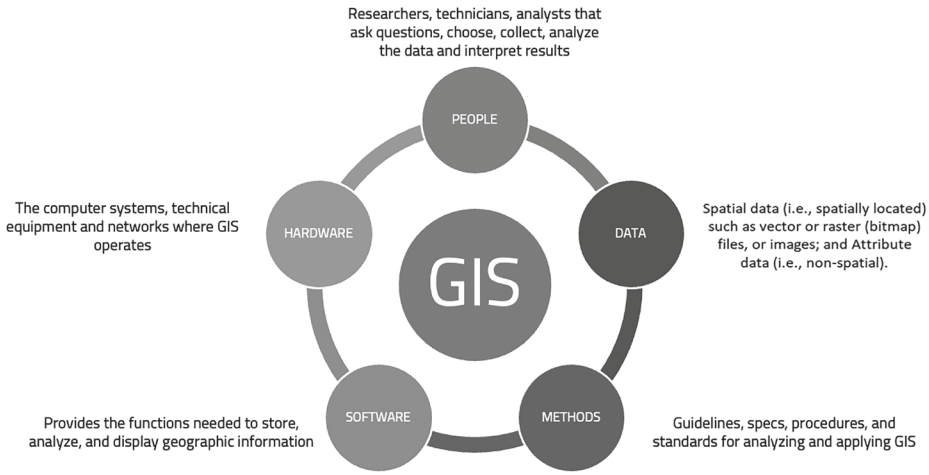

Figure 2: The key components of a GIS.

GIS is an automatic computer-based tool for collecting, analyzing, managing and interactive visualizing geodata, which enables (real-time) spatial analysis, planning strategies and resource management (Costantini et al., 2023). A working GIS integrates five key components: hardware, software, data, people, and methods as shown in Figure 2. Just as it was not exempt from the advent of the world wide web in the 1990s (Dragicevic, 2004), so today GIS establishes a synergy with other new technologies first with the Cloud Computing then with MEC (Multi-Access Edge Computing) and the next frontier is with AI (Artificial Intelligence) toward decentralized intelligence, seizing the opportunities that come with it but at the same time new potential challenges open up (see Figure 3 for the summary of technological evolution). The GIS-Cloud platform offers a dynamic, scalable and cost-effective solution that facilitates real-time data sharing and collaboration, enabling users to make timely decisions (Mell & Grance, 2011). With the GIS-MEC paradigm, cloud capabilities and the IT service environment are enabled at the edge of the network, closer to customers, reducing network congestion, latency, bandwidth requirements, and dependence on centralized IT resources to take advantage of the opportunities offered by next-generation connectivity (e.g., 5G) (ETSI, 2022). All of this is to promote social innovation with the goal of creating

positive societal impact (e.g., smart living and improved quality of life). Finally, Edge-AI enables local data processing on edge devices, reducing the need to transmit sensitive information to centralized servers for analysis, thus improving privacy and security (Wang et al., 2020). AI-powered GIS analysis enables automated data processing, pattern recognition, and predictive modeling of large volumes of geospatial data, enabling organizations to identify trends, detect anomalies, and derive useful information automatically, and users to focus on the most creative-strategic tasks (Ahmad, 2023).

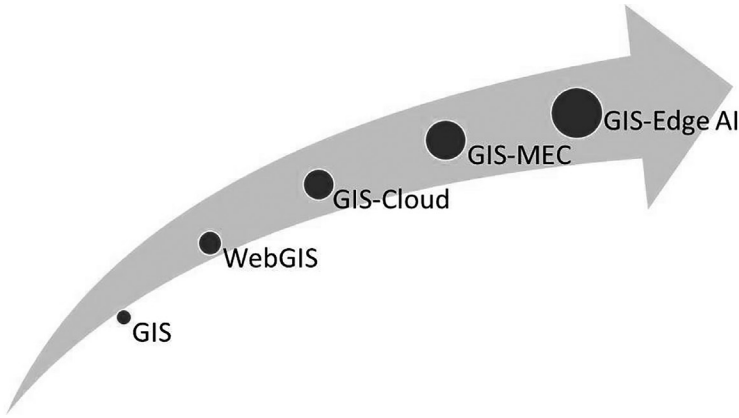

Figure 3: The GIS evolution.

Also, as institutions embrace the Internet of Things (IoT) and sensor technologies, GIS serves as an integration platform (Li et al., 2018).

We can consider GIS a driver of digital innovation, which facilitates spatial analysis, data visualization (including through integration with augmented reality and realistic 3D models), a tool that helps in problem solving (Goodchild & Janelle, 2010). As GIS continues to evolve, public/private organizations should harness the power of geodata and geospatial technologies, and leverage spatial insights to create a more sustainable, resilient and connected society.

2.1. The Role of GIS in Cybersecurity

The synergy of AI with GIS is a promising approach to proactive cybersecurity risk management. GIS can be used to map network infrastructure, visualize threat landscapes, and identify geographic patterns of cyber-attacks (Dash & Sharma, 2022). By integrating GIS with AI, institutions can leverage spatial data to train AI models, enhance predictive analytics, and improve decision making in cybersecurity operations (e.g., identify potential vulnerabilities, mitigate them, and prioritize response efforts) strengthening their posture (Bera et al., 2023; Rathee et al., 2023). Machine learning algorithms can analyze large datasets to identify patterns indicative of cyber threats or anomaly detection, while natural language processing can

analyze unstructured data to gather threat intelligence (Sharma & Dash, 2023; GISGeography, 2024).

Utilities use GIS-AI to analyze spatial data from smart meters and detect anomalies indicative of cyber intrusion or physical tampering; similarly, government agencies use this combination to monitor critical infrastructure, such as transportation and power grids, for cyber threats (Judijanto et al., 2023). These examples highlight the versatility and effectiveness of GIS-AI integration in addressing cybersecurity challenges in various sectors. Future research directions include developing standardized frameworks for GIS-AI integration, solving privacy issues, and exploring new applications of spatial analysis and AI techniques in cybersecurity. Collaboration between academia, industry, and government is essential to advance research in this emerging field and develop practical solutions.

However, challenges such as false positives and adaptability of cyber adversaries require continuous evolution of threat detection mechanisms.

3. An Overview of Cyber for GIS

As GISs continue to evolve, integrate with digital ecosystems, and play an increasingly integral role in the decision-making processes of various sectors (including government, defense, urban planning, environmental management, and others) (Franchi et al., 2024a), it becomes imperative to address the cybersecurity risks to which they are exposed so that data quality is not compromised (ESRI, 2020). By taking proactive measures and remaining vigilant against emerging threats, the USRC can safeguard its GIS infrastructure and preserve the CIA (confidentiality, integrity, availability) Triad for geodata from unauthorized access and exploitation. A balance between reactive and proactive measures should be found (Baskerville et al., 2014).

Among the cybersecurity risks facing GIS are:

1. *Data Breaches*: GIS databases contain a plethora of sensitive information, including geospatial data, demographic details, and infrastructure layouts. Unauthorized access to this data through breaches not only leads to violations of individual privacy, but also compromises national security. For example, exposure of critical infrastructure locations can help adversaries plan targeted attacks.
2. *Ransomware Attacks*: ransomware threats have intensified in recent years and, in a ransomware attack, attackers encrypt GIS data, making it inaccessible until a ransom is paid. These attacks not only disrupt operations, but also result in significant financial losses and erode stakeholder trust.
3. *Insider Threats*: insiders with authorized access to GIS systems, including employees and contractors, present significant risks that can compromise GIS security. Malicious insiders may abuse their access privileges to steal sensitive data, manipulate GIS information, disrupt services, implant malware, sabotage systems, or leak confidential information. In addition, inadvertent actions by well-intentioned insiders can inadvertently expose GIS

systems to vulnerabilities, highlighting the importance of robust access controls and employee training.

4. *Denial of Service (DoS) Attacks*: GIS servers are susceptible to these attacks, in which attackers overwhelm them with an excessive volume of traffic, making them inaccessible to legitimate users and disrupting services. The disruption caused by DoS attacks not only causes downtime and hinders access to critical geospatial information, but also compromises the functionality of GIS applications, potentially affecting emergency response operations and public safety.
5. *Eavesdropping Attacks*: a type of Man-in-the-Middle cyber-attack, which allows hackers to intercept, erase, or modify data transmitted between devices.
6. *Vulnerabilities in GIS Software*: like all software systems, GIS applications and platforms are prone to vulnerabilities that can be exploited by malicious actors both proprietary and open source. From SQL injection and buffer overflows to insecure authentication mechanisms, GIS software vulnerabilities can allow attackers to gain unauthorized access, execute arbitrary code, or compromise GIS data for malicious purposes.

Suggested strategies to mitigate these risks are the following:

1. *Implement Robust Access Controls*: use a defense-in-depth approach to restrict access to GIS systems by implementing access controls based on user roles and responsibilities, least privilege principles, and network segmentation. Use multi-factor authentication, encryption mechanisms, monitoring mechanisms to detect and prevent unauthorized activity, and strong encryption to safeguard data integrity and confidentiality.
2. *Regular Security Audits and Updates*: conduct periodic security audits and vulnerability assessments using scanning tools to identify and correct potential security weaknesses in GIS systems. Apply timely patches and software updates to reduce known security flaws and strengthen the resilience and defenses of the GIS infrastructure. Organizations should deploy intrusion detection systems and traffic filtering mechanisms.
3. *Zero-Trust Architecture (ZTA)*: the underlying concept is "never trust, always verify", meaning that users and devices should not be trusted by default, even if they are connected to an authorized network such as an enterprise LAN (local area network). It describes an approach to designing and deploying IT systems in an enterprise network composed of cloud services, connections to remote and mobile environments, and IoT devices.
4. *Employee Training and Awareness*: educate GIS users on the importance of adhering to cybersecurity best practices, including password hygiene, recognizing social engineering tactics or phishing attempts, and timely reporting of suspicious activity to effectively mitigate insider threats. Promote a cybersecurity culture to reduce insider threats among GIS users through comprehensive training programs and awareness campaigns.
5. *Backup and Disaster Recovery Plans*: implement backup and disaster recovery mechanisms to ensure resilience of the GIS system in the event of an attack such as ransomware or data breach. Maintain regularly updated

backups of GIS data, including off-site copies, and develop comprehensive disaster recovery plans to minimize downtime and facilitate timely restoration of geodata, ensuring business continuity.

6. *Collaborate with Cybersecurity Experts*: collaborate with cybersecurity professionals, practitioners and researchers, industry and government agencies to stay current on emerging threats and best practices in GIS security. Promote collaboration and information sharing initiatives to improve threat intelligence capabilities and strengthen GIS's overall cybersecurity posture. In general, see Information Sharing and Analysis Centers (ISACs), serving the government and national industry, are a resource that enables two-way information exchange between the public and private sectors on cyber causes, incidents and threats (in many cases to critical infrastructure), as well as the sharing of experience, knowledge and analysis.

The human factor seems to be the weakest link in cybersecurity, but organizational posture also matters. PA is trying to increase its cybersecurity by introducing formal policies and training employees, who consequently perceive cybersecurity as important, encouraging them to be aware about. As Alshaikha (2020) suggested, among the ways to improve cybersecurity culture could be the use of incentives, such as "employee of the month"-a reward would ignite a collective call to action, reminding employees that poor cybersecurity practices are not acceptable.

Challenges facing GIS include:

1. *Data Confidentiality*: one of the primary concerns in GIS security is ensuring the confidentiality of sensitive geospatial data. Unauthorized access to GIS databases can lead to data breaches, exposing proprietary information, classified maps, and personal identifiers.
2. *Data Integrity*: maintaining the integrity of GIS data is essential to ensure its accuracy, reliability, and trustworthiness. Malicious actors may attempt to manipulate GIS datasets, altering maps, spatial attributes, or geographic features to mislead decision-makers or disrupt operations.
3. *Service Availability*: for instance, DoS attacks pose a significant threat to GIS service availability, disrupting access to geospatial information and critical applications. Attackers may target GIS servers with overwhelming traffic, rendering them inaccessible to legitimate users.
4. *Over trust in GIS system*: in a fundamental sense, all technology depends on trust, and users need to know how it works. So, it must be trusted without replacing human creativity. Rather, it assists humans as a decision support system to be timely, efficient and predictive.
5. *Ethical issues*: the use of data as a means to exert control over other entities, resulting in an illicit relationship between parent and subsidiary, as also pointed out by Lodi et al. (2014).
6. *Proactive Supply Chain Risk Management*: about the control of data by third parties (Spiekermann et al., 2015). This means that the USRC, like any other PA, must carefully review service contracts and establish clear secu-

rity requirements, including data security, with Managed Service Providers (MSP) and generally with all vendors that support the implementation and operation of smart community technology (e.g., cloud service providers).

The above is summarized schematically in Figure 4.

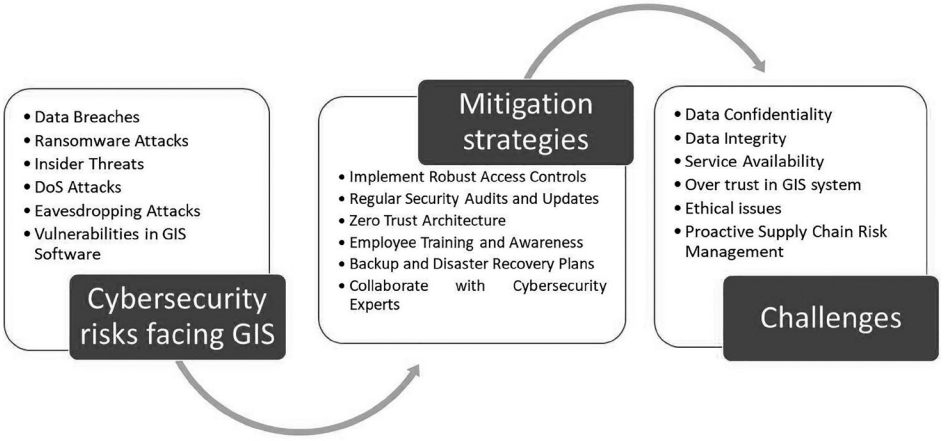

Figure 4: Sum up of Cyber and GIS.

4. The Case Study (hints)

A smart community ecosystem comprises three layers: the edge, which is the frontend (i.e., the devices, such as sensors or smartphones), the core (i.e., the platform, in this case GIS-based in a cloud-edge architecture, which processes the data and generates the business logic to make sense of the data flowing from the edge), and the communication channel (such as Wi-Fi, which establishes a constant two-way data exchange between the core and the edge to integrate the various components of the ecosystem) (Kousis & Tjortjis, 2021).

The development of the GIS platform to support USRC activities is still ongoing and will be completed soon with a kick-off event. The prototype has already been successfully tested (Franchi et al., 2024b). After that, it will be fully adopted by the PA in question. Figure 5 shows a preview of this.

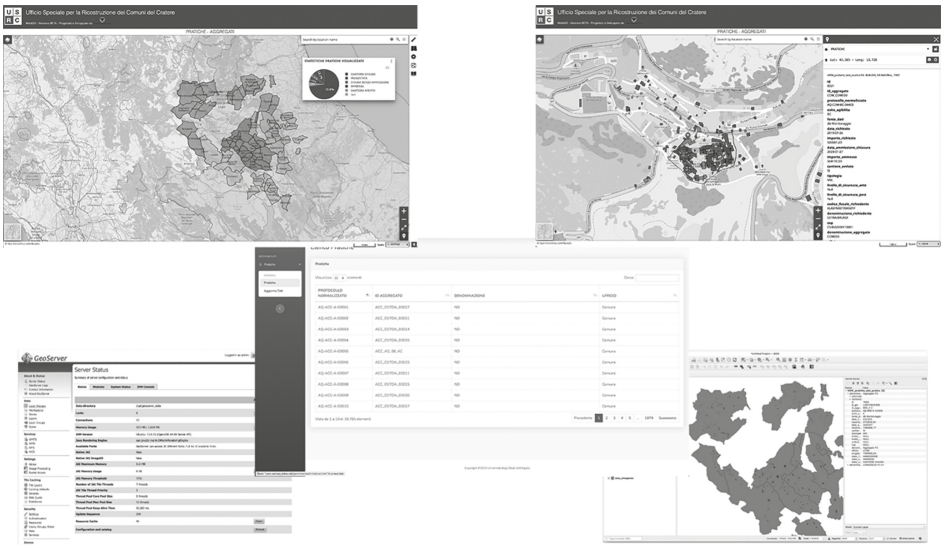

Figure 5: Sneak Peek of the GIS platform under development for the USRC

5. Conclusions

This paper examines cyber risks related to GIS technology supporting the development of smart communities. In the example used is a PA that wants to (re) create smart towns through technological innovation and data-driven decision making, and this introduces potential vulnerabilities and increases the attack surface. Economist J. Schumpeter defines innovation as "creative destruction", two words that seem antithetical but fit well to explain this context and in general that every innovation has costs and benefits, one must be adept at capturing the latter and curbing the former. Thus, the need to address security in data exchange (both processing and storage and transit) perhaps by defining a framework and to take proactive/reactive measures. The pros of this digital strategy, however, include DT and modernization of PA; (re)design of public intervention; efficiency of asset management and infrastructure planning; cost-effectiveness of (public) action; improved quality of city government; and new services provided to the population increase territorial capital. Recommended an interdisciplinary and multistakeholder approach with an ongoing university-institution-industry dialogue to develop solutions and ensure that although innovation runs fast, law is an ally. While the application of increasingly high-performance technologies can certainly improve people's living conditions, it can also, and just as strongly, result in a restriction of their freedom. Hence the decision to identify which public values should be taken

away from the private profit of giant platforms. So much so as stated by the Privacy Guarantor (Jan. 30, 2020), this alliance between technology and law "can be the lintel of a democratic and forward-looking response to the new threats of the digital, inevitably connected to the opposite, extraordinary benefits".

Moreover, the World Economic Forum 2023 reveals a global shortage of cybersecurity talent that needs to be addressed quickly[10]. But as Natasa Perucica says, it is important to remember that "cybersecurity is also the responsibility of all the other employees working for the organization in question. Through their responsible behavior and responsible use of digital technologies, like their devices, they contribute to the security of the overall organization".

Since attacks can have consequences that affect lives, it is imperative that all policymakers prioritize cybersecurity as a strategic necessity when undertaking online and digital initiatives.

In addition, investments by PA are needed to heal the country's structural backwardness, also involving inland and marginal areas. Otherwise, a fragmented system can produce gridlock rather than innovation, leading to what Garret Hardin called the "lifeboat ethic".

It is therefore necessary to be competent digital citizens to consciously navigate our society in the Information Age.

References

Ahmad M. 2023, "AI-Enabled Spatial Intelligence: Revolutionizing Data Management and Decision Making in Geographic Information Systems", in *AI and Its Convergence With Communication Technologies* (pp. 137-166). IGI Global.

Alshaikha M. 2020, "Developing cybersecurity culture to influence employee behaviour: A practice perspective", in *Computers & Security*, 98.

Baskerville R., Spagnoletti p. & Kim J. 2014, "Incident-centered information security: Managing a strategic balance between prevention and response", in *Information & management*, 51(1): 138-151.

Bera S., Glenn L., Raghavan A., Meno E., Cody T. & Beling p. A. 2023, "Deterring Adversarial Learning in Penetration Testing by Exploiting Domain Adaptation Theory", in *2023 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 314-318). IEEE.

Chourabi H., Nam T., Walker S., Gil-Garcia J. R., Mellouli S., Nahon K.,… & Scholl H. J. 2012, "Understanding smart cities: An integrative framework", in *2012 45th Hawaii international conference on system sciences* (pp. 2289-2297). IEEE.

Costantini R. A., Thompson C. M. & Delacour H. 2023, "Leveraging geographic information in organization studies: Beginning the conversation", in *M@n@gement,* (1): 35-51.

Dash B. & Sharma p. 2022, "Role of artificial intelligence in smart cities for information gathering and dissemination (a review)", in *Academic Journal of Research and Scientific Publishing,* 4(39).

Dragicevic S. 2004, "The potential of Web-based GIS", in *J. Geograph. Syst.,* 6(2): 79-81.

10 https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

ESRI 2020, "Designing an Enterprise GIS Security Strategy", Available at https://downloads.esri.com/resources/enterprisegis/UC_Web_GIS_Security_Strategy.pdf

ETSI2022, "Multi-Access Edge Computing (MEC); Framework and Reference Architecture", Available at https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_mec003v030101p.pdf

Fedra K. & Reitsma R. F. 1990, "Decision support and geographical information systems", in *Geographical information systems for urban and regional planning* (pp. 177-188). Dordrecht: Springer Netherlands.

Fico R., Gualtieri R., Pecci D., Mannella A., Di Ludovico M., & Prota A. 2017, "Reconstruction model of residential buildings in the historical centers of the crater municipalities after L'Aquila 2009 earthquake", in *16th World Conference on Earthquake Engineering, 16th WCEE.*

Franchi F., Graziosi F., Di Fina E. & Galassi A. 2024a, "A Survey of Cloud-Enabled GIS Solutions Toward Edge Computing: Challenges and Perspectives", in *IEEE Open Journal of the Communications Society*, 5: 312-331.

Franchi F., Graziosi F., Di Fina E. & Galassi A. 2024b, "A Cloud-Edge Architecture to Support Post-Earthquake Reconstruction in Central Italy", in *IEEE Access*, vol. 12, pp. 91823-91831.

GISGeography 2024, "The Rise of Machine Learning and AI in GIS", available at https://gisgeography.com/deep-machine-learning-ml-artificial-intelligence-ai-gis/ (accessed: June 14, 2024).

Goodchild M. F. & Janelle D. G. (editors) 2010, *Spatially integrated social science*, Oxford: Oxford University Press.

Judijanto L., Rahardian R. L., Muthmainah H. N. & Erkamim M. 2023, "Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government Information Systems in Indonesia", in *West Science Information System and Technology*, 1(2): 90-98.

Kousis A. & Tjortjis C. 2021, "Data mining algorithms for smart cities: A bibliometric analysis", in *Algorithms*, 14(8): 242.

Li S., Da Xu L. & Zhao S. 2018, "5G Internet of Things: A survey", in *Journal of Industrial Information Integration,* 10: 1-9.

Lodi G., Aniello L., Di Luna G. A. & Baldoni, R. 2014, "An event-based platform for collaborative threats detection and monitoring", in *Information Systems*, 39: 175-195.

Longley p. A., Goodchild M. F., Maguire D. J. & Rhind, D. W. 2015, *Geographic Information Science & Systems*, John Wiley & Sons.

Mell p. M. & Grance T. 2011, "The NIST definition of cloud computing".

National Research Council – Division on Earth, Life Studies, Board on Earth Sciences, Geographical Sciences Committee, Committee on Support for Thinking Spatially & The Incorporation of Geographic Information Science Across the K-12 Curriculum 2005, *Learning to think spatially*, National Academies Press.

Rathee A., Malik p. & Parida M. K. 2023, "Network Intrusion Detection System using Deep Learning Techniques", in *2023 International Conference on Communication, Circuits, and Systems (IC3S)* (pp. 1-6). IEEE.

Sharma p. & Dash B. 2023, "Impact of big data analytics and ChatGPT on cybersecurity", in *2023 4th International Conference on Computing and Communication Systems (I3CS)* (pp. 1-6). IEEE.

Spiekermann S., Acquisti A., Böhme R. & Hui K. L. 2015, "The challenges of personal data markets and privacy". *Electronic markets*, 25: 161-167.

Sui D. & Elwood S. (ed.) 2015, *The SAGE Handbook of GIS and Society*, SAGE Publications.

Wang, X., Han, Y., Leung, V. C., Niyato, D., Yan, X., & Chen, X. 2020, *Edge AI: Convergence of edge computing and artificial intelligence* (pp. 3-149), Singapore: Springer.
Worboys M. F. & Duckham M. 2004, *GIS: a computing perspective,* CRC press.