Power Grid Vulnerability and Secure Infrastructure for Energy Transmission

Vivian Sultan
California State University
Los Angeles, CA USA
email: vsultan3@calstatela.edu

Philip Caban
California State University
Los Angeles, CA USA
email: pcaban@calstatela.edu

Samuel Wong
California State University
Los Angeles, CA USA
email: swong100@calstatela.edu

Aaditya Kandel
California State University
Los Angeles, CA USA
email: akandel@calstatela.edu

Juan Talome
California State University
Los Angeles, CA USA
email: jtalome@calstatela.edu

***Abstract*—This report explores the correlation between modern grid infrastructure and the prevalence of cyberattacks, focusing on California's efforts to modernize its electric grid. We aim to identify areas that have undergone significant technology upgrades, such as monitoring devices, metering, and electric-vehicle charging stations. Using data from the U.S. Department of Energy and the open-source ArcGIS Data Repository, we conducted a spatial analysis to understand how these modernizations correlate with reported cyberattacks. The findings revealed that while modernization is generally associated with improved resilience, the lack of comprehensive data on modern technologies and monitoring devices limited our ability to validate the correlation conclusively. Our study concludes that more granular and relevant data are essential for accurate analysis, and we recommend policies to enhance grid security, including increased investment in cybersecurity measures and comprehensive data collection.**

Keywords—Security; Electric Utilities; Cyberattacks.

I. Introduction and Problem Definition

California's proactive stance in modernizing its electric grid aims to improve efficiency, reduce outages, and integrate renewable-energy sources. The electrical grid is undergoing significant modernization efforts, particularly in California, which leads the nation in integrating such new technologies as smart meters, advanced monitoring devices, and electric-vehicle (EV) charging stations. While these advances promise improved efficiency, reliability, and sustainability, they also introduce new vulnerabilities that could be exploited for cyberattacks. This creates a critical need to understand the correlation between these modern grid components and their susceptibility to cyber threats, and to develop effective policies and strategies to enhance the grid's security and resilience. The study builds on theories of infrastructure resilience and cybersecurity and leverages fundamental approaches from geospatial analysis and cybersecurity risk assessment to explore how infrastructure changes influence attack patterns. This report evaluates the impact of modernization on cyberattack risks and provides recommendations to mitigate these risks.

In this report, Section 2 reviews the literature. Section 3 describes the data selection and acquisition. Section 4 details the system used for the analysis. Section 5 lays out the methods used. Section 6 discusses the results. Section 7 offers some recommendations based on the analysis. Section 8 concludes.

California is at the forefront of integrating new technologies, advanced monitoring devices, sophisticated metering systems, and enhanced EV charging stations. Despite these advancements, a notable lack remains in the area of comprehensive, up-to-date reviews exploring the correlation between these modernizations and vulnerability to cyberattacks. This literature review is essential to understanding and mitigating the risks associated with advanced technologies. Previous studies have analyzed the general impacts of modernization on grid resilience, but they have often lacked a focus on the specific correlation between modern grid infrastructure and cyberattacks.

II. Literature Review

Several studies have explored the relationship between grid modernization and cybersecurity. For instance, research has emphasized the critical role of smart grids in enabling two-way communication and real-time monitoring, which significantly enhances operational efficiency [1]. However, these advancements also make grids more susceptible to cyber threats, as highlighted by studies on the vulnerabilities of smart grid components like control centers and substations [2]. Additionally, the U.S. Department of Energy has underscored the importance of cybersecurity measures in protecting modernized grids, citing the increasing frequency and sophistication of cyberattacks [3].

A. Limitations of Existing Solutions

While these studies provide valuable insights, they often lack a comprehensive focus on the correlation between specific modernization efforts and cyberattack patterns. For example, most research has concentrated on general vulnerabilities without delving into how particular technologies, such as EV charging stations or advanced metering systems, contribute to these risks [4]. Furthermore, the absence of granular, high-quality data has been a recurring limitation, making it challenging to validate findings conclusively [5].

B. Future Research

To address these gaps, future studies should aim to

1. Collect and analyze more granular data on modern grid technologies and their vulnerabilities.
2. Develop robust cybersecurity frameworks tailored to the unique challenges posed by grid modernization.
3. Investigate the role of policy interventions in mitigating cyber risks.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

C. Purpose of This Study

Building on the existing body of work, this study aims to fill the identified gaps by conducting a spatial analysis of California's modernized grid infrastructure. By leveraging data from the U.S. Department of Energy and the ArcGIS Data Repository, the research seeks to establish a more nuanced understanding of the correlation between modernization efforts and cyberattacks. The goal is to inform policy recommendations that enhance grid security and resilience.

Here's a breakdown of the approach before going into specifics of data selection and acquisition.

1. Objective-Oriented Focus: The central goal was to examine the correlation between electric grid modernization and cyberattacks. This required obtaining datasets that offered both breadth (covering diverse modernization aspects) and depth (granular data for detailed analysis).
2. Practical Considerations: To optimize research within time and resource constraints, emphasis was placed on leveraging readily available and processed datasets. This approach aimed to reduce inefficiencies like excessive data cleaning and processing, which can consume substantial time without guaranteeing usable results.
3. Addressing Data Scarcity: Recognizing gaps in existing data—specifically on emerging technologies like EV charging stations and advanced monitoring devices—alternative strategies were explored. These included using proxy data, expert consultations, and aggregating insights from multiple sources. However, these strategies were limited by their inability to fully bridge the data gaps.
4. System Compatibility: The choice of tools and methodologies was influenced by the compatibility of available data with spatial-analysis and visualization software like ArcGIS and Excel. Computational limitations (e.g., lack of high-end hardware) also shaped the approach, leading to creative solutions like combining maps and tables for more comprehensive analysis.
5. Flexibility and Iteration: Acknowledging the dynamic nature of research, the methodology incorporated iterative steps for refining data acquisition and visualization. This iterative framework allowed the researchers to adapt to the challenges posed by incomplete data and computational constraints.

This high-level framework underscores the balanced approach to addressing the practical and analytical challenges, laying the groundwork for the specifics that follow in data selection and acquisition.

III. Data Selection and Acquisition

Our primary focus when selecting and acquiring datasets on cyberattacks and electric charging stations was ease of use. We prioritized readily available processed data to minimize wasted time. The biggest challenge was the limited availability of specific data on new technologies, monitoring devices, metering systems, and system vulnerabilities. This scarcity is likely due to underreporting or limited awareness.

Fortunately, we were able to leverage clean, processed, and open-source datasets from the official ArcGIS website. These datasets were readily available in ArcGIS Project format. Time constraints and the limited availability of relevant data hindered our ability to draw definitive conclusions about the impact of cyberattacks on charging stations. This, in turn, limited the analysis tools we could employ. Cleaning raw data is time consuming and may yield unusable results. To address these limitations, we considered such alternative approaches as supplementing with proxy data or seeking expert consultations. However, these methods would not fully resolve the data gaps.

One alternative data acquisition method involved importing a CSV file (worksheet) from the US Department of Energy into ArcGIS. This file contained the locations of alternative fuel stations in California, including EV stations (Figure 1). The cyberattack dataset, collected from the open-source ArcGIS hub, included historical cyberincident data along with longitude, latitude, region (Figure 2), city, time zone (Figure 3), and ISP information. This dataset proved to be the most impactful and valuable for our research purposes.

IV. System

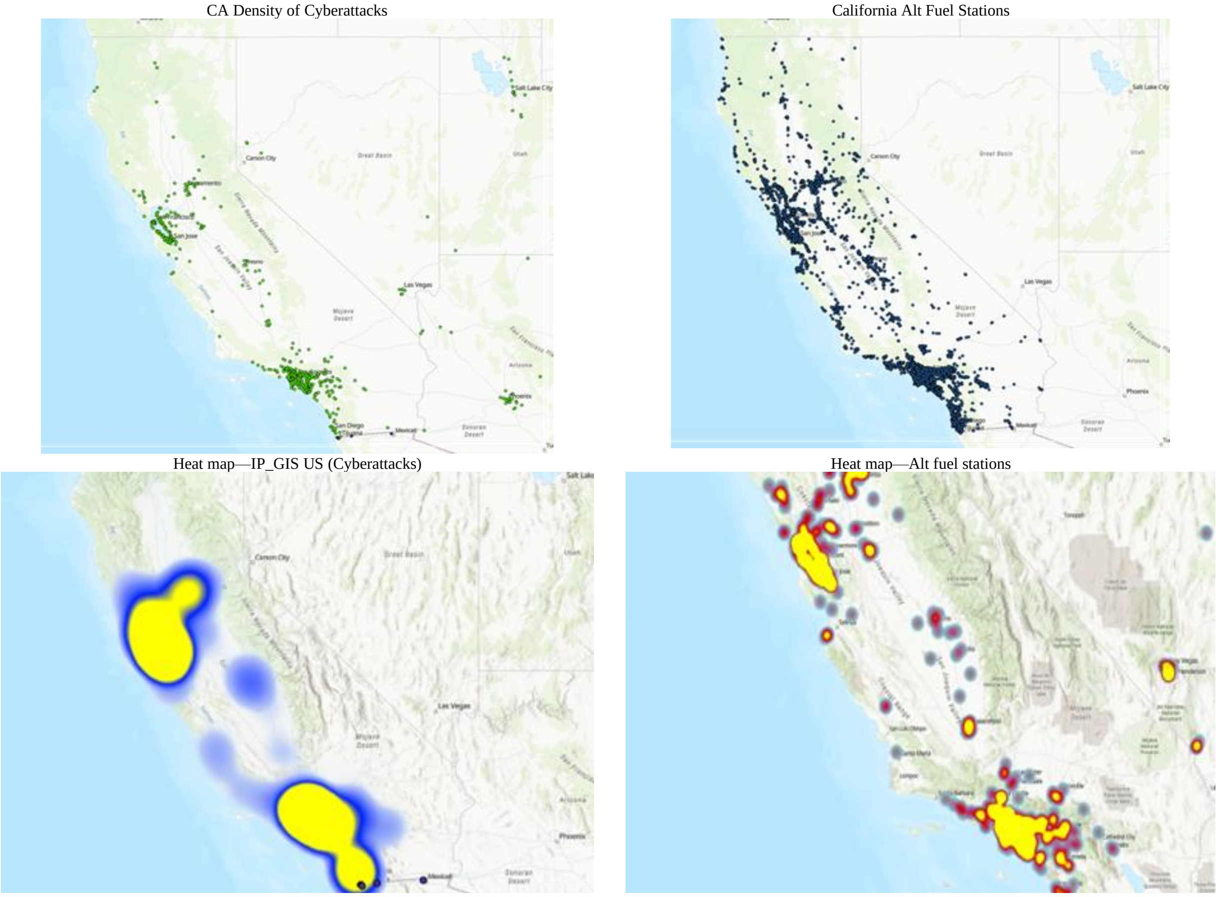
Conducting spatial analysis, mapping, and other forms of data visualization demands significant computing power and specialized software. Much of our analysis relied on mobile workstations or laptops equipped with ArcGIS and Excel. The absence of a dedicated graphics card and the inherent limitations of laptops limited our data analysis. Additionally, the data acquired was insufficient for further analysis.

The same data constraints impacted our software choices. ArcGIS proved inadequate for comprehensive spatial analysis, yielding inconclusive results. Consequently, we used Excel, importing attribute tables from ArcGIS into pivot tables. This approach of using both software products provided more insights than the original maps. Subsequent sections of this paper showcase charts and graphs generated from pivot-table analysis, revealing previously undetected patterns.

V. Methodology

We conducted spatial analysis to identify patterns and relationships between modernization features and attack frequencies; the data for this analysis was provided by Arc GIS.com and the U.S. Department of Energy. The analysis shows a correlation between the modernization of the electrical grid and cyberattack incidents and hotspots with higher levels of cyberattacks. The Data Overlay tool was used to visualize the overlap between grid modernization efforts and cyberattack incidents, and statistical methods were used to identify patterns and relationships between modernization features and attack frequencies. We employed such geographic information system (GIS) functions and operations as the *create new map layer* feature, which helped by combining cyberattack events and EV charging station locations to create a new map layer named MODERN POWER GRID/CYBERATTACK LOCATION. Another ArcGIS Pro tool used was the Merge tool to combine two or more features on the same layer into a new feature. Bar charts

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org



CA Density of Cyberattacks

California Alt Fuel Stations

Heat map—IP_GIS US (Cyberattacks)

Heat map—Alt fuel stations

Figure 1. Cyberattacks and Fuel Stations.

were also used to show types of EV ports at different charging stations and cyberattacks by city, revealing which cities have higher levels of cyberattacks (Figure 4).

VI. RESULTS/DISCUSSION

After performing our ArcGIS Pro analysis, we found specific hotspots where charging stations are more susceptible to being hacked, putting people's personal data in danger (Figure 5). The outcome of our initial analysis indicated a general pattern where modernized areas with advanced technologies exhibited varying degrees of cyberattack susceptibility. However, the results were inconclusive due to insufficient data on specific modernization aspects, such as monitoring devices and metering systems. These modernization aspects are important because their absence can expose sensitive such information as credit-card information or vehicle data, compromising people's privacy. The findings from this research project can raise awareness of this issue and prompt electrical companies with vulnerable locations in the EV charging infrastructure to enhance their equipment and protect against cyberattacks. The main problem we encountered was the lack of relevant data because little research and data is available on this topic. Time constraints were also a limitation because of the small timeframe given in class.

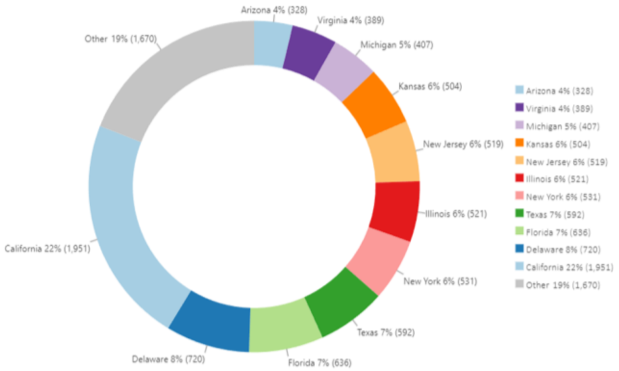


Figure 2. Percentage of Cyberattacks by Region.

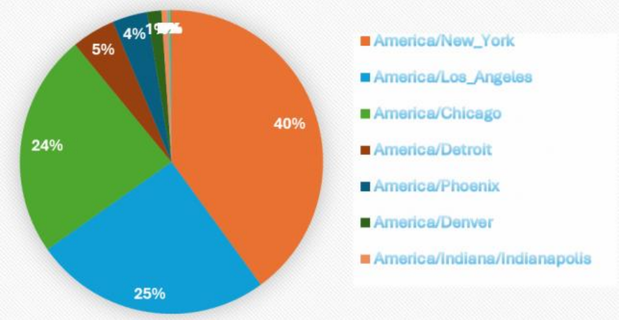


Figure 3. Cyberattacks by Time Zone.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

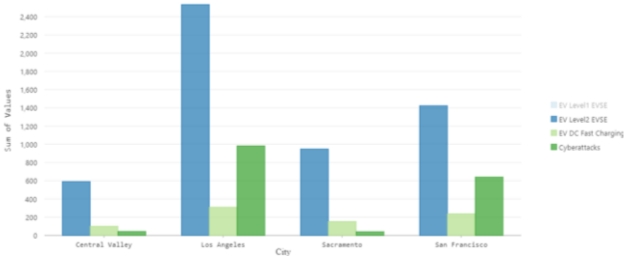


Figure 4. EV Charging and Cyberattacks by Region.

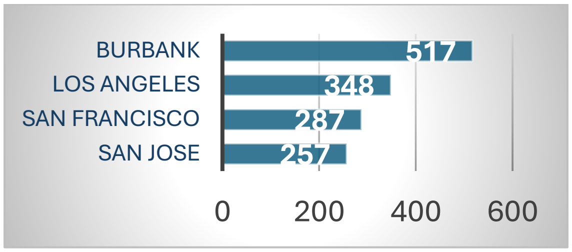


Figure 5. Most Attacked California Cities.

- **Outcomes:** The analysis indicated a general pattern where modernized areas with advanced technologies exhibited varying degrees of susceptibility to cyberattacks. However, the results were inconclusive due to insufficient data on specific modernization aspects, such as monitoring devices and metering systems.
- **Visual Output:** The report includes maps showing modernized grid areas and their correlation with cyberattack incidents, alongside graphs illustrating attack frequencies in relation to infrastructure changes.

VII. Recommendations

What can power grids and other similar infrastructure do to protect their systems and prepare for future cyberattacks? They can employ enhanced cyberattack standards, implement continuous monitoring and assessment, develop stakeholder collaboration, and invest in research.

Enhanced Cybersecurity Standards: Developing or adopting cybersecurity standards or practices tailor-made for the current and future grid technologies and infrastructure by regularly updating IT security policies based on the latest threat intelligence and technological advancements will improve IT security.

Continuous Monitoring and Assessment: How would a smart grid implement continuous monitoring of grid systems and regular assessment of modern technologies to identify vulnerabilities? Teams of network professionals can enforce updated practices through such monitoring systems as a real-time dashboard of smart-grid connected IoT devices. Such a dashboard could provide continuous information for data warehouses to be analyzed for cyberattacks trends and to test the effectiveness of modern security measures before exploits can harm the integrity of a grid's infrastructure.

Enhanced Data Collection: Collect and analyze more data on cyberattack trends and the effectiveness of modern security measures.

Stakeholder Collaboration: Foster collaboration between technology providers, grid operators, and cybersecurity experts to share threat intelligence and best practices.

Investment in Research: Support research and development into new technologies and their security implications to stay ahead of potential threats. Consider how future cybercriminals can gain unauthorized access. For example, outdated system software, insufficient cybersecurity measures, and lack of encryption is enough to risk any highly technical smart grid. Cybersecurity and cybercriminals are constantly changing and innovating, from malware as a service to simple social-engineering techniques. Therefore, continuous research and development, though costly, is necessary to protect the grid in the equally growing field of cybersecurity.

By addressing these recommendations, California can better safeguard its electric grid against evolving cyberthreats and continue leading the nation in modernizing its energy infrastructure.

VIII. Conclusion

California's efforts to modernize its electric grid with new technologies, monitoring devices, metering systems, and EV charging stations represent significant advancements in improving grid efficiency and sustainability. However, these advancements also introduce new cybersecurity challenges. By adopting robust cybersecurity frameworks, enhancing incident response, fostering collaboration, and addressing data gaps, California can reinforce the security and resilience of its electric grid against cyberattacks. Implementing these recommendations will be crucial to ensuring that the state's grid modernization efforts lead to a more reliable and secure energy infrastructure. The inconclusive results regarding the impact of modernization on cyberattack frequencies highlight the need for further research and data collection to validate the effectiveness of security measures and technologies.

References

[1] National Institute of Standards and Technology, "Cybersecurity for smart grid systems," 2023. [Online]. Available from: https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems. Accessed March 3, 2025

[2] U.S. Department of Energy, "Spotlight: Advancing cybersecurity to strengthen the modern grid," 2021. [Online]. Available from: https://www.energy.gov/sites/default/files/2021/01/f82/OTT-Spotlight-on-Cybersecurity-final-01-21.pdf. Accessed March 3, 2025

[3] Upstream, "Automotive & smart mobility global cybersecurity report," 2025. [Online]. Available from: https://upstream.auto/ty-upstreams-2025-global-automotive-cybersecurity-report. Accessed March 3, 2025

[4] Clarion Energy, "Data is the backbone of grid modernization," Renewable Energy World. 2024. [Online]. Available from: https://www.renewableenergyworld.com/power-grid/smart-grids/data-is-the-backbone-of-grid-modernization. Accessed March 3, 2025

[5] National Association of Regulatory Utility Commissioners, "Cybersecurity baselines for electric distribution systems and DER," 2022. [Online]. Available from: https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines. Accessed March 3, 2025

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org