JOURNAL OF CYBERSECURITY

*Journal of Cybersecurity*, 2025, tyae032
https://doi.org/10.1093/cybsec/tyae032

Research Paper

# Measuring the size and severity of the integrated cyber attack surface across US county governments

**Charles Harry**[1,‡], **Ido Sivan-Sevilla**[2,*,‡], **Mark McDermott**[3,‡]

[1]School of Public Policy, University of Maryland, College Park, MD 20740, United States
[2]College of Information, University of Maryland, College Park, MD 20740, United States
[3]Center for the Governance of Technology and Systems, University of Maryland, College Park, MD 20740, United States

*Corresponding author. College of Information, University of Maryland. College Park 20740, USA. E-mail: sevilla@umd.edu
‡The authors wish it to be known that, in their opinion, all authors should be regarded as joint first authors

Received 1 April 2024; revised 23 September 2024; accepted 5 December 2024

## Abstract

Limited methodologies to measure, enumerate, aggregate, and evaluate the cyber attack surface of US county governments prevent the full estimation of the importance of local government cybersecurity to national resilience. Our study aims to address this gap. We further develop existing OSINT-based methodologies to measure the attack surface and assess the size and vulnerability of publicly accessible county infrastructures. By collecting data on 42 735 Internet-facing devices across 3095 US county governments (98% of all counties), we show, for the first time, variations in size, diversity, and vulnerability of exposed county government attack surfaces. We develop and compare service- and Common Vulnerability Exposure (CVE)-based measures for attack surface diversity and severity, each showing different correlation trends with county population. We also highlight the lack of correlation between density of CVEs and likelihood of exploitation and develop measures to quantify the risk, revealing the impact of county government vulnerability on national cyber resilience. Previously studied as islands of insecurity, our novel empirical approach holistically estimates potential county vulnerability to common attack vectors upon service misconfiguration and aggregates CVEs, their severity, and probability of exploitation across county infrastructures, shedding light on the integrated and aggregated attack surface exposed across US county governments.

**Keywords:** Attack Surface; County Government Cybersecurity; Cyber Risk Quantification; OSINT Cyber Research

## Introduction

The current literature lacks a rigorous, data-driven, universal approach to assess the size and severity of the attack surfaces exposed by county government infrastructures. Despite a clear call and need for these assessments in US policy documents [1] (The 2020 Solarium Commission Report notes: "Critical infrastructure resilience requires the United States to be able to develop a comprehensive understanding of national risk and to translate that understanding into resources to manage or minimize that risk over time." [1]), policymakers and scholars have been struggling to comprehensively assess cyber risk across localized government services. Current methodologies to estimate the risk are limited, usually including surveys among county government employees. They do not reveal the actual attack surface or calculate its national impact. We aim to bridge this gap and further develop existing OSINT-based methodologies by collecting, analyzing, aggregating, and evaluating the cyber attack surface across all US county government systems that support service delivery and are exposed on the Internet. A usually under-funded cybersecurity sector, county governments are known to wrestle with attacks on a daily basis [2]. The size, scope, diversity, and severity of potential threats, however, are left unclear. IT departments at the county level manage their security independently, and there is no holistic view on the attack surface and potential exploitation across *all* county government networks (We do not include state-controlled IT networks

in our analysis as many of the government support services for citizens are delivered by independent county governments, operate in independent enclaves distinct from state networks, and are often not readily explored in the literature.).

We utilize NIST's definition of attack surface for an organization, but expand on the concept by stitching together thousands of individual county government organizations to build a single cohesive *integrated attack surface* across 3095 US county governments (out of 3143 US county governments overall, excluding US territories) (We could not find domains for 34 counties and could not retrieve IP addresses for additional 14 counties with domains. Our collected data covers 98% of all US county governments or county-equivalents according to the most recent US Census count.). Our integrated attack surface model encompasses over 42 735 internet facing devices, with over 51 487 open ports supporting 82 unique services across the 3095 county governments under study. The model was developed by combining a manually compiled list of 4948 web domains tied to specific county governments, a custom Python application developed by the authors, and access to third-party search engines—Shodan and Censys—which continuously and rapidly scan the entire IPv4 address space and ∼150 million in-use IPv6 addresses.

Utilizing this approach, we attempt to answer the following questions: (1) How many internet facing devices, ports, software services, and common exposures and vulnerabilities (CVEs) are exposed across the entirety of county government networks? (2) How does the integrated attack surface vary across geographies, population centers, and type of online services? (3) What is the relationship, if any, between potential vulnerability and county population? Vulnerability frequency and likelihood exploitation? Vulnerability risk and counties' geographies? And (4) what policymakers should do across counties to ensure national cyber resilience?

Our findings reveal how nuanced the regional attack surface of county government infrastructures is. We show that exposed county services follow a pareto (power law) distribution, and maintain a positive correlation between the amount of services exposed and county population, and a positive correlation between the number of IP addresses publicly accessible in a county and the number of open ports and services available for potential exploitation. We apply and compare service- and Common Vulnerability Exposure (CVE)-based measures for county government attack surfaces and visualize vulnerability based on both measures across counties. For service-based attack surfaces, our findings show significant correlation with population levels and demonstrate the diversity and quantity of services that local county managers need to protect. For CVE-based attack surfaces, our findings show the lack of correlation between density of CVEs and probability of exploitation as well as the lack of correlation between county population and CVE-based risk quantification.

Clearly, the data collected and synthesized raises some concerns surrounding the inappropriate use of the aggregated data presented in this paper. While the data utilized is available on the internet, the ability to group the data in a more contextually relevant manner requires us to be careful in how specific devices, services, or locations are discussed. Where possible, we attempt to obfuscate specific details of technology and precise vulnerability location, and instead focus on the strategic contours of the attack surface, informing questions relevant to the likelihood, frequency, or effect of cyber risks. Further, presentation of aggregated data in Tables is kept at the state or regional level with no identification of specific counties. Associated charts and maps are designed with a similar approach.

The paper proceeds in five sections. First, we discuss existing studies on local/county government cybersecurity in the USA and existing approaches for measuring attack surfaces with OSINT-based tools. The review highlights the discrepancy between the limited methodological approaches applied thus far to study county governments, and the urgent need to better assess, understand, and aggregate vulnerabilities in regional infrastructure supporting critical functions. Then, we introduce our methodology and detail our data collection steps that leverage the concept of "integrated attack surfaces" along with computational aggregation across the entirety of the USA and through the query of four OSINT-based sources. The third section presents our results on the size, diversity, and severity of county government attack surface, comparing service-based and CVE-based attack surface measurements. Fourth, we summarize and discuss our findings, detailing limitations, policy relevance, and future research avenues. We show that our approach both informs the broader debate on how observed technical realities shape state behavior as well as helps clarify how defensive investments can help reduce strategic cyber risks. We aim to inform policymakers and provide the means for closing local cybersecurity gaps in a near real-time cycle.

## From local and limited toward national and holistic understanding of county government attack surfaces

Despite the critical functions they fulfill, there is a paucity of empirical scholarship on county government cybersecurity. To better understand the security posture of county environments, we currently rely on various surveys, some with limited response rates [In their article, Caruson et al. (2012) discussed data from a survey that they conducted among 466 local government officials in the state of Florida, which produced a response rate of 24%. Norris et al. (2019) got a 11.9% response rate across a sample of 406 local governments. In a later survey, only 15 employees responded to a survey among top cybersecurity officials in US local governments. According to Norris and Mateczun (2022), CISOs and other cybersecurity officials feel that revealing anything about their cybersecurity could put the local government at risk.], that were conducted across local government employees. The surveys indicate that local governments in the USA have been practicing cybersecurity poorly, despite being under constant attack attempts [2]. Researchers found a lack of cybersecurity preparedness, awareness, training, and adequate funding [2–7], which makes local governments susceptible to criminals and state hackers, as demonstrated by some of the recent and troubling ransomware attacks on local government entities [8] (In 2019 alone, there were 162 reported ransomware attacks against state and local governments in the USA.).

Given their impact on society, documented gaps in county government cybersecurity are alarming. County governments collect and process sensitive information about US citizens, manage regional arrangements for emergency and police response, facilitate elections, supply water to citizens, operate local school districts, and are responsible for developing local economies. Even though those local sectors are not traditionally considered "critical infrastructures," the consequences of poor cybersecurity at the local level can be disastrous [9].

At scale, county cyber vulnerabilities can create serious national damage. Cyberattacks on urban infrastructures can bring local services to a complete halt for days or months, damaging quality of life [10]. A November 2020 ransomware attack on the Baltimore County school system, for instance, still prevents retired teachers from changing their medical insurance payments, even after those teachers change their policies. The district owes thousands of dollars to some retirees who are paying for benefits they no longer receive, while others are underpaying and will face high insurance bills soon

[11]. The spread of 'Internt of Things' (IoT) devices across county governments has further increased the potential attack surface, making local governments individually more vulnerable, while generating emergent consequences for the nation as a whole [12].

At the same time, it has been a challenge to assess the cyber vulnerability of regional critical functions. The interconnectedness of local infrastructures across agencies and levels of government makes it difficult to grasp the problem [9]. National-level decision makers face a gap between the level of sectors that compromises critical infrastructure and their authority to control those systems [13], leading to lack of visibility on the range of vulnerabilities found across independent local organizations. Networks that support localized emergency services, allow citizens to pay water bills, or to manage school districts, are controlled at the county level and are therefore difficult to assess holistically, since those systems run by multiple and independent organizations. Second, the lack of a scalable approach to measure aggregated cyber risk in these organizations across widely ranging geographies is missing, with DHS noting that "we lack integrated and scalable adoption and application of systemic risk assessment, resulting in ineffective and uncoordinated application of resources for cybersecurity" [14]. A recent FBI report on Internet crime showed how smaller counties and municipalities, with limited budgets and resources, are the primary victims of cyber attacks at the local level, stressing the need for a national-level approach to protect regional critical functions [15]. The 2023 White House National Cybersecurity Strategy has been calling for the development of large-scale, system-wide metrics for cybersecurity to better measure and assess the risk [16]. Still, county government operations, that can be categorized under one of the 16 critical sectors (Local Government can be classified under "Government Facilities," "Emergency Services," or "Water and Waste Water Systems" under PPD-21.) or as part of several sets of National Critical Functions (NCF) (Several local government operations are characterized under CISA's NCF framework include: " Operate Government," "Educate and Train," "Manage Wastewater," "Provide Public Safety," "Enforce Law," and "Conduct Elections".), cannot be easily assessed or prioritized for defense funding.

The high stakes of cyber insecurity at the county level along with the limited methodologies applied thus far to study this space, are especially surprising given existing knowledge on OSINT-based attack surface measurements. Scholars have been using OSINT-based tools, like Shodan, Censys, and others, to analyze publicly available IP addresses, services and vulnerabilities, measuring attack surfaces across European countries, hospitals in Germany, the telecom sector in Finland, and critical infrastructures in Turkey and Portugal [17–22]. Most studies highlight commonly used protocols and services across these sectors, flagging certain unsecure features in one [18] or more service configurations [17], across one or more critical sectors. A few studies also engage in CVE-based vulnerability identification and their associated Common Vulnerability Scoring System (CVSS) scores for severity, providing an additional dimension for capturing the security posture of organizations by linking collected data with NIST's vulnerability database [19–22]. Even though previous research found that combining multiple OSINT-based tools provides a more comprehensive view of the attack surface [23], a few studies only use a single OSINT resource for their attack surface measurement [17, 19].

Across these studies, various gaps in attack surface measurement still exist. There is no clear methodology for evaluating and quantifying cyber risk (per region/per sector) based on collected data. The demographic and geographical context of the vulnerability are also missing and there are no clear indicators for the severity and diversity of the risk. At the same time, existing work on attack surface measurement is a promising starting point for closing the gaps in attack surface enumeration and evaluation. We aim to automate the use of a combination of existing OSINT-based tools to group infrastructures per our unit of analysis—counties—and show vulnerability identification and assessment at the granular county-level across infrastructure sectors. We also aspire to produce a more nuanced measurement of the risk per county, appreciating the distinct value of service- and CVE-based measurements of the attack surface.

## Methodology: defining, enumerating, and aggregating county-level attack surfaces based on OSINT tools

The term "attack surface" was originally coined by Michael Howard in an MSDN magazine article (2003). It was then used by Howard, Pincus, and Wing (2005) as a metaphor for risk assessment in software, and appeared in a variety of contexts since [24] [Theisen et al. (2018) conducted a systematic literature review on "cyber attack surface" definitions, identifying 644 works from prior literature that use the term, including research papers, magazine articles, and technical reports [25].], relating to a range of attributes. For simplicity, we adopt the definition used in publications by the National Institute of Standards and Technology (NIST), which defines cyber attack surface as "the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from" [26]. Simply put, we relate to the term "attack surface" as the potential entry points to an organization.

To measure the attack surface exposed by county governments we chose to rely on passive reconnaissance. Active scanning of county infrastructures without explicit permission can be considered unethical and illegal. Therefore, we do not directly interact with county systems or perform active scans ourselves. We build on existing works that apply passive reconnaissance through OSINT-based tools and leverage the capabilities of specialized search engines—Shodan and Censys—that conduct and constantly update their comprehensive Internet scans, including scans of county government networks. To evaluate the collected data, we use two additional publicly available sources—NIST's National Vulnerability Database (NVD) to retrieve CVSS scores and First.org to retrieve EPSS scores for collected CVEs. We automate data collection via these public resources and create our framework to assess the size and exposed ports, services, common platform enumeration (CPE) values, the associated CVEs for the revealed CPEs, and the severity and probability of exploitation rates of collected CVEs across all US county governments.

We stitch together all publicly available county government infrastructures to comparatively analyze and aggregate the cyber attack surface across three locality scales—county, state, and Federal Emergency Management Agency (FEMA) regions. We aim to offer a holistic, integrated picture of the size, scope, scale, diversity, and severity of cybersecurity vulnerabilities that county governments create. Instead of considering county governments as islands for cyber-insecurity, we aggregate vulnerabilities in publicly accessible county government infrastructures to understand their potential national impact.

Our methodology measures a specific subset of the entire county government attack surface—the range of services on county government domains that are publicly available for potential exploitation. Our goal is to compile an "integrated cyber attack surface" across all US county governments and understand consequences at the national level. The validity of this approach was recently demonstrated when researchers from Censys found hundreds of publicly facing devices in more than 50 Federal Civilian Executive Branch organizations that

were exposed to exploitations across a variety of services [27]. We seek to apply a broader approach, across all regions of the USA.

Our data collection process started with compiling a list of all 3143 US county governments across 50 states + DC (not including US territories) from the most recent Census data on US county governments [28]. For each county we identified and collected the .gov, .org, .net, and .com county domains. This was done through association of the latest officially registered .gov addresses from the General Services Administration [29] and supplemented through open source research to manually add county domains we could systematically map across states for every county (For 32 counties we could not find any domains. Also, at this first data collection phase, we could not systematically map all county infrastructures. Essential services such as hospitals, treatment centers, fire departments, and wastewater infrastructures are likely left out in this first step. A few steps later, when we collect county IP addresses based on SSL/TLS certificates with the county domain name, we might pick up county services that go beyond our initial list of domains.).

1. General County Services [county-name.gov]: the domains associated with this category include the general county website, with options for residents to pay utility bills (e.g. water), look up voter registration information, as well as general county government operations.
2. County School Board [county-name-schools.org/.net/.com]: each county maintains control over its public schools. Counties typically have a unique domain for this part of county government.
3. Economic Development [county-name-economic-development.org/.com]: some counties maintain a separate organization to develop economic activity, and associate a separate domain for it.

To be consistent with our county-level data collection, we chose to exclude state-level domains that are not associated with specific county governments. For instance, the domain (in.gov) includes more than 900 IP addresses from the state of Indiana, but was not evaluated with our dataset because it represents state-level infrastructure that is likely supported by better funded and more consistent state-level efforts. Generally, county governments operate in conjunction with state entities, but independently. By capturing only county-level infrastructures our approach allows for a more standardized, balanced, precise, and focused scale of measurement of county-level vulnerability. Therefore, we included in our dataset only publicly accessible domains that can be associated with one unique combination of state name and county name (One outlier for that in the data is the domain wjccschools.org, which is associated with more than one county equivalent in Virginia—Williamsburg City and James City County.).

We assembled a list of 4948 US county government domains. The federated list was then categorized based on the associated county, state, and FEMA region of each domain. The categorization of county domains to FEMA regions was done for the purpose of being consistent with how US federal policymakers group together regions to assess national risk. The domain list was further expanded to a set of query terms including the www. prefix for domains (as some counties hosted only one of the pair "domain.gov" and "www.domain.gov''), and the IP addresses behind each domain, determined by DNS type A and type AAAA records. These IP addresses are the web server addresses tied to domains, which include information from content delivery networks used by government counties.

With our harvested domain sets and several IP addresses associated with web servers in county's content delivery networks, our team generated a procedure using Python code to query the assembled county domains through Censys—a platform that regularly scans Internet-facing infrastructure, associates it with domain names, and provides the consolidated data through an interactive API [30]. From the domain queried Censys data we collected the IP addresses, open ports, and services associated with county government domains.

Those Censys queries enabled a significant enrichment and expansion of our set of IP addresses per county infrastructures. First, based on past Censys queries and existing databases, the Censys service associated additional county subdomains to our initial query, beyond our assembled domains list. If a county used a subdomain utility.county.gov, Censys would associate our query term "county.gov" with that previously unidentified domain name "utility.county.gov." Second, Censys relies on its on-going collection of transport layer security (TLS)/secure sockets layer (SSL) certificates in past Internet scans from publicly facing devices that are associated with our domains of interest [In this context, the TLS and SSL certificates are security certificates that are used by county servers and include the county domain name under the "Subject Distinguished Name (DN)" rubric in the certificate, giving us a method to associate additional IP addresses/devices with each county. Those certificates are routinely collected by the Censys service, once observed as part of a TLS handshake during previous Censys scans of the public Internet.). This provides data on additional IP addresses that have no domain name and are not directly associated with the web servers registered with the Regional Internet Registries and the hosting of websites that are linked to the registered county domains. Those newly discovered IP addresses hold a county-related security certificate, and are therefore part of the county infrastructure and potential attack surface. This allowed us to increase the publicly identified infrastructure in counties by a factor of five, well beyond the ∼5000 IP addresses of the web servers across the three county government categories we started with. We were able to capture an array of publicly facing devices across all county government functions, even without domain names, that potentially include fire protection, parks and recreation services, wastewater infrastructures, housing services, emergency medical services, municipal courts, treatment centers, transportation services (including public transportation), and social services [31, 32].

Then, based on Censys' port scans on the various IPs that were found to be associated with the county, we were able to identify the ports and related services that are open for potential exploitation per county. Importantly, Censys has the ability to recognize exposed services such as Microsoft's Remote Desktop Protocol (RDP) or SQL Server based on the service banner, regardless of the port number they are listening on. We aggregated the results from the query set back to the original domains, combining the IP addresses returned from Censys and our DNS queries, with the ports and services that were found for each of those IP addresses.

The set of resulting IP addresses was then used as input to another commercial Internet scanner, Shodan, which regularly scans the Internet and provides CPE values for each IP, and the associated common exposures and vulnerabilities (CVEs) for those CPEs. It is important to note that we do not include in our data all provided CVEs for the CPEs found by Shodan. We only collect CVEs for CPEs that have specific associated version numbers for the software platform (for example, preserving "cpe:/a: jquery: jquery:2.2.0" but not "cpe:/a: jquery: jquery"). The strategy ensures less false positives, allowing to collect only "non-verified" CVE data that is associated with a specific version of the exposed county software platform ("Non-verified" CVEs is a terminology used by Shodan, indicating that the output provided relates to known CVEs associated with the CPE that was found. Those CVEs could be patched, but still appear as CVEs in

**Table 1.** Data points collected on each county domain.

| Domain X | Query terms for domain X | IPs for domain X query terms | Number of IPs | Ports for domain X query terms | Number of open ports | Services exposed for domain X | CPEv2.2 and CPE v2.3 | CVEs per CPE | CVSS and EPSS per CVE |
|---|---|---|---|---|---|---|---|---|---|

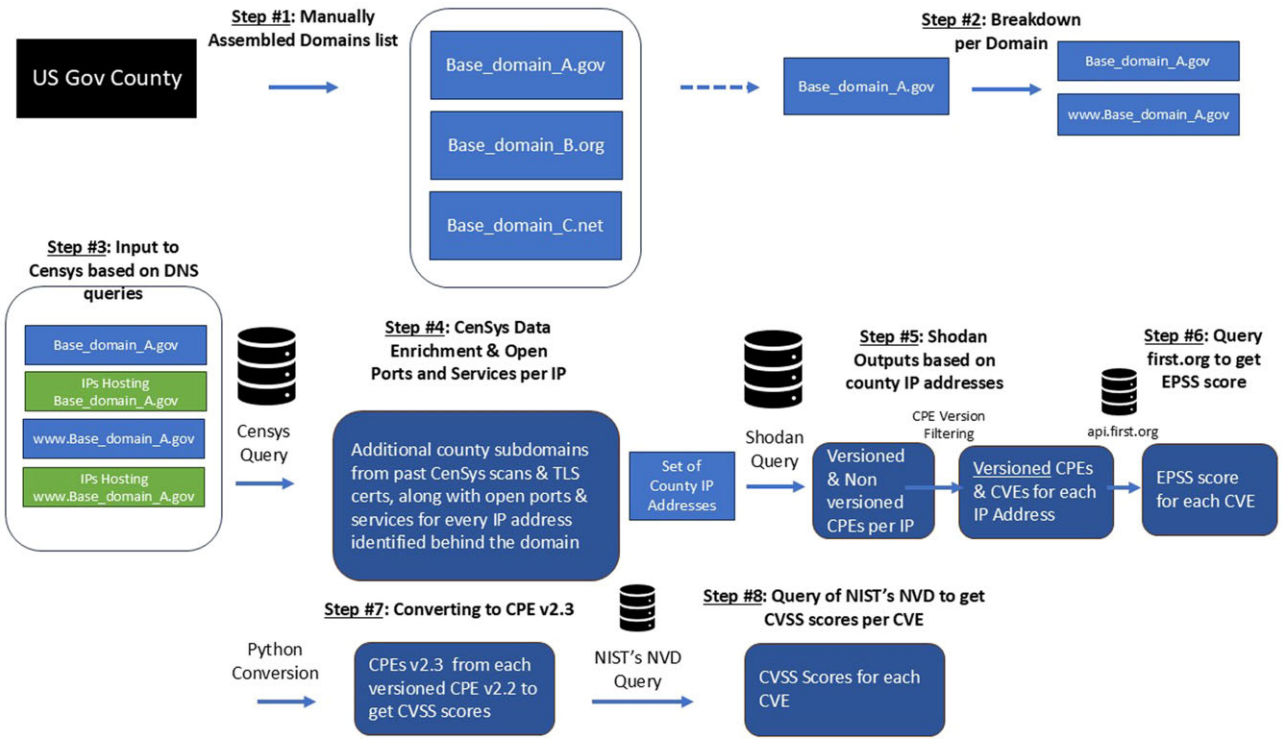


**Figure 1.** Data collection and aggregation steps per county.

our data. That is why we are referring to them as "potential CVEs". We only report on CVEs from versioned CPEs to be as specific as possible for each county.).

To obtain the higher confidence set of CVEs for the subset of versioned CPE 2.2, we used NIST's NVD "cpeMatch" value. However, because the NVD's cpeMatch only reports CPE v2.3, we were first required to convert our obtained CPE v2.2 to CPE v2.3 format, using Python3's cpe module. This NVD data was additionally used to map our versioned CPE v2.3 (through associated CVE) to CVSS metrics also present in our database. Finally, we used an Exploit Prediction Scoring System (EPSS) API from First.org to link the collected CVEs to their (current, at the time of the run) EPSS scores.

At the end of this process, each original county domain from our list had the (1) IP addresses associated with it from both Censys and DNS records; (2) count of those IP addresses; (3) open ports that were found to be associated with those IP addresses; (4) services that were tied to those ports; (5) CPEs v2.2 and v2.3 running on those IP address and their associated, nonverified, CVEs; (6) the associated CVSS scores for those CVEs; and (7) the EPSS score for each CVE that was found. See Table 1 for the data points collected on each county's domain in the list.

Appendices 1–4 include output examples from Censys, Shodan, and NIST. The examples show the type of data we put together for every county-related domain and IP address.

Figure 1 visualizes the steps in our data collection and aggregation efforts for mapping the attack surface per county. The starting input to our computational data collection appears in black. In light blue you can see results used for additional queries and in dark blue data outputs that we associate with each county government domain that is eventually included in its attack surface data. The server icons mark the points where we reached out to OSINT-based databases.

## Descriptive and comparative analysis of county-level size and severity of attack surfaces

To understand the amount and severity of attack surfaces exposed by publicly facing devices across county governments we enumerated 3095 out of 3143 (98.5%) US county government networks across 4905 individual web domains. 4905 domains remained from the 4948 after, 34 of the counties had no domains, and for 15 counties with only one domain, no IP address was found. The scan of county domains took place on February of 2024.

Out of the 49 missing counties, 18 are from the state of Oklahoma, where counties mostly use state-level infrastructures, 5 from Alaska, 5 from South Dakota, 4 from Montana, 4 from North Dakota, 3 from Indiana, 2 from Wisconsin, and the 8 other states have one county missing (We have domains for 3095 out of 3143 US counties. We could not find domains/IP addresses for the following 48 counties: MS, Issaquena; IN, Fayette; IN, Randolph; IN, White; NM, De Baca; OK, Cherokee; OK, Ellis; OK, Harmon; OK, Harper; OK, Haskell; OK, Jefferson; OK, Johnston; OK, Major; OK, Marshall; OK, McIntosh; OK, Murray; OK, Nowata; OK, Okfuskee; OK, Pushmataha; OK, Roger Mills; OK, Wagoner; OK, Washita; OK,

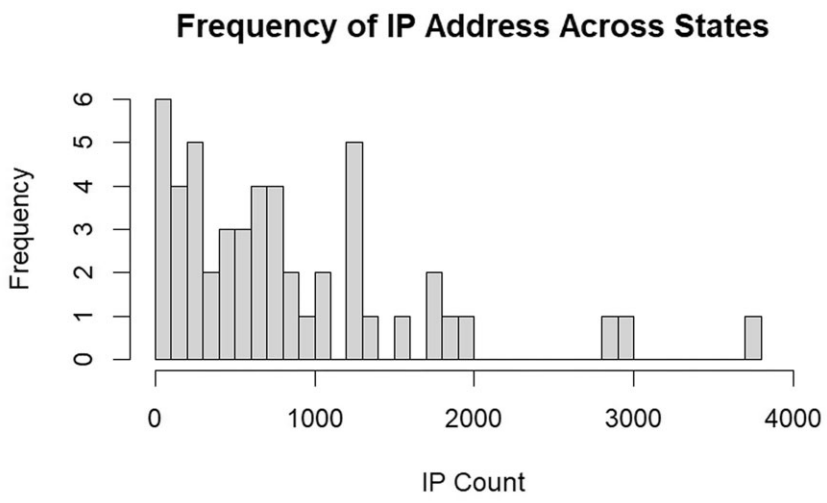


**Figure 2.** Overall number of IP addresses per state across all states.

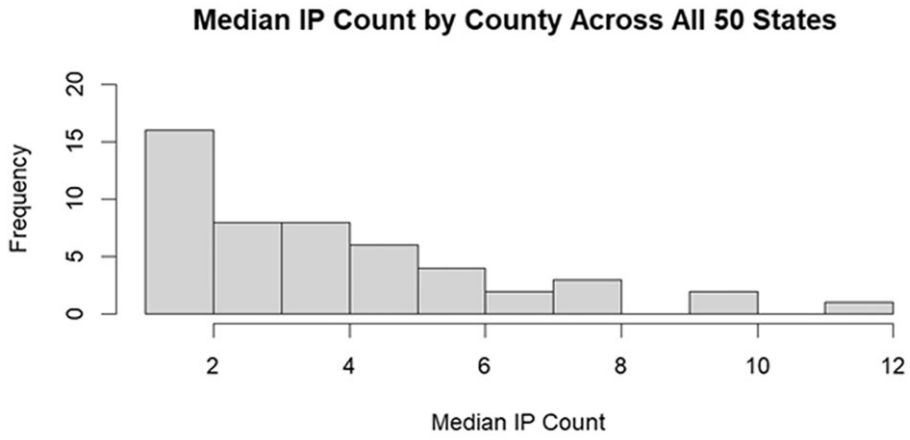


**Figure 3.** Median number of IP addresses per county across all states.

Woods; KS, Edwards; SD, Brule; SD, Grant; SD, Jackson; SD, Mellette; SD, Potter; HI, Kalawao; AK, Chugach; AK, Copper River; AK, Kusilvak; AK, Prince of Wales-Hyder; AK, Southeast Fairbanks; NE, Hitchcock; MT, Granite; MT, Meagher; MT, Roosevelt; MT, Sheridan; ND, Dunn; ND, Steele; ND, Sheridan; ND, Kidder; WI, Forest; WI, Iron; IL, Jefferson; and MO, Putnam.). Missing data on those counties do not introduce bias in the results since the states with missing counties are sporadically spread across the nation, and the missing counties are a small percentage of the total number of counties in that state (less than 10%). Two outliers are the states of Oklahoma for which 18 out of 77 counties (23%) are missing, and Alaska, for which 5 out of 30 counties are missing (16.67%). Still, the vast majority of counties across the nation (98.5%) and counties within a state (75%–100%) are covered in the data.

We found a total of 42 735 individual IP addresses, averaging 8.58 accessible IP addresses per county, with the median IPs per county being three addresses. The minimum number of IP addresses per county was 1 and the maximum per county was 677 (in Carbon, WY). We found a total number of 51 487 open ports, exposing 83 distinct services across county government networks. Each county has 10.34 open ports on average, with the median being five open ports per county. The minimum number of open ports per county was 1, and the maximum was 1262 open ports for one of the counties. The four subsections below present and analyze our findings. The next two subsections discuss the *size* of the revealed attack surface and the following two sections present and discuss attack surface diversity and severity.

## Attack surface size: amount and variation in exposed IP addresses

Figure 2 shows variations in the number of IP addresses across states. We can see the distribution of IP addresses follows a Pareto distribution with 15 states (30%) having over 1000 exposed addresses, but most states have 500 or less publicly available IP addresses.

Figure 3 shows the median count of IP addresses in counties per state. A few counties in our data have a wide array of exposed infrastructure and might skew the average. We decided to look at the median number of IP addresses per county instead, to get a better estimate of the attack surface size per state. The state of California, for instance, has 58 counties, each with its own set of IP infrastructure discovered through our methodology. Considering the IP addresses that belong to each county in California, the median number of county IP addresses for California is 12. Most states in Fig. 3 have a median number of IP addresses per county that ranges between 1

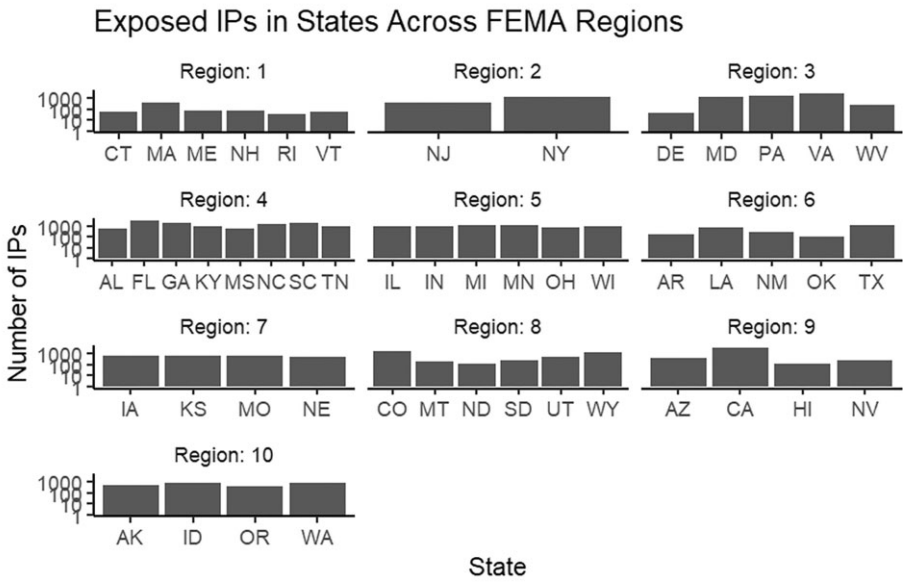


**Figure 4.** Sum of IP addresses per state across FEMA regions at a logarithmic scale.

and 6. Then we see states with a median count of IP addresses between 6 and 12.

When aggregating publicly available IP addresses to the FEMA region level (FEMA regions consist of 10 regions in the continental USA and territories, grouping neighboring states together. Those regions are traditionally used by US policymakers to assess risks across the country [33]. We do not account for infrastructure found in territories (e.g. Marshall Islands), which are often aggregated in FEMA regions. While this excludes infrastructure in some FEMA regions, the focus of our efforts remain within states. We make this decision given the complicated structure of territory governance, which would unnecessarily complicate the results of this analysis.), we see that the attack surface for certain regions is potentially larger than for others. We tested for correlation between state population and amount of IP addresses exposed per state and found a fairly strong positive relationship, with a correlation coefficient of 0.7303 that is statistically significant at the 99% confidence level ($P$-value = 1.744e-09). The need for county and local services grows as population expands, leading to more exposed IP addresses at the county level.

Figure 4 shows the amount of IP addresses in every state, per FEMA region, at a logarithmic scale. We can see how highly populated states like California or New York expose thousands of IP addresses, while areas that are less populated, such as Rhode Island or Delaware, expose much less IP addresses. FEMA Region #4, in the Southeast of the nation, exposes a lot of IP addresses, distributed almost evenly across all states in the region. FEMA Regions #5, #7, and #10 follow the same pattern, while in others, the amount of IP addresses per state varies more significantly.

## Attack surface size: amount and variation in exposed ports

A port is a process or application-specific software element serving as a communication start and/or endpoint for the Transport Layer IP protocols UDP and TCP [34]. Ports are software based and managed by a computer's operating system, with services (applications/programs) running behind them, essentially serving as the interface points between running programs on computers. Because they serve as an entry point for humans or other computers to give commands to a hosting computer or obtain information from the computer, open access to services comes with risks proportional to the access that the service provides.

When analyzing open and publicly available ports per county, and aggregating the data to the state FEMA region levels, we see that different regions are differently exposed. Figure 5 shows a histogram of the amount of unique open ports per state (in a unique set of IP and port). Twenty-seven states expose less than 1000 ports each, with Delaware and Rhode Island, on the lower-end, exposing less than 100 distinct open ports each. Twenty-three states expose more than 1000 ports, with Virginia exposing more than 4000 unique ports when assessing all of the IP infrastructure evaluated in its jurisdiction.

Figure 6 shows the median count of open ports in counties per state. For 32 states, the median number of open ports per county is more than five, with seven states having more than 10 open ports as the median number per county.

Aggregating the number of unique open ports per state to the FEMA region level (Fig. 7), we see a geographic distribution of ports per state and FEMA region. We used a logarithmic scale to show the different scales in the amount of open ports across states. FEMA regions #1, #2, and #10 have a couple thousands of open ports, with a variation between states. In region #1, for example, Rhode Island, Vermont, New Hampshire, and Maine are at scale of hundreds or below unique open ports. Massachusetts exposes around 374 unique open ports, and Connecticut only a couple of hundred. Highly populated areas—New York and California—drive their FEMA Regions #2 and #9 to hold the highest average of unique open ports per county and the highest standard deviation among the number of open ports per county, with California exposing over two thousand unique open ports. Regions #3, #4, and #5 expose more than 15 000 open ports, with every state but Delware contributing a significant amount, especially Florida and Virginia with around 1500 and 2800 open ports each, respectively. FEMA Region #4 is the most concerning region for unique open ports, with more than 13 000 open ports that are broadly distributed across all eight states. Mississippi has the fewest with under 1000. Alabama, Kentucky, Florida, North, and South Carolina all have under 2000 unique open ports, while Tennessee and Georgia both have over 2300 unique open ports. We

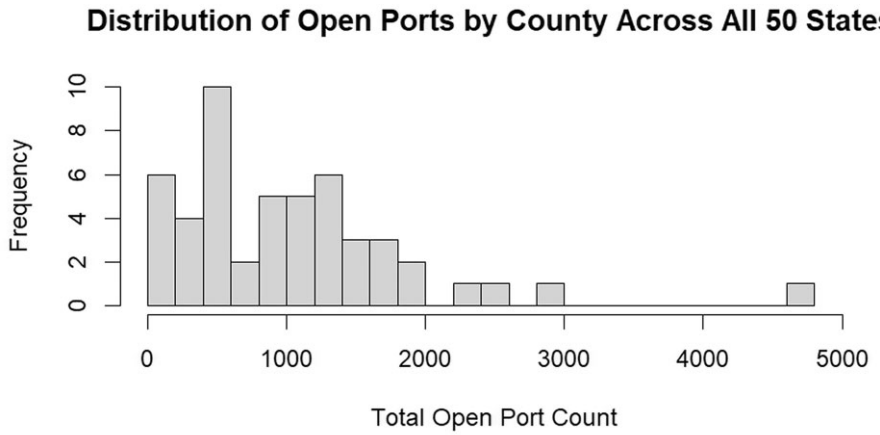


**Figure 5.** Overall number of open ports per state across all states.

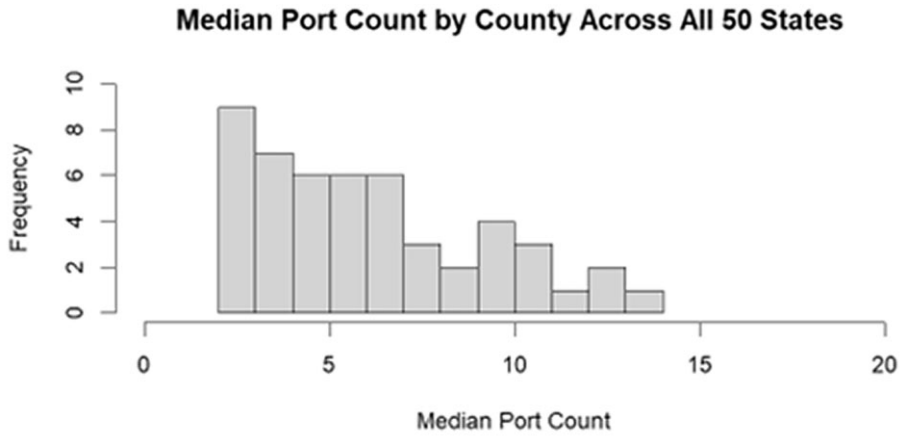


**Figure 6.** Median number of open ports per county across all states.

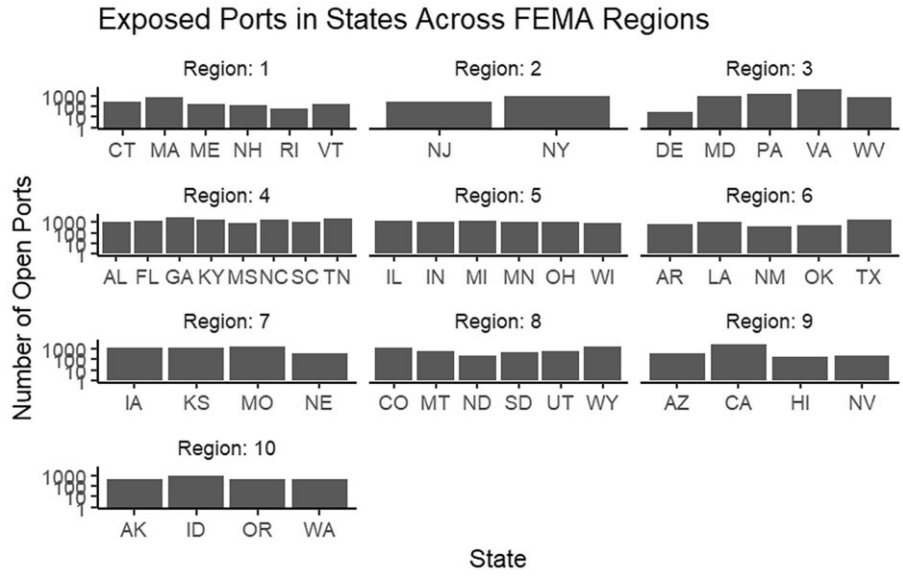


**Figure 7.** Sum of open ports per state across FEMA regions.

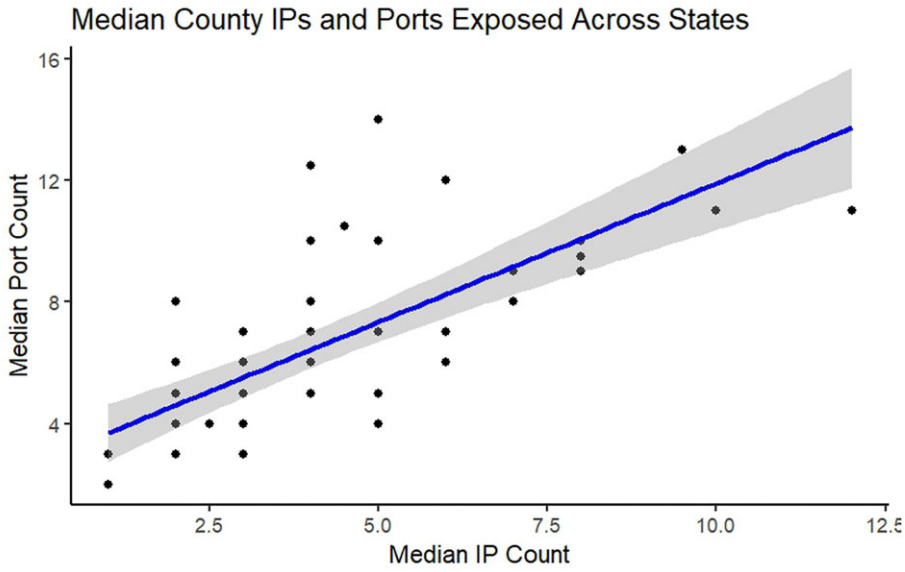


**Figure 8.** Median IP addresses count versus median open ports per county at the state level.

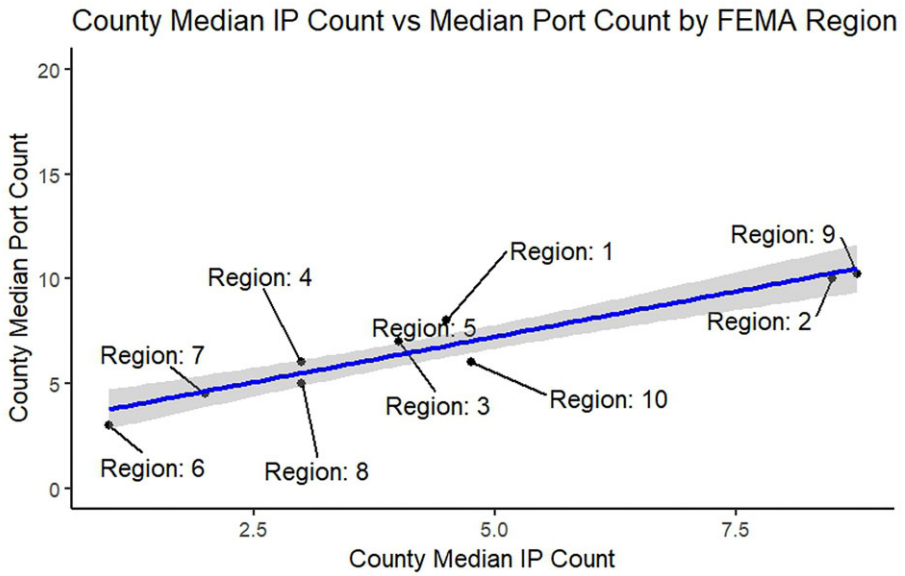


**Figure 9.** Median IP addresses count versus median open ports per county at FEMA region level.

tested for correlation between state population and open ports and found a moderate positive relationship with a correlation coefficient of 0.4978 that is statistically significant at the 99% confidence level (*P*-value = .0002345).

Figure 8 shows the crossing of the median IP addresses count with the median unique open port counts per county at the state level. We see an unsurprising trend line according to which the larger the number of accessible IP addresses in state counties is, the more unique open ports appear in those counties. This has been evident across highly populated areas like California or New York. With more county government infrastructure comes a greater number of access vectors potentially used by threat actors.

In Fig. 9, we see the same crossing but grouped at the FEMA region level. FEMA region #9, which includes California, is likely to be the most highly exposed FEMA region, followed by Region #2, which includes New York. Regions #6 and #7, which are less populated, are potentially the least exposed regions with small median numbers for IP addresses and open ports per county. Just like at the state level in Fig. 8, this figure shows that the positive slope created by contrasting the number of IP addresses with the number of open ports is maintained at the county level.

## Attack surface diversity: amount and variation in exposed services

Next, we investigated the type of services that could be exploited to develop a service-based measurement of attack surface diversity. Thus far, we showed aggregated data on the size of the attack surface, detailing publicly accessible IP addresses and open ports in each county, aggregated at the state and FEMA region levels. We

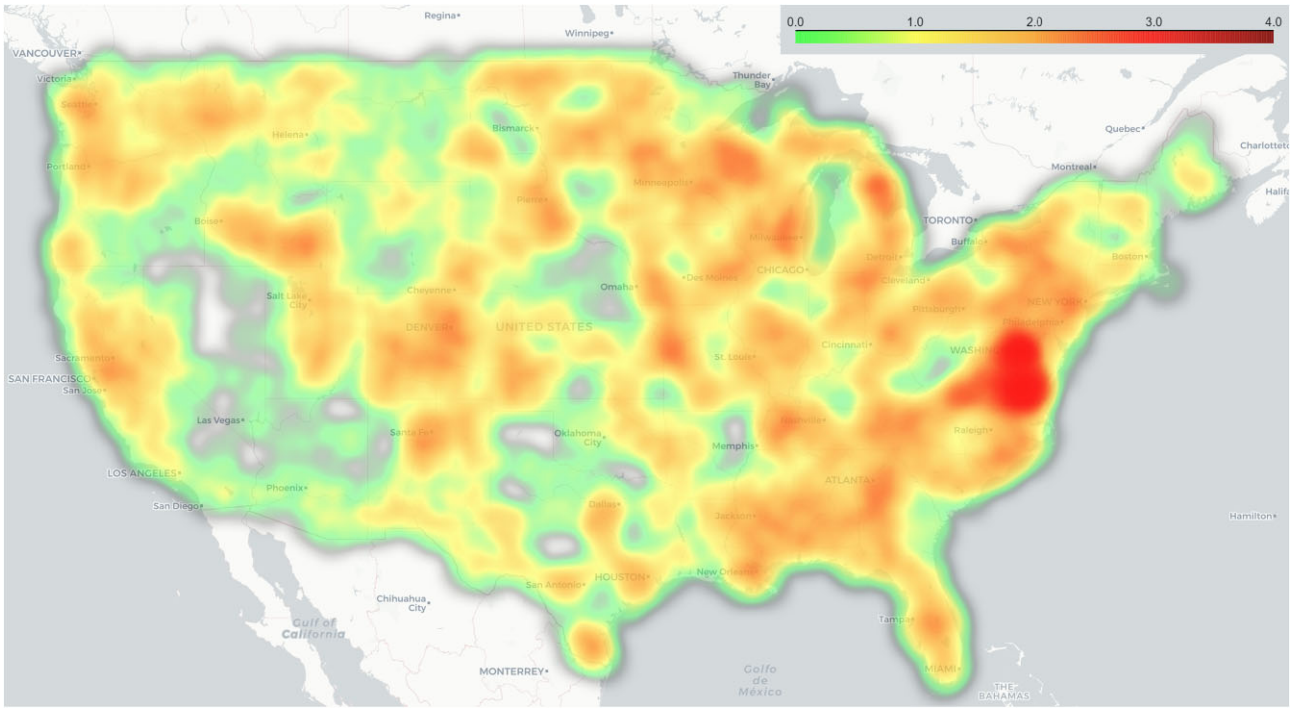


**Figure 10.** Heatmap of county government vulnerability based on exposure to one or more of four service-based attack scenarios.

demonstrated a variation in the sizes of attack surfaces, as well as a linear relationship between deployed county infrastructure (number of IP addresses) and exposed ports, and between IPs, ports, and state population. What is still missing is a measurement of the *quality* of the exposed attack surfaces, that would allow us to understand how many different types of attack an organization might be subjected to. It is important to note that exposure of a service in and of itself does not mean it can or will be attacked. Attacks often require a service to be misconfigured or compromised through exposed credentials. Despite this limitation, mapping exposed services in the attack surface does highlight potential vectors of attack across the entirety of the integrated attack surface.

The rationale for service-based attack surface measurement is detailed below. Open and available services for potential exploitation are an important attack surface component since exposure or misconfiguration of those services, which is not visible in the number of potential CVEs associated with that service, can lead to serious damage. Misconfiguration or use of credentials with exposed services (e.g. TELNET) are susceptible to infiltration by various threat actor groups (In some cases, unencrypted services such as FTP or TELNET can allow user passwords to be compromised through collection of unencrypted traffic in so called man-in-the-middle attacks.). Once exposed, services in combination with either a vulnerability or a set of valid credentials can facilitate illicit access into a victim's network. A recent CISA report found that the most common successful attack technique is hacking via "Valid Accounts," cracking password hashes was found to be successful in almost 90% of US Coast Guard risk and vulnerability assessments during 2023. Valid accounts can be accessed through default or stolen administrator accounts, or former employee accounts that have not been removed from the domain controller [35]. In one such case, threat actors leveraging the Trigona ransomware ecosystem, gained access to their victim's network through the use of compromised user credentials and an exposed RDP service on a publicly accessible device (The Trigona ransomware was leveraged in December 2022, with the technical details of the event documented on the DFIR technical blog [36].). Once a system is accessed, threat actors are able to engage in a variety of actions that lead to impacts on the confidentiality, integrity, or accessibility of data and systems.

To evaluate county vulnerabilities to specific open services our research looked at four specific classes of attack scenarios. Even though we found 82 unique services utilized across county government networks, we focus our analysis on services that enable four known types of attacks, which have been recently utilized by hackers. This enables us to demonstrate the applicability of our methodology for future policy efforts aimed at reducing cyber risk in the county government sector. Although we have the ability to point to very specific regions, counties, and systems susceptible to these specific attacks, we choose to aggregate results to the state level. These aggregations limit exposure of exactly which counties and which networks might be susceptible to which attacks. This is done in an attempt to not accidentally point state hackers or criminals toward specific vulnerable infrastructures.

While our approach to categorizing service vulnerabilities is tied to examples of specific services shown to be used in hacking episodes, it is possible to define additional categories that might result in differing measures of concern. For example, researchers interested in parsing vulnerabilities specific to virtual machine management (CISA identified CVE-2021-21985, a vulnerability to VMware vCenter Software as a frequently exploited vulnerability in 2021.), web-conference software [37], or even enterprise security products [38] might define diversity measures differently. While this is an interesting question and one bound to raise additional questions concerning optimal measures, it remains outside the bounds of this paper.

Our visualization in Fig. 10 aggregates the number of attack vectors that might be available in the scanned counties. Each county is scored between 0 and 4 according to the following method: when one of the four following attack scenarios was found to be available

in that county, the county gets an additional point. Counties that get the score of 4 are potentially vulnerable to all of the four following attack scenarios, highlighting a large diversity of potential attacks. Findings at the precise county level are masked through a heat-map type of visualization.

We first classify which government counties are potentially susceptible to DNS misconfiguration. For counties where the DNS service was publicly available for exploitation, the attacker can flood the county domain's DNS servers in an attempt to disrupt DNS resolution for that domain. Such flooding might compromise the ability of a county website/web application/online service to respond to legitimate traffic from residents [39]. In a recent example, healthcare websites in the USA were flooded by fake DNS requests in on-going attacks. The attack was deployed by botnets consisting of thousands of hacked devices, which sent requests to exposed DNS services in a manner that overwhelmed the processing ability of devices disturbing the functionality of healthcare websites across the county [40].

We are also interested in classifying government counties that may become targets for illicit access to government databases. Our data collection came across various open services tied to the use of databases (MSSQL, MYSQL, and POSTGRES) across US government counties, making a potentially critical government database server accessible from the Internet. Hackers might reveal an outdated SQL server or lack of password protection on a database server that could make the database vulnerable to unauthorized access. Exposure of database services on the organization's attack surface exposes the potential for threat actors to either take advantage of a known vulnerability in the underlying software or to craft requests that bypass authentication processes (An example of how SQL injection can be performed can be found here: https://owasp.org/www-community/attacks/SQL_Injection). In a recent example, a SQL injection vulnerability was exposed at the file transfer software MOVEit, allowing a malicious actor to take over clients' databases. The US Cybersecurity and Infrastructure Security Agency (CISA) issued an alert for MOVEit clients to patch their systems immediately [41], demonstrating the criticality of such vulnerability.

The third type of service-based attack we were interested to inspect enables insecure authorization to county government systems and devices. We classified government counties based on whether TELNET, FTP, RDP, or SSH services were found to be open for possible exploitation on their networks. A recent malware spotted by researchers in the wild was found to be using default TELNET credentials to exploit known flaws and perform remote code execution on target devices. Once a device was breached, it became part of a botnet army for a set of Denial of Service (DoS) attacks. The malicious activity took place between July 2022 and December 2022, demonstrating the risk in having insecure TELNET services open for exploitation [42]. In another example, insecure authorization through the RDP was named by the FBI as one of the top three infection vectors for ransomware incidents in 2022 [15]. CISA has recently published an advisory on the BianLian Ransomware Group, detailing how the group has been utilizing open RDP and FTP ports at their victims [43]. The FBI recommends those who use RDP to secure and closely monitor it, which raises concerns given the frequency and variety of counties in our data that expose such service to the public. Similar concerns were raised by the state of New Jersey on open RDP, TELNET, and SSH services among organizations, based on their threat intelligence data [44].

We were also inspecting the data to realize which counties expose services that allow insecure file sharing, such as NetBIOS and SMB. These services enable file sharing and printing in Microsoft Windows environments, but were found to be vulnerable and dangerous, causing the notorious WannaCry ransomware attack in 2017. The attack struck a number of important and high-profile systems, including the UK's National Health Service, and overall affected more than 300 000 computers across 150 countries, costing hundreds of millions of dollars to the victims [45, 46]. The attack was spread through flaws in the SMB protocol, and an unpatched version of the implementation of that protocol could enable the execution of arbitrary code by attacks, an exploit known as EternalBlue [47]. Microsoft specifically asked its customers to block access to the SMB service from the Internet and protect devices inside the organizational network, in contrast to what our data show for many US government counties [48].

Figure 10 presents a heatmap of US counties' potential vulnerability to those open services, colored on a scale from green to red based on the number of attack scenarios from the above that are potentially exposed in their infrastructures. Counties get the score of 4 and are colored dark red when all four types of attacks can potentially take place in their networks. Counties get the score of 0 and are colored light green when none of the attack scenarios above was found to be possible in their networks. We have 46 counties in our data without domains or IP addresses, and they are colored white/gray in the heatmap. We can see that highly populated regions are potentially more vulnerable to service-based attacks, with the states of California, Florida, and Virginia raising particular concerns. The Midwest and Northeast parts of the nation pose less of a concern for those types of attacks.

US states that are not visible in Fig. 10—Hawaii and Alaska—are showing some concern as well. Alaska (Fig. 11) has two boroughs (equivalent to counties) that were scored 3—susceptible to three types of attacks. Hawaii (Fig. 11) only has a single county with a severity score of 2, however that county is the location of the single largest population center and therefore produces a significant concern to the vast majority of residents in that state. County regions were reduced to dots in these maps.

We then wanted to understand whether there is a connection between the amount of infrastructure that county IT administrators need to manage, and exposure of those counties to one or more of the service misconfiguration attack vectors mapped in our data. Figure 12 shows that distribution at the state level. We see that when the IP count is below 1000, there is a linear positive slope between size of attack surface (number of IP addresses) and exposure to services of concern. Then, in states where 1000–2000 IP addresses are managed at the county level, we see a sharp decrease in slope, almost to an horizontal line. More county infrastructure does not make the state more exposed at this stage. At a certain size of attack surface, IT admins are somewhat successful in maintaining an equilibrium between size of IT to manage and exposure to attacks. But as complexity increases and the attack surface expands, there is almost an exponential slope. Two states get rapidly exposed to potentially serious attacks when the IP count crosses the 2000 mark, showing how a large digital footprint may lead to high complexity and difficulty navigating the potential risks.

We then broke down service exposure across these four services of concern to see which states are more/less susceptible to which types of attacks. For each service of concern, we calculated the percentage of counties that are potentially susceptible to exploitation through that service. Figure 13 shows potential vulnerability to DNS misconfiguration attacks. The states of California and Virginia were found to be at potentially high risk for this type of attack, with more than 75% of their counties exposing services that could be exploited for DNS misconfiguration.

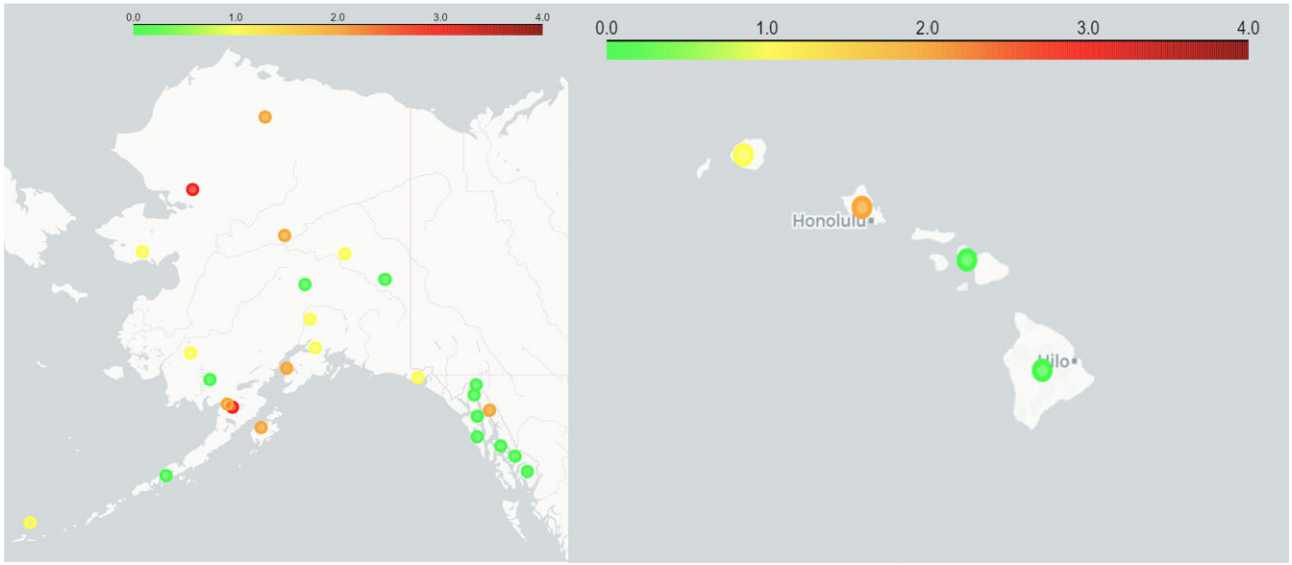


**Figure 11.** Alaska and Hawaii colored based on their exposure to 0–4 types of attacks.

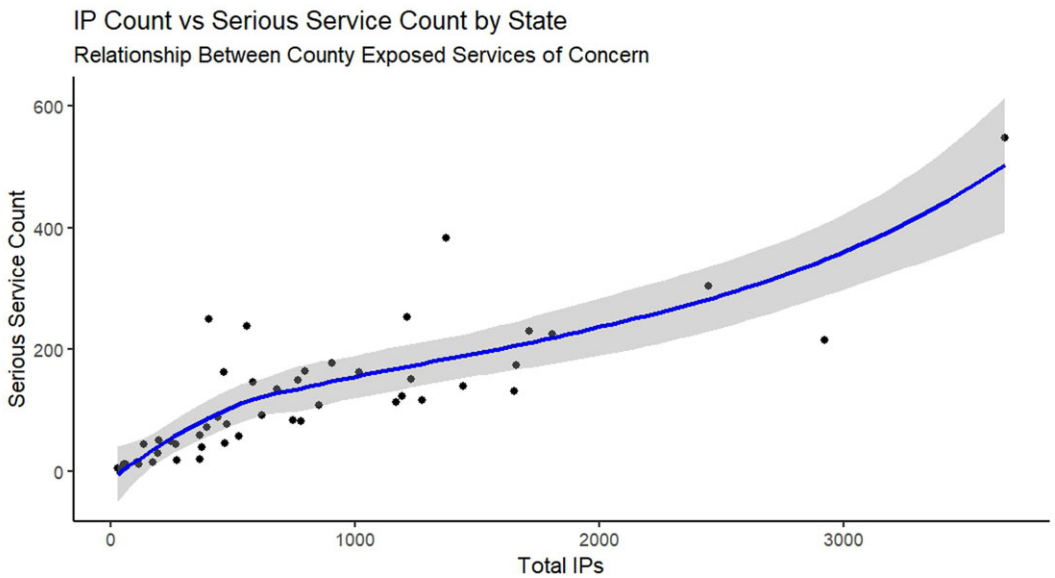


**Figure 12.** Sum of IP addresses versus amount of services of concern exposed at the state level.

Figure 14 shows potential vulnerability to illicit access to government databases. The states of Virginia and Tennessee were found to be at potentially high risk for this type of attack, with respectively 75% and 50% of their counties exposing services that could be exploited for illicit data access.

Figure 15 shows potential vulnerability to insecure authorization to government infrastructures. For most states, more than 50% of their counties are potentially vulnerable to insecure remote authorization by an adversary, due to the high number of remote access services they expose on the public Internet. Virginia with almost 100% of its counties, followed by California and Florida with around 75% of their counties, are leading the list, highlighting the importance of properly applying two-factor authentication and strong password for county government infrastructures.

Figure 16 shows potential vulnerability to insecure file sharing. We were encouraged to learn that most counties do not expose the known-to-be-vulnerable SMB and NETBios services, with Arizona being an outlier, with around 25% of its counties exposing those dangerous services in the wild.

## Attack surface severity: amount, variation, severity, and probability of exploitation in exposed CVEs

Next, we wanted to develop CVE-based measures for the attack surface and understand variations in the amount, severity, and likelihood of exploitation of CVEs across counties. Our dataset with regards to county CVEs is more limited, covering 1003 counties, about a third of all US county governments. Beyond the limitation of missing counties without domain names (34) or counties for which we could not retrieve IP addresses for (15), we have no CVE data for domains with IPs but without open ports (12), domains with IP addresses and open ports but for which we get no CPEs (393), domains that only include

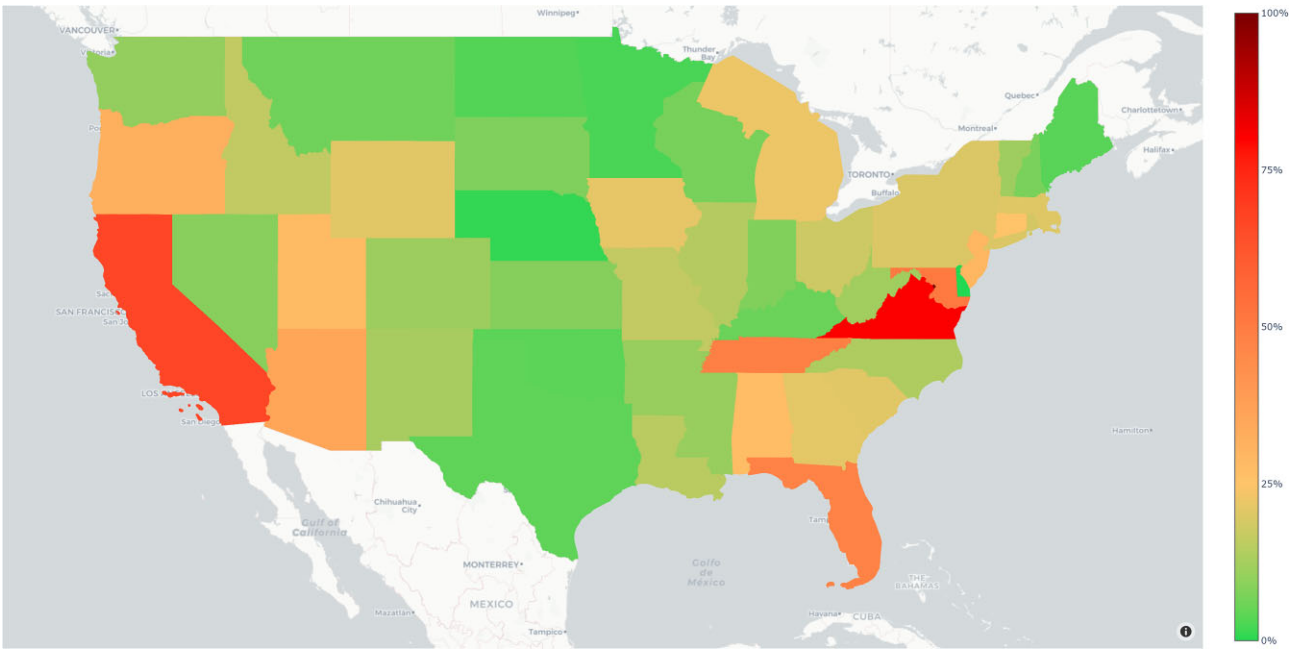


**Figure 13.** Percentage of counties within US states that are potentially susceptible to DNS misconfiguration attacks.

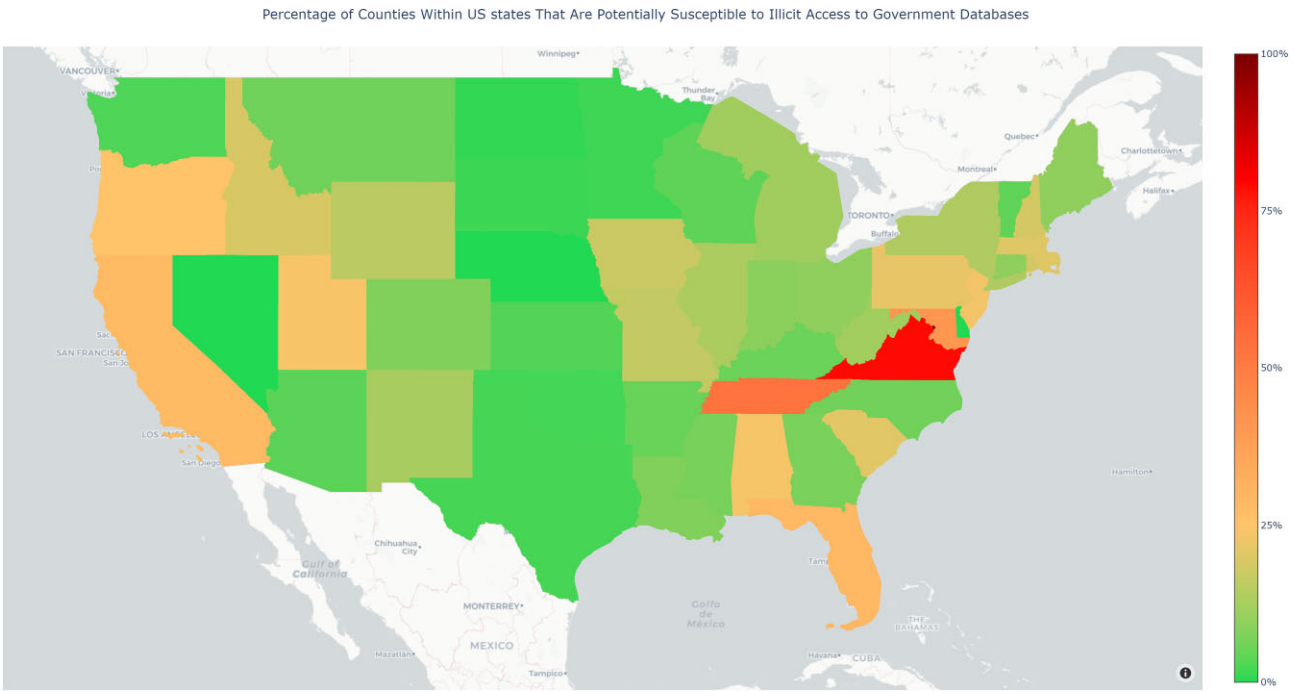


**Figure 14.** Percentage of counties within US states that are potentially susceptible to illicit data access.

nonversioned CPEs that we chose to omit (1232), and domains that only contain CVEs that were classified by Shodan as "Unknown" (2118). Those limitations left us with 1145 domains with CVEs related data, covering 1003 counties.

In the sample Shodan response shown in Appendix 3, of the three CPE returned (two distinct CPE strings), only one of them presented with a CPE version. In this example, with the intent of higher vulnerability confidence and with the goal of providing an accurate accounting for services running on county infrastructure, the Microsoft Windows CPE would not be carried through our analysis. This filter drop is further carried through when CVE are generated through NIST queries, but only for versioned CPE, dropping our covered counties for this section from 3095 out of 3143 (98%), to 1003 out of 3143 (32%). The source of this limitation is missing data from Shodan, either on what CVEs are associated with particular CPE, or the supply of only nonversioned CPEs for the majority of county domains.

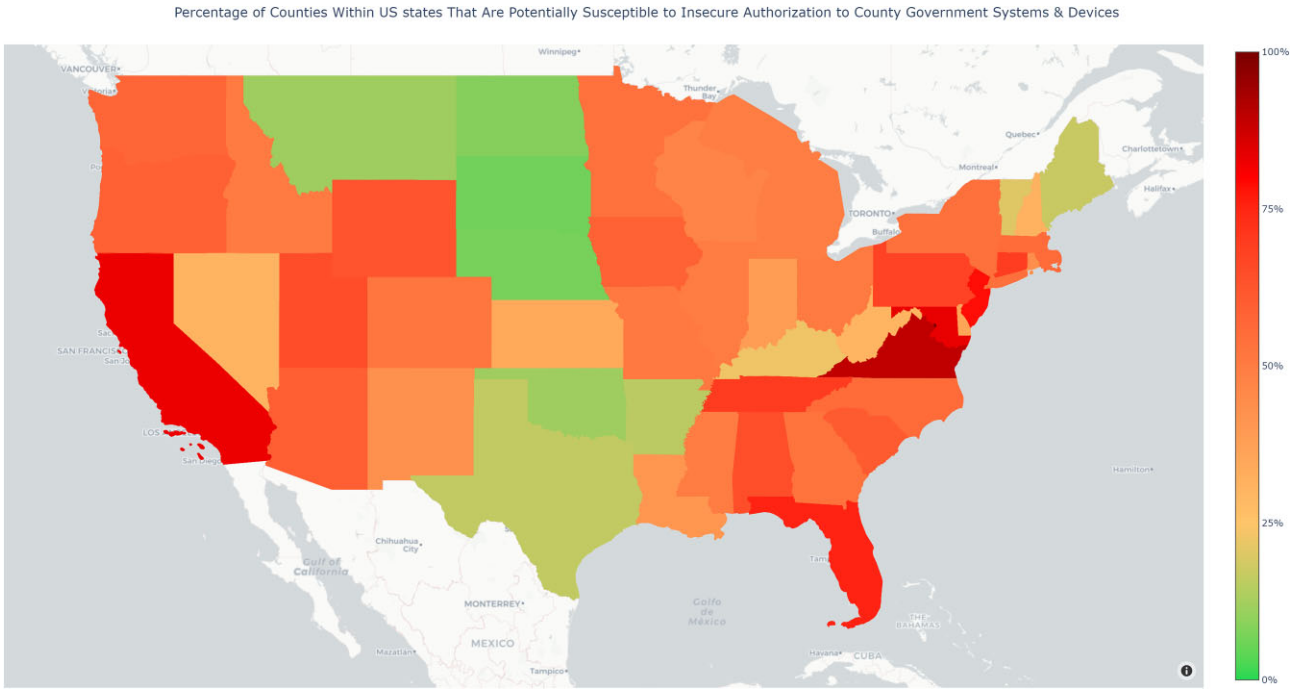


**Figure 15.** Percentage of counties within US states that are potentially susceptible to insecure authorization.

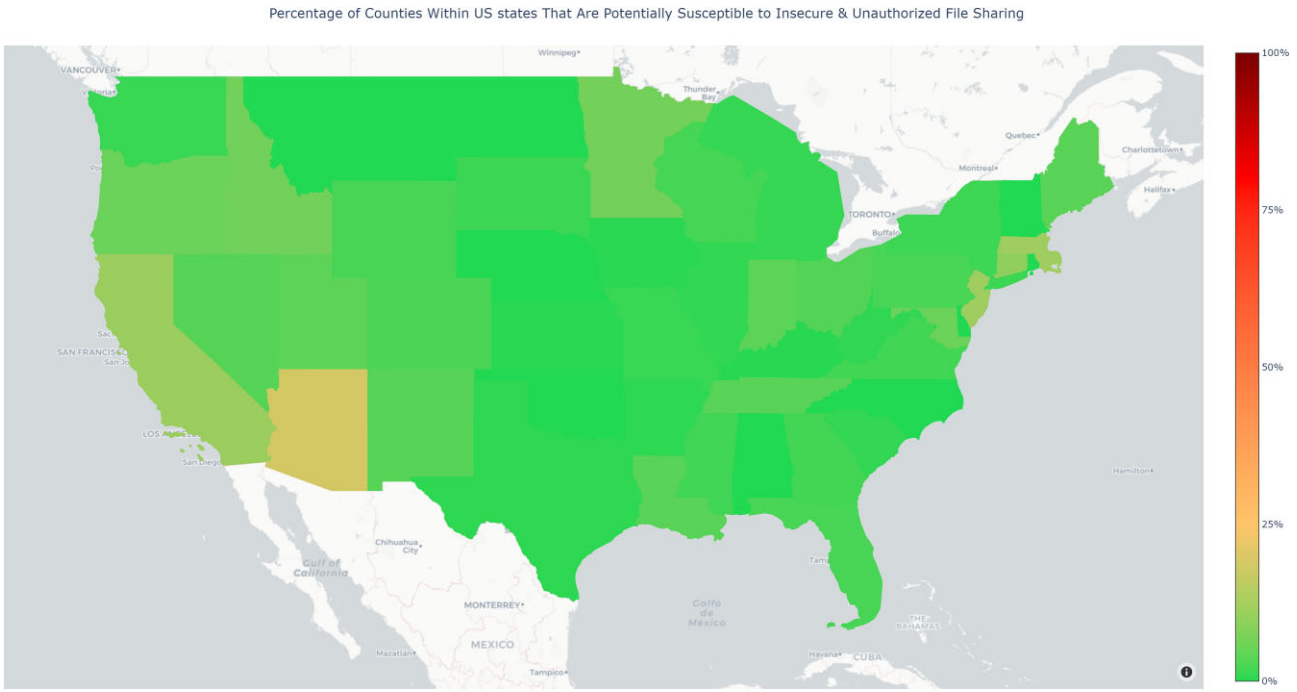


**Figure 16.** Percentage of counties within US states that are potentially susceptible to insecure file-sharing.

Across the 50 states + Washington DC, we were able to collect, on average, versioned CVE data for 33.59% of the counties in each state, with the median percentage across states being 33.3% of the counties covered and a standard deviation (SD) of 18.17. While the percentage of covered counties with CVE data varies between states, the majority of the states have 20%–40% of their counties covered. See the box plot of the distribution of counties with CVE data per state in Fig. 17.

Specifically, for eight states, the majority of the counties are covered, with the states of Wyoming (100%), West Virginia (75%), and Wisconsin (62%) having many counties covered. At the same time, 10 states have less than 20% of its counties with CVE data. Alaska has none, Atlanta and Arizona have less than 10%, and California, Colorado, Connecticut, Washington DC, Delaware, and Florida have less than 20% of their counties covered with CVE data. Sixteen states have between 20% and 33% of their counties with CVE data, and

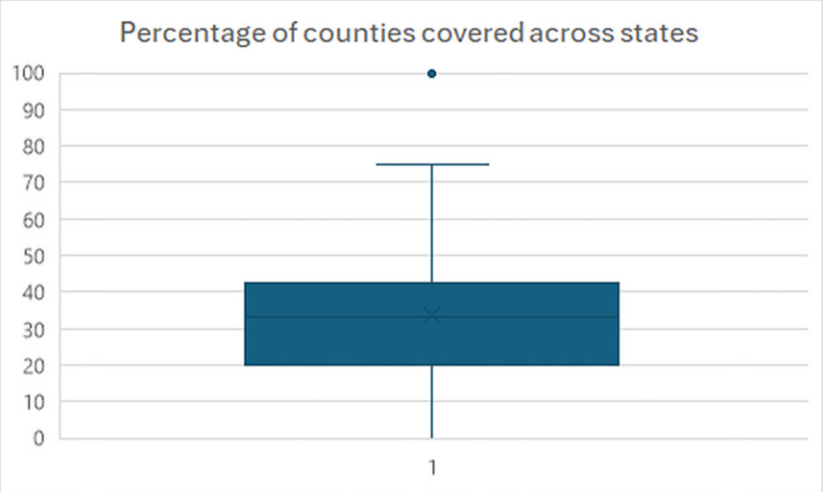


**Figure 17.** Box plot for the distribution of covered counties with CVE data across states.

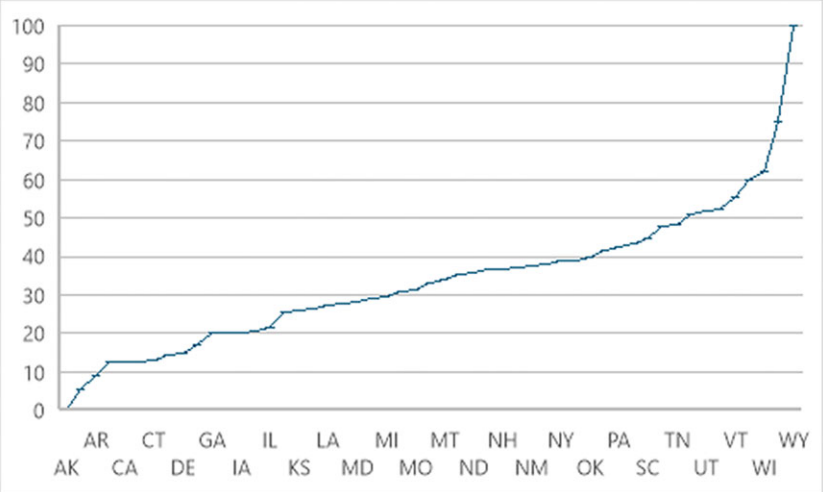


**Figure 18.** Percentage of counties covered with CVE data across states.

17 states have between 34% and 48% of their counties covered. Figure 18 shows the percentage of counties covered with (versioned) CVE data in each state.

Beyond a few outliers, the distribution of missing data is almost evenly spread across the states, maintaining the randomness of the sample and allowing us to still generalize attack surface findings. Data are missing completely at random, and the likelihood of missing values is the same across the vast majority of observations, equally affecting most states.

### CVE density

In contrast to our findings with regards to service-based attack surface measurement, the amount of CVEs across counties is not correlated with the level of population in those counties. The correlation coefficient is 0.1737 and statistically significant at the 99% confidence level ($P$-value < 2.2e-16).

We then moved to investigate "CVE density" for each county, aggregating CVE counts from all IP addresses associated with a county and dividing that by the total number of IP addresses per county. We wanted to get a sense of how vulnerable counties are per each IP address they manage. Figure 19 visualizes this measure across counties, masking the exact location of counties, while visualizing the vulnerable regions. 927 counties have up to 5 CVEs per IP address, the remaining 76 have between 6 and 49(!) CVEs per county IP address (In some cases, a single IP address running a severely outdated operating system or software version generates a significant number of potential vulnerabilities. However, it is important to remember that this analysis is based on the data generated from CENSYS scans that report service responses, which may or not be updated after a patch. CVEs are identified based on these service/software versions.). For five and above CVEs per IP address the counties are colored with dark red. 498 counties have less than 0.5 CVE per IP address and are colored green, and 427 counties are in between 0.5 CVE per IP and 5 CVEs per IP, colored from yellow to orange in the map. Regions colored white are regions with missing CVE data, or regions that are geographically large on the map and colored just by a single dot to mask exact location.

We can see high density of CVEs along the Southern parts of the Mississippi river all the way up to Iowa, in parts of FEMA regions #4, #6, and #7, especially in Louisiana, Mississippi, Tennessee, Atlanta,

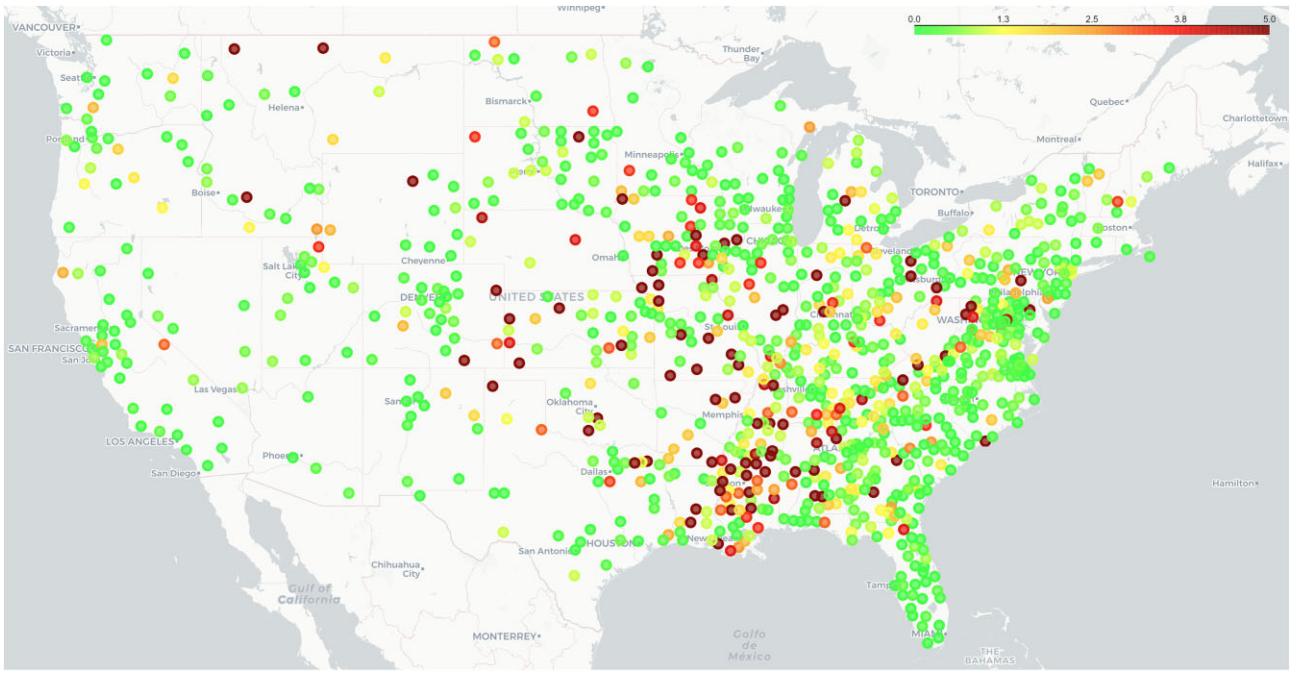


**Figure 19.** CVE density (CVEs per IP address) across US counties.

and Montana. Following our finding about the lack of correlation between total number of CVEs and county population, we also found very weak correlation between the density of CVEs and the overall IP address count for each county. The correlation coefficient is −0.102 and it is significant at the 99% confidence level (*P*-value is .001132).

### Average probability of exploitation

To understand the likelihood of exploitation per county, we summarized the EPSS score for each CVE found in a county and divided that by the total number of CVEs per county. The intuition for this measurement is that a county with just one CVE that is highly likely to get exploited poses a greater risk than a county with many CVEs that are less likely to each get exploited. Figure 20 maps US counties for which we have CVE data for (1003 counties) according to their probability of exploitation per CVE (0–1), masking exact county location, while still showing regional areas of vulnerability and adding important nuances to our CVE density mapping from the previous figure.

Counties are colored based on the average probability of exploitation of their exposed CVEs. Dark red areas suggest a very high probability, on average, for CVE exploitation. We can see that those counties exist across the US, regardless of how populated a region is. Twenty three counties, including counties in VA, TX, NY, NE, MT, MO, KS, IL, AK, MI, IA, IN, CO, and SC suggest a potential probability of exploitation of 95%. Forty-eight counties in the USA suggest an average probability between 74% and 95% to get exploited. These include counties from both more or less populated regions. Sixty-four suggest a probability between 50% and 68% to get exploited, bringing us to 135 counties in our data that face 50% probability or more, on average, to get exploited. As can be seen in the dotted map, those orange to dark red counties come from all over the nation. Populated regions that unsurprisingly stood out in service-based measurement of the attack surface do not necessarily include CVEs that are highly likely to get exploited. Many counties in the east coast or the state of California suggest a probability of exploitation that is 20% or lower. Overall, 664 counties present a probability of exploitation that is less than 20%, with 388 of them suggesting an average exploitation probability of less than 1%. Here again, and in contrast to our findings with regards to service-based attack surface measurement, the average probability of CVE exploitation is not linked to the level of county population. The correlation coefficient is 0.0464 and statistically significant at the 95% confidence level (*P*-value = .0246).

We also explored the relationship between density of CVEs and probability of exploitation across counties. We tested for correlation between CVE count per IP and EPSS score per CVE for each county. We found that for all counties that are above the CVE density median (0.5), the Pearson correlation value is (−0.141) at the 99% confidence level (*P*-value is .00309). This is a very weak but statistically significant lack of correlation between density of CVEs and probability of exploitation, showing that above 0.5, the number of CVEs per IP is not related to the probability of exploitation, stressing the need to patch "smart," rather than patch everything.

### Quantification of cyber risk per county

Mapping exposed infrastructure, their associated CVEs, and the related CVSS and EPSS score for each, allows for the estimation of risk across counties. By definition, risk is a product of severity and probability. For each CVE found in a county, we use its CVSS score as a proxy for severity and EPSS score as a proxy for its probability. We then calculate the average CVSS score across all CVEs found in a county and multiply that by the average EPSS score across all CVEs found in a county. This computation produces a (0–10) risk score per county. The resulting products are mapped geographically to provide a visualization of risk across counties, states, and regions (see Fig. 21).

Every CVE has an associated CVSS score from 0 to 10 based on its exploitability and impact on the target system. Factors such as the attack vector (remote versus local), attack complexity, privileges required, user interaction, and the potential of the vulnerability to affect the confidentiality, integrity, and availability of the target

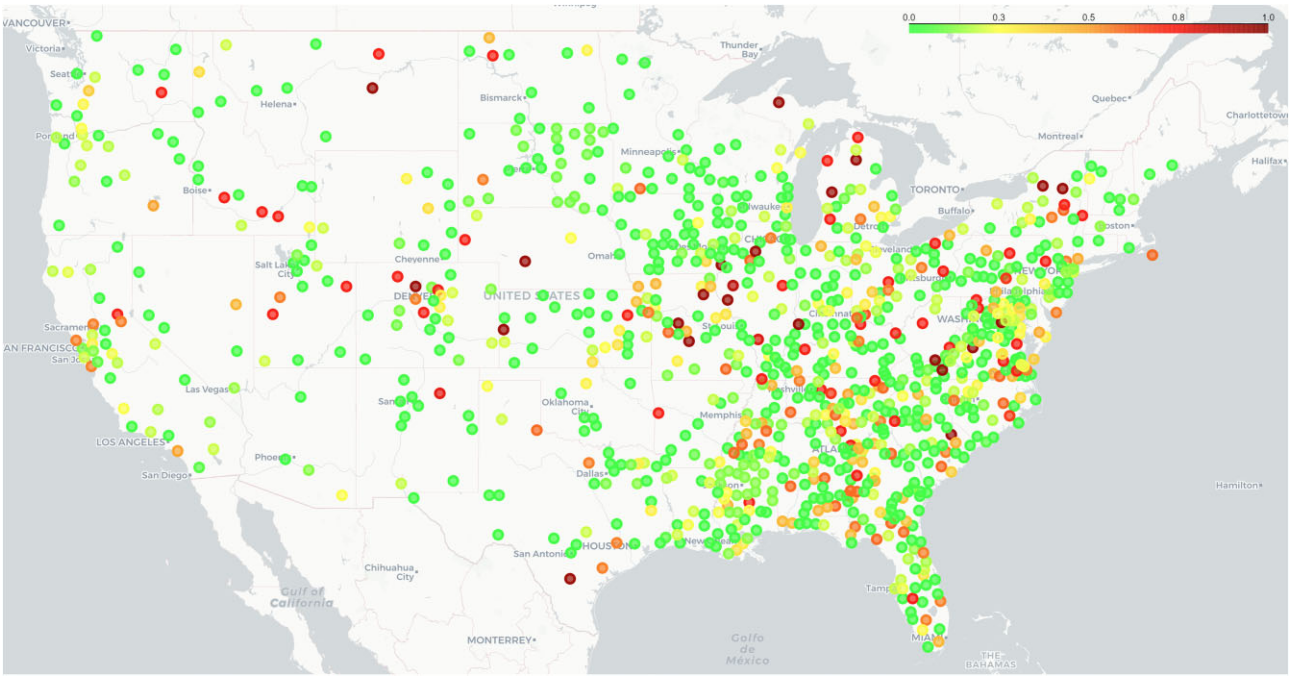


**Figure 20.** Average exploitability probability per CVE across US counties.

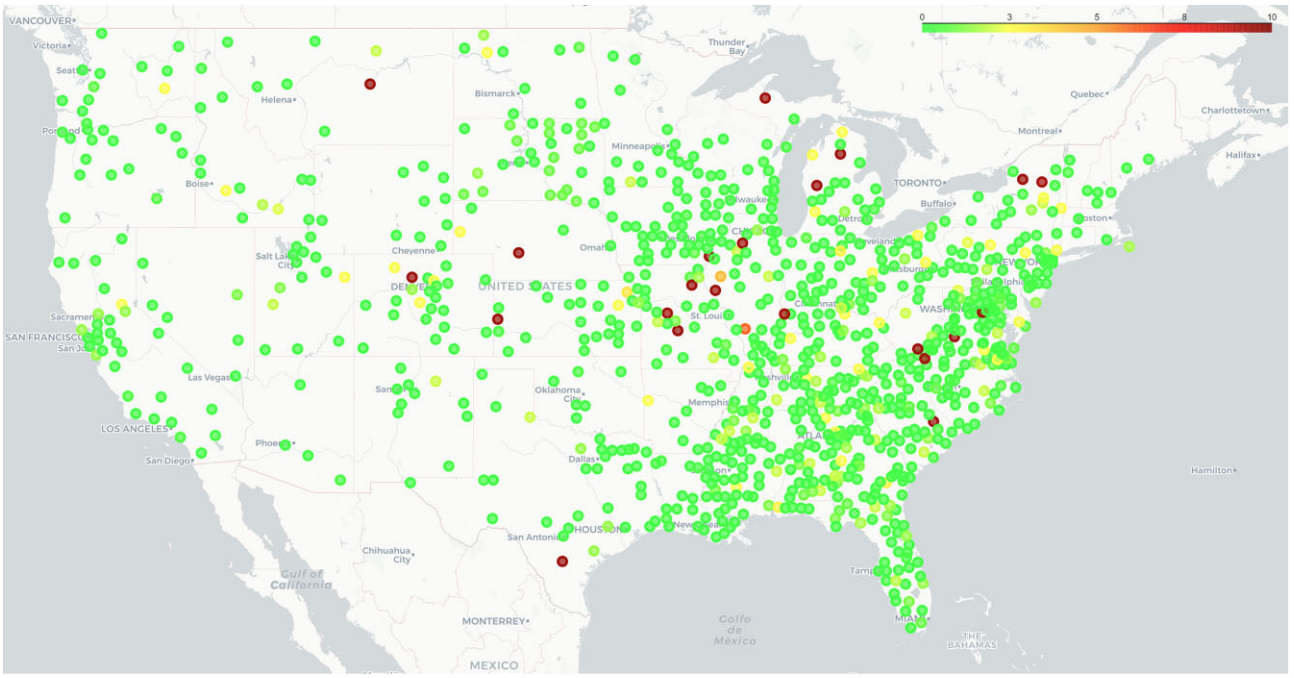


**Figure 21.** Risk quantification for each county across the US.

system are all taken into account. Multiplying that by EPSS, the result is a quantification of the cyber risk posed by each county, based on the computation of risk as: [severity (average CVSS)] ∗ [probability (average EPSS)] for each county.

Figure 21 shows the spread of risk based on our metric across counties. To mask exact county location, we used dotted marks instead of exact county borders/locations, showing only the approximate area of vulnerability. 829 counties have less than 1.0 risk score and are colored green on the map. 89 counties have a score between 1.0 and 2.0 and are colored light green; 52 counties have a risk score between 2.0 and 3.0 and are colored yellow; 3 counties have a score between 3.0 and 6.0 and are orange on the map; and 23 counties have a risk score of more than 9.0 and are colored dark red. The average risk score across counties is 0.586 and the median score is 0.0817.

The counties that pose the greatest risk are spread across the nation, with correlation coefficient between risk score and county population is −0.06 that is statistically significant at the 94% confidence

level (*P*-value is .059). Again, as opposed to service-based attack surface measurement, risky counties are not correlated with population levels, suggesting other contexts for county vulnerability that require further investigation.

**Counties that require immediate attention**

Importantly, not all identified vulnerabilities are of equal concern. In many cases vulnerabilities require direct physical access to devices, are theoretical and have yet to be paired with specific code to take advantage or are found in services not broadly utilized. Therefore, mapping all CVEs is likely to cloud the broader set of concerns among policymakers who might be generally concerned about strategic vulnerability in a county, state, or national environment. In our analysis, we found 852 unique CVEs across 1003 county governments. Of those, six CVEs (0.7%) appear in CISA's Known Exploited Vulnerabilities (KEV) Catalog representing the federal government's areas of greatest concern, and ones likely to be leveraged by threat actor groups (This is much lower than the known baseline of 5% of exploited CVEs from all publicly known CVEs [49], but corresponds to the fact that we are examining only a subset of potentially vulnerable infrastructures—CPEs that are remotely accessible.). Those six specific CVEs are found dispersed across 19 different counties. In one specific California county, we found five CVEs, raising serious concerns about the ability of that county government to manage its potential susceptibility to attack. In the other 18 county governments, we find at least 1 CVE from CISA's KEV catalog. The counties are generally spread across the nation, in both populated and less populated regions. This finding highlights potential areas where national, state, and local policymakers can coordinate and remediate areas of greatest concern.

## Discussion and conclusion

Existing scholarship on county government cybersecurity is methodologically limited, challenging policymakers to make progress in this space. Previous studies rely on employee surveys and fail to assess the strategic threat that county governments pose at the state and national levels. Therefore, despite their importance to national resilience, we have no clear assessment of the threat that county government cyber vulnerabilities create, or a holistic, practiced, and consistent response to such threats across the country.

There is a mismatch between county government technical realities, and the funds allocated at a national or state level to address them. Our methodology and research results can bridge this gap. We rely and further develop existing OSINT-based attack surface measurements to assess county government cybersecurity vulnerability based on the scanning of Internet-facing infrastructures and services of all county governments across the nation, and aggregate and visualize the results at the state, FEMA region, and national levels. We spot geographic areas, where lack of county government cybersecurity is accumulating, potentially impacting national cyber resilience.

Enumerating and assessing the cyber attack surface exposed by US county governments reveal an attack surface that is driven by disparities across counties, states, and FEMA regions. We have shown variations in the amount of IP addresses and open ports available for exploitation across counties and demonstrated how the size of the attack surface is driven by the size of the regional population, with open ports and available IP addresses are positively correlated as well. The quantity of accessible IP addresses and open ports both drive the exploitation-size of an attack surface. These two counts tend to increase and decrease together allowing the degree of one to be a highly suggestive proxy for the degree of the other. Greater needs for online county and local services create more opportunities for attackers. This trend holds when aggregating size results to the FEMA region level as well. The entire southeast part of the country offers a larger county government attack surface than other, less populated, FEMA regions.

Following our discussion on the size of the attack surface, we present first results on the diversity and severity of county government attack surfaces, based on two types of measurements: (1) service-based and (2) CVE-based severity measurements. We first present our rationale for measuring diversity based on the availability of services for exploitation. Often overlooked in regular CVE counts, open services can point hackers into misconfigured software or allow hackers to launch their campaigns based on stolen credentials. This has been found to be the most common attack vector for successful attacks, and we present a first appreciation of open services for exploitation at the county level.

We present our service-based attack surface measurement scale, based on four well-known attack vector scenarios. Results echo the previous trend. Greater service exploitation opportunities exist for highly populated areas, with the states of CA, VA, and FL showing particular concerns. FEMA region #4, in the southeast of the USA, shows the greatest vulnerability and potential for national impact on US cyber resiliency. We do see links between highly populated regions in the east and west coasts and high levels of service-based vulnerabilities, but at the national level, the eight US states of FEMA region #4—Atlanta, Florida, Georgia, Kentucky, Mississippi, North and South Carolina, and Tennessee collectively pose the greatest vulnerability to service-based attacks. Overall, we found larger urban/suburban centers expose larger numbers of people to cyber insecurity risks. Rural communities, however, without the same large demand for digital services, tend to have smaller service-based attack surfaces.

When testing the relationship between the amount of infrastructure to manage and the existence of exploitable services, an interesting trend emerges. We showed how under 1000 IP addresses per state, service diversity increases with the amount of IP addresses. Between 1000 and 2000 IP addresses, we see a sharp decrease in the slope, hinting that the infrastructure in those counties does not introduce significantly more opportunities for attack. But above the 2000 IP addresses mark, the service-based attack surface diversity expands exponentially, hinting at the difficulty of IT managers to navigate larger digital footprints by counties. As the management of IT infrastructure becomes more complex, there is a certain fluctuation point from which counties struggle to keep it safe. The overall trend demonstrates how diversity exposure increases linearly (from 0 to 50 IP addresses), then reaches an equilibrium (roughly between 50 and 2000 IP addresses), only to explode when complexity increases (beyond 2000 IP addresses).

When we break down states' exposure based on the type of attack they might be susceptible to, DNS misconfiguration and insecure authorization are risks across most US states, having more than 50% of their counties susceptible to such attacks. We found that not all services are equally exploitable across the nation—with Virginia standing out as highly susceptible to three out of four attack scenarios, and Arizona exhibits a much higher percentage of exposure across its counties to attacks on its insecure file sharing services.

We contrasted these findings with a CVE-based measurement of the attack surface. We show a contrasting trend for this measurement, as the total number of CVEs is not correlated with levels of population, and the density of CVEs per IP address in counties is not correlated with the overall count of IP addresses available in counties.

CVE density varies across the nation and is very high across counties in certain states, with three counties from the same state holding 49(!) CVEs per managed IP address, on average.

We contrasted that with the average probability of exploitation per CVE, and found 135 counties that on average, have more than 50% probability of getting hacked. Again, the average probability of exploitation is not correlated with population levels and is not correlated with CVE density for counties that have more than 0.5 CVE per IP address (the median of the CVE density distribution). This finding demonstrates the urgent need to "patch smart" instead of patching "everything."

The CVE-based attack surface measurement shows no correlation with population levels, Counties that are less populated appear as risky if not more, compared to counties that are heavily populated. The measure enabled us to recognize 19 counties that need immediate attention, as their potential CVEs appear in CISA's KEV catalog. In contrast to highly populated regions that drove the size, complexity, and severity of service-based attack scenarios, probability of CVE exploitation is as high for less populated counties, uncovering the difficulty to secure county-level infrastructures even for rural and small counties. Our research team is in the process of finding and notifying appropriate points of contact for the most vulnerable configurations discovered.

CVE-based measurement of the attack surface has also enabled the quantification of the risk posed by counties based on the (severity × probability) formula. We recognized 23 counties that introduce very high levels of risk, at the 9.0 out of 10.0 level, while the vast majority of the counties (829) present very low risk levels, up to 1.0 out of 10.0. The risk score for counties is not correlated with county population levels, suggesting alternative contexts for CVE-based vulnerabilities across counties.

The results open an important discussion on how to cope with county government attack surface to ensure national resilience. Should we be guided by size, and shrink the exposed services to decrease the size of the surface in highly populated areas? Or should we hand pick our patching efforts to close CVEs of exploits that are already visible in the wild, even for counties with a small footprint? According to the service-based measure, we found that large counties have greater potential vulnerability and shrinking the amount of exposed services would decrease the chances of service misconfiguration and increase the security of systems in those regions. At the same time, highly exploitable CVEs sporadically exist across the nation and might serve as an easy starting point for threat actors, regardless of county configurations. Simply put, should we shrink large attack surfaces as much as possible, or patch specific CVEs in smaller networks? What can make counties good in one but not in the other?

We argue that both service- and CVE-based measurements of the attack surface are valid and help put county vulnerability in context. The projected effects of attacks on highly populated counties differ from attacks on small county networks, where lateral movement might be limited. At the same time, unauthorized access to smaller counties might be easier due to lack of resources and capacities to properly protect the residents. Each type of exposed vulnerability holds different implications for national resilience, and both should be jointly considered in the effort to address the integrated attack surface exposed by US county governments. Minimizing cyber risk can proceed through both risk measures, each addressing different types of threat actors on the one hand, and organizational capacities within counties on the other hand. The automation and visualization of both measures, over time, would help policymakers direct their resources based on the type of risk they aim to minimize.

## Limitations

Our results have a few important limitations. First, we have missing data for both service- and CVE-based attack surface measurements. Service-based measurement covers 98% of all US counties, and as noted earlier, we are still missing 34 missing county governments for which we have no domains and 15 county domains without IP information. CVE-based measurement covers 32% of all counties, with each state having between 20% and 40% of its counties covered with a few outliers (see Section 4.4). The selection bias does not impact the ability to generalize from our results since data is missing completely at random, but we are working to address the sources of those limitations, which mostly come from Shodan's classification of CVEs as "Unknown" for CPEs that were identified with their version. Our plan is to bypass Shodan's CVE information retrieval by conducting direct queries to the NVD database based on the versioned CPEs that we get for each county. Direct NVD queries of single CVE proved to be, at the time, infeasible with query limits and token access, but remains an open goal for future research and possible attack surface model improvements.

Second, we are only measuring the publicly exposed attack surface, as identified through scans of the public Internet. We have yet to complement this measurement through interviews with counties and get a more complete picture of county networks. Deeper assessment of individual networks might reveal more complex attack surfaces that would add greater fidelity to the analysis presented in this paper.

Third, our results for the severity of the attack surface represent a high bound of county vulnerability and do not necessarily determine that county governments are exposed. For service-based measurements, our results are a high bound because the county service might be properly configured. There is a wide set of configurations, such as two-factor authentication and forbidden anonymous access, that can be associated with the exposed services and make the job of hackers much more difficult. For CVE-based measures our results are a high-bound as well. County systems might be patched without an effect on CPE versions, or old version CPEs might have been backported, so the given CVE indications for the collected CPEs might not reflect the actual vulnerability status. In order to improve our attack surface measurement, we will need to be able to evaluate the defense mechanisms applied by counties.

Nonetheless, it remains urgent to pay attention to the existence of the reported CVEs collected from the public Internet. The OSINT-based tools used for this research are available to attackers as well, who can conduct large-scale scans of vulnerable county hosts within mere hours of a vulnerability disclosure. While their exploitability depends on various factors, being aware of these vulnerabilities would enable counties and decision makers to assess risks, take necessary measures to reduce them, and actively manage vulnerabilities to improve counties' security posture. The exposure of widely known vulnerable services such as RDP, TELNET, FTP, and SMB, or county CVEs that either appear in CISA's KEV catalog or have a close to one EPSS score, or a high risk score, point to regional areas that deserve careful attention.

## Insights for policymakers

Our approach, which quantifies and explores integrated attack surfaces across geographies, is useful for policymakers who struggle to determine where to invest scarce resources. Even though our attack surface measurements suggest a high bound for county vulnerabilities, they put a spotlight on regions that require careful attention and investment of resources to close the gaps. Locally man-

aged infrastructures, whose vulnerabilities are not wholly understood can lead to misperceptions of risk and limit the effectiveness of state or national lawmakers who seek to support local government cybersecurity. For example, in the state of Maryland, the 2022 "Local Cybersecurity Support Act" ("The Local Cybersecurity Support Act" provides a sizable fund for state leaders to allocate to local governments to assist in the management of risk to government networks, thereby providing a mechanism to actively strategically manage cyber risk at the local level [50].) provides funding for state officials to assist county and municipal governments in improving their local cybersecurity. However, given the localized nature of network management, those same policymakers might struggle to identify risks across all counties and municipalities in their state. By linking county geographies with network infrastructure, exposed services, and CVEs, our approach allows state and national leaders to quantify the size, scope, and depth of exposed infrastructure. This could help policymakers assess the county government cybersecurity risk in a more strategic manner, and invest resources accordingly.

We provide, for the first time, data and tools for US policymakers to grasp the scope of the problem, across various regional levels, through various attack surface measures, allowing the prevention of future harms. Our goal in this paper is to explain our novel methodology and demonstrate its applicability to the cyber risk management efforts of local and national government officials. We view this as a continuous effort for better assessing and acting upon cybersecurity risks at the county level and their potential national impact. The findings raise serious concerns about the ability of county government officials to address the cybersecurity threat that their digital infrastructures are creating, calling for urgent funding and a more careful management of IT infrastructures for US government counties. The data we chose to share here is only part of a much larger dataset that can help policymakers reach evidence-based decisions on county government cybersecurity.

More broadly, our data and methodological approach have clear applications for increasing US cyber resiliency. CISA for instance, as the national cybersecurity critical infrastructure coordinator, has been providing alerts noting active exploitation of exposed services. For example, Chinese threat actors were observed accessing critical infrastructure providers supporting military facilities in the US territory of Guam [51]. Exploiting the FORTIGUARD service, Chinese state actors accessed key infrastructure that posed a significant risk to US military operations. Applying that specific example in our dataset, we note that there are over 63 counties potentially susceptible to the same approach. National policymakers as well as state officials utilizing this approach can more readily identify exploitable services and direct emergency actions to resolve the issue expeditiously.

## Future research

This project has opened a rich set of opportunities for future research. First, we can expand on attack surface variations between sectors with counties, exploring various critical infrastructures managed by independent organizations but tied to specific geographies. For example, instead of focusing solely on county governments, an analysis that incorporates hospitals, transport links, or schools could provide a more comprehensive view of vulnerability for a particular population. We plan to query the various domains that were found through collected SSL certificates by Censys to understand the different types of county government infrastructures in our data. We also found clusters of shared hosting services through a single IP across various counties, making a specific infrastructure a single point of failure for many counties at once. We aim to uncover those ties and understand who is vulnerable to the same attack vector. Inevitably, our lack of access to county government officials thus far, prevents us from mapping each county with greater precision. We are now in the process of working with some state governments to study county government attack surfaces with the counties themselves and understand when and how counties rely on state infrastructures, allowing for a potentially richer and nuanced understanding of their attack surfaces, as well as building relationships, practices, tools, and procedures to best nationalize vulnerability identification and response mitigation.

Second, we can further study the temporal development of the attack surface. With regular data collection contextualized by sector (e.g. county government) and geography, there is an opportunity to identify not only where unverified vulnerabilities exist, but also how quickly they might be resolved. Given the concern among policymakers about the speed at which vulnerabilities in critical infrastructures are addressed, this research is likely to be welcomed and can highlight where government programs may or may not support broader strategic cybersecurity goals. Specifically, analysis about the temporal dimensions of this approach offers a rich area for exploration with specific focus on the dynamic nature of the attack surface itself. This expansion would also enable an analysis of adoption of CISA recommendations stemming from its advisory notification services to state and local officials.

Our methodology defines an approach to leverage publicly accessible, or at least knowable, information. However, as it relies on data "seen" from outside the organization it limits the ability for policymakers to fully appreciate the risks internal to organizations residing throughout an entire sector. This approach could be augmented with internally collected data deemed more sensitive but available to policymakers, thereby greatly improving the conclusions of the analysis. More plainly, despite some limitations this approach provides an ability to aggregate findings through the context of sector and geography while creating opportunities to supplement it with information more closely protected by policymakers to expand the quality and precision of the risk analysis.

Third, the paper can also serve as a starting point for building more sophisticated measures for attack surfaces that allow for a scaled score displayed across the country. However, how that score is constructed warrants further exploration, with alternative approaches identified and tested to determine better methods for understanding security at scale. For instance, we plan to come up with more nuanced and contextual scores for the severity of CVEs found in county government networks. We currently rank vulnerable infrastructure based on their open services, and CVEs with certain CVSS and EPSS scores, but those existing scales do not take into account the aggregated regional and sectoral contexts of software vulnerabilities, missing important aspects of their effects and severity. Looking ahead, we plan to merge the existing risk quantification for CVE exploitation with regional and sectoral variables on county government networks and CPE indexes and operating systems distributions. We plan to include additional OSINT-based datasets, including the ability to combine exposed services with compromised credentials found on the dark web to expand our ability to make more nuanced estimates of risk, tying exposure with access credentials and analyze the ratio of known valid accounts paired with open services.

## Conflict of interest

None declared.

## Funding

None declared.

## Acknowledgments

We are grateful for the valuable research support provided by Mr Parthav Poudel. We would like to thank Rishipal Yadav and Ann Daley for their support in earlier phases of the project. We are also thankful to Mrs DeBrae Kennedy-Mayo for her wonderful comments and feedback provided during the 2023 Cybersecurity Law and Policy Scholars Conference, and anonymous reviewers who helped us significantly improve the paper.

## Author contributions

Charles Harry (Conceptualization [equal], Investigation [equal], Methodology [equal], Project administration [equal], Resources [equal], Software [equal], Supervision [equal], Validation [equal], Visualization [equal], Writing – original draft [equal], Writing – review & editing [equal]), Ido Sivan-Sevilla (Conceptualization [equal], Data curation [equal], Formal analysis [equal], Investigation [equal], Methodology [equal], Resources [equal], Software [equal], Supervision [equal], Validation [equal], Visualization [equal], Writing – original draft [equal], Writing – review & editing [equal]), and Mark McDermott (Conceptualization [equal], Data curation [equal], Formal analysis [equal], Investigation [equal], Methodology [equal], Software [equal], Validation [equal], Writing – review & editing [equal]).

## Appendix 1: output sample from CENSYS

```
>>> from censys.search import CensysHosts
>>> censys_hosts = CensysHosts()
>>> result_censys = list(censys_hosts.search(query_term, per_page=100, pages=200))

>>> print(json.dumps(result_censys, indent=3))
[
  [
    {
      "dns": {
        "reverse_dns": {
          "names": [
            "xxx-xx-xx-xx-xxx.us-west-2.compute.amazonaws.com"
          ]
        }
      },
      "last_updated_at": "YYYY-MM-DDTHH:MM:SS.SSSZ",
      "autonomous_system": {
        "country_code": "US",
        "description": "AMAZON-02",
        "bgp_prefix": "1.2.0.0/14",
        "asn": xxxxx,
        "name": "AMAZON-02"
      },
      "ip": "1.2.3.4",
      "services": [
        {
          "port": 80,
          "extended_service_name": "HTTP",
          "transport_protocol": "TCP",
          "service_name": "HTTP"
        },
        {
          "port": 443,
          "certificate": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
          "transport_protocol": "TCP",
          "service_name": "HTTP",
          "extended_service_name": "HTTPS"
        }
      ],
      "location": {
        "city": "some-city",
        "coordinates": {
          "latitude": 0.000,
          "longitude": 0.000
        },
        "country_code": "US",
        "province": "Oregon",
        "continent": "North America",
        "country": "United States",
        "timezone": "America/Los_Angeles",
        "postal_code": "xxxxx"
      },
      "matched_services": [
        {
          "port": 443,
          "extended_service_name": "HTTPS",
          "transport_protocol": "TCP",
          "service_name": "HTTP",
          "certificate": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
        }
```

Continued


```
        ]
      },
      {
        "dns": {
          "reverse_dns": {
            "names": [
              "xxx-xx-xxx-xxx-xxx.us-west-2.compute.amazonaws.com"
            ]
          }
        },
        "autonomous_system": {
          "description": "AMAZON-02",
          "bgp_prefix": "1.2.0.0/11",
          "asn": xxxxx,
          "name": "AMAZON-02",
          "country_code": "US"
        },
        "services": [
          {
            "transport_protocol": "TCP",
            "service_name": "HTTP",
            "extended_service_name": "HTTP",
            "port": 80
          },
          {
            "port": 443,
            "transport_protocol": "TCP",
            "certificate": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
            "service_name": "HTTP",
            "extended_service_name": "HTTPS"
          }
        ],
        "last_updated_at": "YYYY-MM-DDTHH:MM:SS.SSSZ",
        "ip": "1.2.3.4",
        "location": {
          "country": "United States",
          "coordinates": {
            "longitude": -119.70058,
            "latitude": 45.83986
          },
          "timezone": "America/Los_Angeles",
          "postal_code": "97818",
          "country_code": "US",
          "city": "Boardman",
          "province": "Oregon",
          "continent": "North America"
        },
        "matched_services": [
          {
            "extended_service_name": "HTTPS",
            "port": 443,
            "transport_protocol": "TCP",
            "service_name": "HTTP",
            "certificate": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
          }
        ]
      }
    ]
}
```

## Appendix 2: output sample from SHODAN

```
>>> import requests
>>> STRING_SHODAN_ENDPOINT_BASE = "https://internetdb.shodan.io/"
>>> query_string_shodan = STRING_SHODAN_ENDPOINT_BASE + "1.2.3.4"
>>> result_shodan = requests.get(query_string_shodan).json()
>>> print(json.dumps(result_shodan, indent=3))

sample 1:
{
   "ip": "1.2.3.4",
   "cpes": [
      "cpe:/a:microsoft:internet_information_services:10.0",
      "cpe:/a:jquery:jquery",
      "cpe:/o:microsoft:windows",
      "cpe:/a:getbootstrap:bootstrap",
      "cpe:/a:microsoft:internet_information_services"
   ],
   "hostnames": [],
   "ports": [80, 443],
   "tags": [
      "cloud"
   ],
   "vulns": []
}

sample 2:
{
    "ip": "1.2.3.4",
    "cpes":[
        "cpe:/o:microsoft:windows",
        "cpe:/a:microsoft:internet_information_services:7.5",
        "cpe:/a:microsoft:internet_information_services"
    ],
    "hostnames":["domain.com","www.domain.com"],
    "ports":[80,443],
    "tags":[],
    "vulns":[
        "CVE-2010-3972",
        "CVE-2010-2730",
        "CVE-2010-1899"]
}
```

## Appendix 3: output sample from NIST for CPE

```
FROM SHODAN: cpe:/a:getbootstrap:bootstrap

Python Conversion:
cpe.CPE('cpe:/a:getbootstrap:bootstrap').as_fs()          >> 'cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:*'

Hyphen conversion to cpeName:
https://services.nvd.nist.gov/rest/json/cves/2.0?cpeName=cpe:2.3:a:getbootstrap:bootstrap:-:*:*:*:*:*:*:*

{
    "resultsPerPage":5,
    "startIndex":0,
```

Continued


```
"totalResults":5,
"format":"NVD_CVE",
"version":"2.0",
"timestamp":"2023-12-06T11:30:50.280",
"vulnerabilities":[
  {"cve":{
      "id":"CVE-2018-14040",
      "sourceIdentifier":"cve@mitre.org",
      "published":"2018-07-13T14:29:00.213",
      "lastModified":"2023-11-07T02:52:53.940",
      "vulnStatus":"Modified",
      "descriptions":[
        {"lang":"en","value":"In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute."},
        {"lang":"es","value":"xxx"}
      ],
      "metrics":{
        "cvssMetricV30":[
          {
            "source":"nvd@nist.gov",
            "type":"Primary",
            "cvssData":{
              "version":"3.0",
              "vectorString":"CVSS:3.0\/AV:N\/AC:L\/PR:N\/UI:R\/S:C\/C:L\/I:L\/A:N",
              "attackVector":"NETWORK",
              "attackComplexity":"LOW",
              "privilegesRequired":"NONE",
              "userInteraction":"REQUIRED",
              "scope":"CHANGED",
              "confidentialityImpact":"LOW",
              "integrityImpact":"LOW",
              "availabilityImpact":"NONE",
              "baseScore":6.1,
              "baseSeverity":"MEDIUM"
            },
            "exploitabilityScore":2.8,
            "impactScore":2.7
          }
        ],
        "cvssMetricV2":[
          {
            "source":"nvd@nist.gov",
            "type":"Primary",
            "cvssData":{
              "version":"2.0",
              "vectorString":"AV:N\/AC:M\/Au:N\/C:N\/I:P\/A:N",
              "accessVector":"NETWORK",
              "accessComplexity":"MEDIUM",
              "authentication":"NONE",
              "confidentialityImpact":"NONE",
              "integrityImpact":"PARTIAL",
              "availabilityImpact":"NONE",
              "baseScore":4.3
            },
            "baseSeverity":"MEDIUM",
            "exploitabilityScore":8.6,
            "impactScore":2.9,
```

Continued


```
                    "acInsufInfo":false,
                    "obtainAllPrivilege":false,
                    "obtainUserPrivilege":false,
                    "obtainOtherPrivilege":false,
                    "userInteractionRequired":true
                }
            ]
        },
        "weaknesses":[
            {"source":"nvd@nist.gov","type":"Primary","description":[{"lang":"en","value":"CWE-79"}]}
        ],
        "configurations":[
            {
                "nodes":[
                    {
                        "operator":"OR",
                        "negate":false,
                        "cpeMatch":[
                            {
                                "vulnerable":true,
                                "criteria":"cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*",
                                "matchCriteriaId":"C11E6FB0-C8C0-4527-9AA0-CB9B316F8F43"
                            }
                        ]
                    }
                ]
            },
            {
                "nodes":[
                    {
                        "operator":"OR",
                        "negate":false,
                        "cpeMatch":[
                            {"vulnerable":true, "criteria":"cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:*", ...}
                            {"vulnerable":true, "criteria":"cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:*", ...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*", ...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*",...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*",...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha4:*:*:*:*:*:*",...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*",...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*",...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*",...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*",...}
                            {"vulnerable":true,"criteria":"cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*",...}
                        ]
                    }
                ]
            }
            ],
            "references":[ … ]
    }},
    {"cve":{"id":"CVE-2018-14042", ... }},
    {"cve":{"id":"CVE-2018-20676", ... }},
    {"cve":{"id":"CVE-2018-20677", ... }},
    {"cve":{"id":"CVE-2019-8331",  ... }}
  ]
}
```

## Appendix 4: output sample from NIST without CPE query

```
https://services.nvd.nist.gov/rest/json/cves/2.0?startIndex=0&resultsPerPage=XXXX
{
   "resultsPerPage": XXXX,
   "startIndex": 0,
   "totalResults": 240564,
   "format": "NVD_CVE",
   "version": "2.0",
   "timestamp": "2024-03-05T15:08:36.657",
   "vulnerabilities": [
      {"cve": {"id": "CVE-1999-0095", ... }}
      {"cve": {"id": "CVE-1999-0082", ... }}
      ... total of XXXX results …
   ]
}
```

## References


1. King A, Gallagher M. *Cyberspace Solarium Commission Report*. Washington, DC: U.S. Congress, 2020.
2. Norris DF, Mateczun L, Joshi A. *et al.* Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Adm Rev* 2019;**79**:895–904.
3. Macmanus SA, Caruson K, Mcphee BD. Cybersecurity at the local government level: balancing demands for transparency and privacy rights. *J Urban Aff* 2013;**35**:451–70.
4. Ponemon Institute. *State of Cybersecurity in Local, State & Federal Government*., Traverse City, MI, 2015.
5. Hatcher W, Meares WL, Heslen J. The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. *J Cyber Pol* 2020;**5**:302–25.
6. Norris DF, Mateczun LK. Cyberattacks on local governments 2020: findings from a key informant survey. *J Cyber Pol* 2022;**7**:294–317.
7. Caruson K, MacManus SA, McPhee BD. Cybersecurity policy-making at the local government level: an analysis of threats, preparedness, and bureaucratic roadblocks to success. *J Homeland Secur Emer Manag* 2012;**9**. https://doi.org/10.1515/jhsem-2012-0003.
8. Sophos. The state of ransomware in government 2021. Abingdon, 2021.
9. Preis B, Susskind L. Municipal cybersecurity: more work needs to be done. *Urban Aff Rev* 2022;**58**:614–29.
10. Bagwe M. Cyberattack on records vendor affects scores of US counties. Princeton, NJ: BankInfoSecurity, 2023. https://www.bankinfosecurity.com/cyberattack-on-records-vendor-affects-scores-us-counties-a-20856 (12 September 2024, date last accessed).
11. Marks J. A 2020 ransomware attack is still harming Baltimore teachers. Washington, DC: *Washington Post*, 2022. https://www.washingtonpost.com/politics/2022/04/18/2020-ransomware-attack-is-still-harming-baltimore-teachers/ (5 July 2023, date last accessed).
12. Caldarulo M, Welch EW, Feeney MK. Determinants of cyber-incidents among small and medium US cities. *Govt Inf Quart* 2022;**39**:101703.
13. DHS. *Critical Infrastructure: Long-Term Trends and Drivers and Their Implications for Emergency Management*. Washington, DC: Department of Homeland Security, 2011.
14. DHS. *Cyber Risk Economics Capability Gaps Research Strategy*. Washington, DC: Department of Homeland Security, 2018.
15. Federal Bureau of Investigation. *Internet Crime Report*. Washington, DC, 2022.
16. Healey J. Measuring policy effectiveness of cyber defensibility and deterrence. Washington, DC: Lawfare, 2024.
17. Lovric E, Moric Z, Redzepagic J. *et al.* Detecting security vulnerabilities on internet-connected devices. In: Katalinic B (ed.), *DAAAM Proceedings*. Vol. **1**. 1st edn. Vienna: DAAAM International, 2023, 0103–10.
18. Everson D. Cyber attack surface mapping for offensive security testing. Dissertation, The Graduate School at Clemson University, 2023.
19. Klick J, Koch R, Brandstetter T. Epidemic? The attack surface of German hospitals during the COVID-19 Pandemic. In: *Proceedings of the 2021 13th International Conference on Cyber Conflict (CyCon)*. Tallinn: IEEE, 2021, 73–94.
20. Rathi J. Mapping the attack surface of telecommunication networks from the public internet. Stockholm: KTH Royal Institute of Technology, 2023.
21. Pervez MH, Dağ H. Risk assessment for critical infrastructure: a novel approach using OSINT Framework. *Authorea* 2024. https://doi.org/10.22541/au.172114508.86122493/v1.
22. Pereira AKF. Resilience to cyber-attacks in critical infrastructures of Portugal. Lisboa: Edições Sílabo, 2021.
23. Ashley T, Gourisetti SNG, Brown N. *et al.* Aggregate attack surface management for network discovery of operational technology. *Comput Secur* 2022;**123**:102939.
24. Howard M, Pincus J, Wing JM. Measuring relative attack surfaces. In: Lee DT, Shieh SP, Tygar JD (eds), *Computer Security in the 21st Century*. Boston, MA: Springer, 2005, 109–37.
25. Theisen C, Munaiah N, Al-Zyoud M. *et al.* Attack surface definitions: a systematic literature review. *Inf Softw Technol* 2018;**104**:94–103.
26. NIST. *Security and Privacy Controls for Information Systems and Organizations*. Revision 5. Gaithersburg, MD: National Institute of Standards and Technology, 2020.
27. Gatlan S. Hundreds of devices found violating new CISA federal agency directive. Huntington Station, NY: Bleeping Computer, 2023.
28. US Census Bureau. Counties and Statistically Equivalent Areas of the United States, Puerto Rico, and the Island Areas (2020). Census.gov. Suitland-Silver Hill, MD, 2020.
29. GSA. A complete list of .gov domains. Washington DC, USA. 2014. https://18f.gsa.gov/2014/12/18/a-complete-list-of-gov-domains/.
30. Censys. Exposure Management and Threat Hunting Solutions. 2023. https://censys.com/.
31. The White House. *State and Local Government*. Washington, DC.
32. Benton JE, Kincaid J. *Counties as Service Delivery Agents: Changing Expectations and Roles*. 1st edn. Westport, CT: Praeger, 2002.
33. FEMA.gov. *Regions, States and Territories*. Hyattsville, MD, 2022.
34. IANA. Service name and transport protocol port number registry. Los Angeles, CA, 2023.
35. CISA. *CISA Analysis: Fiscal Year 2023 Risk and Vulnerability Assessments*. Washington, DC, 2024.
36. DFIR. Buzzing on Christmas Eve: trigona Ransomware in 3 hours. *The DFIR Report*. 2024.
37. Lakshmanan R. Apache OpenMeetings web conferencing tool exposed to critical vulnerabilities. The Hacker News, 2023.

38. Arghire I. Veeam patches critical vulnerabilities in enterprise products. SecurityWeek, 2024.
39. CloudFlare. What is a DNS flood? | DNS flood DDoS attack. 2023.
40. Davis J. Healthcare websites flooded by fake requests in ongoing DDoS attacks. SC Media, 2023.
41. CISA. Progress Software releases security advisory for MOVEit transfer. Washington, DC, 2023.
42. Toulas B. New Mirai malware variant infects linux devices to build DDoS botnet. Huntington Station, NY: Bleeping Computer, 2023.
43. CISA. *#StopRansomware: BianLian Ransomware Group*. Washington, DC, 2023.
44. NJCCIC. *Remote Access: Open Ports Create Targets of Opportunity, Undue Risk*. West Trenton, NJ, 2017.
45. Chappell B, Neuman S. U.S. Says North Korea "directly responsible" for WannaCry ransomware attack. NPR, 2017. https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack (28 June 2023, date last accessed).
46. Fruhlinger J. WannaCry explained: a perfect ransomware storm. Framingham, MA: CSO Online, 2022.
47. Eset.com. Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN. Bratislava, 2017.
48. Microsoft.com. Secure SMB Traffic in Windows Server. Washington, DC, 2023.
49. Jacobs J, Romanosky S, Adjerid I. *et al*. Improving vulnerability remediation through better exploit prediction. *J Cybersecur* 2020;**6**. https://doi.org/10.1093/cybsec/tyaa015.
50. State of Maryland. Legislation—SB0754. Annapolis, MD, 2022.
51. Microsoft Threat Intelligence. Volt Typhoon targets US critical infrastructure with living-off-the-land techniques. Washington, DC: Microsoft Security Blog, 2023.