

5-2023

Protecting the Infrastructure of Michigan: Analyzing and Understanding Internet Infrastructure

Samuel Blaser


Travis Munyer

Damian Ramirez

Lester Juarez

Jackson Servant

Follow this and additional works at: https://digitalcommons.unomaha.edu/university_honors_program

 Part of the [Data Storage Systems Commons](#), [Digital Communications and Networking Commons](#), and the [Hardware Systems Commons](#)

Please take our feedback survey at: https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE

Protecting the Infrastructure of Michigan

Gathering and Mapping Internet Infrastructure Information

Sam Blaser, Lester Palencia Juarez, Travis Munyer, Damian Ramirez, Jackson Servant

CYBR 4580-850 Greg Hoff

Michigan National Guard DCOE

Table of Contents

Table of Contents	1
Project Sponsor	2
Problem Statement	3
Research Focus	4
Information Not Available via Open Source	6
Meeting With CISA	7
QGIS Tool	8
QGIS User Guide	8
TraceRoute	12
TraceRoute User Guide	13
TraceRoute Data Center Recon (Web Hosts)	14
Hardening Infrastructure	16
Resources	20

Project Sponsor

The Michigan National Guard DCOE contacted the University of Nebraska Omaha to request assistance with collecting information on the internet infrastructure of Michigan. The direct project sponsor is First Lieutenant Andrew Scott. He has worked in coordination with Wade Watts to create the initial plan for the capstone project. First Lieutenant Andrew Scott has met with our team weekly to discuss project updates and plans. Andrew Scott also plans to share our project with his cybersecurity team to assist with overall training and knowledge on the infrastructure of the internet.

Problem Statement

The Michigan National Guard wishes to enhance their understanding of the physical, electrical, protocol, and logical topography of internet services. The capstone team will study, describe, and illustrate the infrastructure of the global internet to prepare hardening tactics, improve user training, and develop contingency plans in case of an attack or outage. Areas to research and study include finding where data lives, locating data centers in the region, identifying global infrastructure, infrastructure ownership, and potential for hardening.

Our goal for this semester is to set up the tooling and infrastructure to create and store the map data. Once this tooling is set up, we intend to focus on mapping regions local to Michigan, and to start mapping the major lines across the US. With the infrastructure set up, either the Michigan National Guard or future capstones can more easily focus on the actual map-making process.

Research Focus

In order to understand and map the infrastructure of Michigan's Internet, we first had to identify the most vital pieces of infrastructure. To gain a general understanding of the existing infrastructure we first found all available internet providers in Michigan. This step gave us a list of companies we could look into to find other pieces of infrastructure such as data centers and main data lines.

The bulk of our focus was on data centers in Michigan. Data Centers are one of the most vital pieces of the Internet infrastructure because they centralize an organization's IT and allow for the storage, processing, and dispersal of information. Data centers often hold an organization's most important information and processes, so they are vital to protect. In order to better understand the data centers that exist, we collected data about their power systems, network hardware, cooling systems, and existing security.

Power systems are vital because, without sustainable and protected power, data centers cannot remain operational. It is also important to understand if a data center has backup power, and the limitations of their backups. Network hardware information provides knowledge on the capabilities of a data center and information on any backup systems in place. Cooling systems are responsible for ensuring that the technology inside of a datacenter is kept at operational temperatures. Redundancies are often in place for cooling systems. Understanding the security systems in place at a data center is one of the most important pieces of information we sought out. Knowing that a data center is well protected can give the reassurance that information will not be stolen or taken easily. Most data centers have physical and cyber security. Most employ armed guards as well as restricted access via key cards. Another vital area to understand is the main internet lines that run through Michigan.

Internet lines can be hard to pin down, as there are so many in existence that a message from one computer to another may never take the same route twice. There are, however, main lines that most messages take somewhere along their trip. It is important to understand where these main lines are and how to protect them because they are a high value target to attackers. Using systems such as traceroute we can ping data centers to understand the typical routes that information would take to travel to and from the location. This can allow us to identify main lines throughout Michigan and can help to protect the transfer of information.

We also looked to areas near the border of Michigan, as most lines and information transfers are not bound by state borders. Understanding how threats around Michigan can impact the functionality of data centers and internet lines in the state is also important. Areas such as Chicago, Milwaukee, and Cleveland have a large amount of data centers and lines that intertwine with the infrastructure of Michigan. Understanding these major areas and the threats that could impact them can help to protect Michigan as well.

Information Not Available via Open Source

One of the areas we struggled to find information on the most was locating data and telephone lines on a local level. While the major lines that run through an area are available, we haven't found a source for information on internet provider lines that run through communities. This means we can only follow a general route the data takes from one location to another and are not able to follow the exact line. We also had struggles with finding data centers that are owned by major internet providers. Data center locations are available for data centers that allow individuals to purchase services. It is far more difficult to find the major internet provider data centers.

We also attempted to make contact with internet providers in the area to see if they were willing to give us any additional information. Much to our relief, they were not willing to hand out the information to just anyone. We tried convincing them we were capstone students, we told them we were working with the military, we tried convincing them we worked at their company, and many other techniques. We were told many times that they only give out the information to business inquiries and official businesses.

Meeting With CISA

One fulfilling and interesting opportunity the group got to participate in with the completion of this project was a video meeting with Cybersecurity & Infrastructure Security Agency (CISA) analysts. CISA is a government agency that, as defined in their mission statement, leads “the national effort to understand, manage, and reduce risk” for the country's physical and cyber infrastructure. Our meeting was led by Regional Analyst Jana Lamplota Chaudhri. Jana is a Region 5 analyst (which includes Michigan as a part of the region). Another notable member of our meeting was Kelley Goldblatt, who is the current CISA Cybersecurity Advisor for Michigan and Ohio. Within this meeting, we received a better overall understanding on a path to take in regards to how to complete the project, we gained new valuable web sources that we utilized throughout different phases of our project, and we gained new potential contacts if needed to help us with the completion of the project.

QGIS Tool

QGIS is a free, open-source, cross-platform desktop geographic information system (GIS) application that supports viewing, editing, printing, and analyzing geospatial data. The team used this tool to plot data center locations in Michigan and around Michigan. In addition, we added metadata of the data center's ID, Company, Address, Website, PowerSys, NetworkHW, Cooling, PhySec, Name, Notes, PhoneNum, City, and Region on the map in the QGIS tool. Lastly, we added a physical line representing the fiber network of the Peninsula Fiber Network company.

QGIS User Guide

Before using the QGIS tool, the user will have to download and install the software via the QGIS website. QGIS is available for Windows, MacOS, and Linux operating systems so

users must install the appropriate version of QGIS for their operating system, as well as follow installation instructions provided by the QGIS or their operating system to ensure a successful installation.

Downloading Github Repository

Our project is on a Github repository and can be downloaded to make updates in QGIS.

Download the QGIS project from the GitHub repository:

(<https://github.com/TravisMunyer/CYBRCCapstone-PhysicalInfrastructureMap>)

1. Visit the Github site and navigate to the repository that contains the QGIS project.
2. Click the “Code” button on the right side of the repository page and download the ZIP file.
3. Proceed to extract the ZIP file to the computer.

Opening the QGIS Project

After downloading the QGIS project from the GitHub repository, open the project using the following steps:

1. Open QGIS.
2. Click the “Open Project” button on the toolbar and navigate to the file location of the project.

Adding Data & Working with Layers

Before working with the data, a layer needs to be added to the QGIS project using the following steps:

1. Click on the “Add Layer” icon on the top toolbar.
2. Navigate through the drop-down menu and choose the preferred data type.

Our team has provided 2 different layers– DataCenters, and PhysicalLines layer. Each layer has a list of metadata called attributes which stores the information about each data center or physical line.

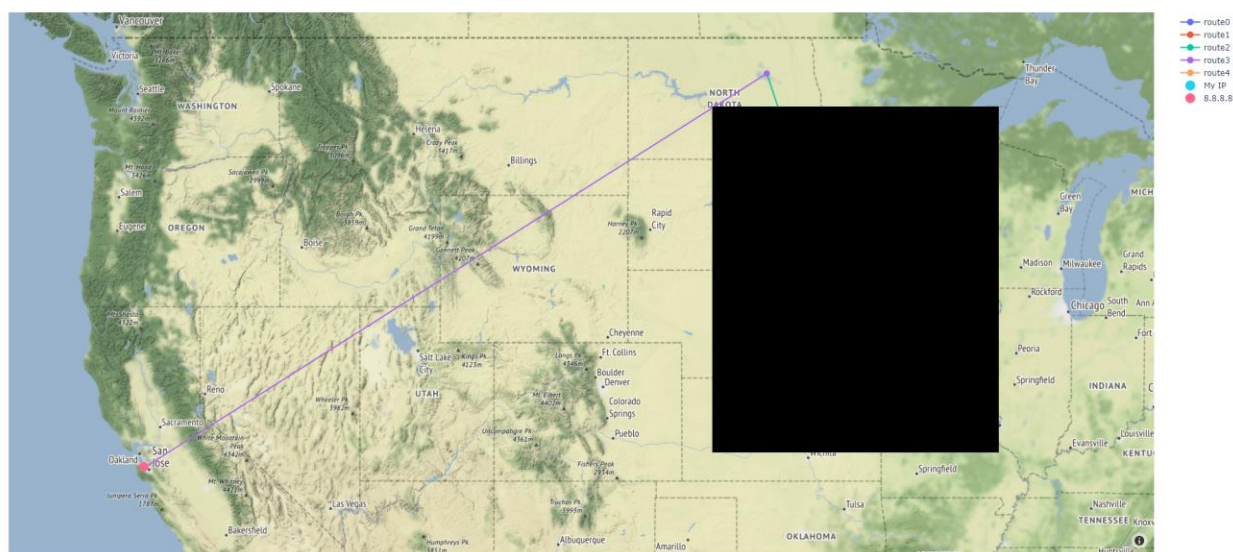
- Data Center Layer
 - id - Unique ID of the feature
 - Company - Name of the company that owns the data center
 - Address - The address of the data center
 - Website - Link to the data centers website
 - PowerSys - Description of the data centers power system
 - NetworkHw - Description of the data centers networking hardware
 - Cooling - Description of the data centers cooling system
 - PhysSec - Physical security mechanisms employed by the data center
 - Name - The name of the data center
 - Notes - Miscellaneous notes for the data center
 - PhoneNum - The data centers phone number (at the time of feature creation)
 - City - The city the data center is located in
 - Region - The region or state in which the data center is located

- Physical Line Layer
 - id - Unique ID of the feature
 - CableType - The material or type of the cable (e.g., fiber)

- Company - The company that owns the cable

TraceRoute

While a major part of this project focused on mapping the data centers, which is where data is stored at rest, Michigan National Guard also mentions interest in how data moves from one point to another. Mapping how data moves is a more difficult problem than mapping how data is stored at rest, however. Due to how the internet is implemented, the route data takes from one route to another may not always be consistent, as there may be some variations on the route. So, rather than create a static map of how data flows, we provide a tool that shows the route taken to a destination at one given time. To achieve this, we use a combination of the common traceroute operating system tool, which prints the ip addresses visited to reach a destination, and whois server queries. Whois is a protocol for querying databases that store registered users or assignees of an internet resource (e.g., ip addresses or domain names). The traceroute tool retrieves the ip address of interest, and the whois query obtains the information corresponding to the ip address. This information is then displayed on a map, which provides a visual of the physical route taken to a destination from the current ip address. An example of the map produced is shown below, with the first few steps redacted for privacy.



TraceRoute User Guide

- 1) Get a copy of the GitHub repository locally from the github here:

<https://github.com/TravisMunyer/traceroute-maps>

- 2) Download anaconda from here: <https://www.anaconda.com/>
- 3) Start up the anaconda prompt and navigate to the local github repository
- 4) Create a conda environment with python version 3.11

```
conda create -n TRoute python == 3.11
```

- 5) Install tool dependencies

```
pip install -r requirement.txt
```

- 6) Run the tool on a given ip address, hostname, or domain

```
python main.py [ip/hostname/domain]
```

Note: The tool used to collect information on addresses (ipapi) will occasionally lock you out after repeated use, as the traceroute tool uses the free tier of that ipapi. If the tool prints an error stating that information could not be found, then it is likely you are temporarily locked out of ipapi, and must wait until the lock is gone.

TraceRoute Data Center Recon (Web Hosts)

With the implementation of the traceroute tool we utilized during our research, we were able to determine different web hosts utilized by the data center websites. Determining the web hosts used by a data center's website could be valuable information for understanding the reliability of service for the data center. The ability to use the data center's site as a point of contact, as well as gain information on updates or changes being made to the data center does hold relevance in the terms of security and reliability. Now that we have identified the web hosts being used by the data center's websites using traceroute, the data can be used if there is ever an event or issue with the web host being used.

An example of how this process went for each data center website is displayed below.

For the data center website www.colomichigan.com traceroute displays:

```
C:\Users\jacks\Desktop\Capstone>python main.py www.colomichigan.com
1      1 ms      1 ms      1 ms      2600:8804:1324:d100:e6bf:faff:fe51:e4c3
2     39 ms     20 ms     10 ms     2600:8804:137f:ffff::1111
3      *        9 ms      *        2001:578:c00:7:f:0:5:8000
4     20 ms     35 ms     13 ms     2001:578:c00:4:5000::1a
5     20 ms     19 ms     20 ms     2001:578:1:0:172:17:249:64
6     21 ms     20 ms     20 ms     2400:cb00:14:3::8d65:49fb
7     24 ms     75 ms     20 ms     2400:cb00:14:3::
8     22 ms     19 ms     21 ms     2606:4700:3035::ac43:a2a3
2600:8804:1324:d100:b8b8:2462:6f66:a7f7 --- Omaha
104.21.15.131 --- Toronto
```

So, the returned IP address is 104.21.15.131

(Map below shows result returned by the above implemented traceroute)



After determining the returned IP Address, we then used the website *who.is* to determine the host returned from the IP address. Using the above IP address, *who.is* displays:

IP Whois		cache expires in 22 hours, 46 minutes and 41 seconds
NetRange:	104.16.0.0 - 104.31.255.255	
CIDR:	104.16.0.0/12	
NetName:	CLOUDFLARENET	
NetHandle:	NET-104-16-0-1	
Parent:	NET104 (NET-104-0-0-0)	
NetType:	Direct Allocation	
OriginAS:	AS13335	
Organization:	Cloudflare, Inc. (CLOUD14)	
RegDate:	2014-03-28	
Updated:	2021-05-26	
Comment:	All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse	
Ref:	https://rdap.arin.net/registry/ip/104.16.0.0	

who.is allows us to see that **Cloudflare, Inc.** is the web host for the **ColoMichigan** website.

Below is the list created while finding the IP addresses for the different web hosts associated with the data center websites located.

Data Center	Website	IP Address (Web hosting)
Liquid Web DCs	www.liquidweb.com	108.157.142.50 – Kansas City
Global Dataplex Lansing	N/A	N/A
Lumen Lansing	www.lumen.com	207.120.32.237 – Chicago
ColoMichigan DC1 - Southfield	www.colomichigan.com	104.21.15.131 – Toronto
Subrigo Corporation	www.subrigo.net	199.180.152.18 – Los Angeles
TelNet Worldwide partners with EdgeConnex	www.telnetww.com	141.193.213.11 – Austin
365 Data Centers	www.365datacenters.com	172.67.194.48 – Toronto
123NET Data Center	www.123.net	216.109.194.6 – Midland
Online Tech Westland(Otava)	www.otava.com	141.193.213.21 – Austin
SunGard Detroit	www.sungardas.com	199.60.103.225 – Cambridge
US Signal Grand Rapids South	www.ussignal.com	104.16.103.71 – Toronto
Switch SUPERNAP Pyramid Grand Rapids	www.switch.com	141.193.213.20 – Austin
US Signal Grand Rapids East	www.ussignal.com	104.16.103.71 – Toronto
Mid-Michigan Data Center	www.otava.com	141.193.213.21 – Austin

Hardening Infrastructure

The information that has been gathered can be used to help further protect the internet infrastructure of Michigan. Understanding the existing security of a datacenter can help to provide assurance that the information stored there is well protected, but there are other things that can be done to further protect the information and data.

Collecting information on contacts for each data center and internet provider can help the Michigan National Guard to establish a chain of contacts that can help to diagnose threats and problems. These contacts will have inside information and a better understanding of the systems they are protecting than any one person outside of the company, so their input can be invaluable in protecting infrastructure. These contacts also have the ability to contact other experts in their company to further expand the web of security for the Michigan National Guard. This leads to a rapid and effective response time when an incident does occur.

Having a rapid response time in the case of an incident is vital when it comes to protecting assets from attacks. Being able to quickly identify where the problem is occurring, who will be affected by the problem, and potential ways to stop the problem are vital pieces of information that the QGIS and GitHub data can assist in collecting. Along with providing information on who to contact when an incident occurs, the data collected will also allow for the Michigan National Guard to use their own maps and information to start building an incident mitigation and response strategy.

While having a response plan in place is necessary, it is important to also have proactive systems in place. With the data we have collected about the power systems, cooling, and security of each datacenter location, the Michigan National Guard's team of cyber experts can identify which datacenters may be at more risk than the others. This information will allow them to keep

a closer eye on these weaker sites as well as potentially working with the organization to improve their overall security.

Understanding what datacenters have vulnerabilities in their power systems, cooling, and security have can allow the Michigan National Guard to identify the threats before they occur. Power systems with insufficient backups or no backups at all are an easy target for attackers. One power is shut down to datacenters they become inoperable. This not only means that the information stored there is no longer accessible, but information that would pass through the datacenter no longer can.

This can stop vital communications, especially during a time of an attack. Ensuring that communication is available during a time of crisis is one of the most important things that protecting infrastructure can provide. A way to get around the problem of communication halting is establishing agreements and contracts between datacenter companies that will allow them to bypass information through each other instead of simply cutting off routes. The Michigan National Guard could assist with these steps by providing a trusted third party to assist in the storage and re-routing of information. Another threat area that can shut down the functionality of a data center is the cooling systems.

While having backups in place for power systems is vital to the functionality of a datacenter, cooling systems are equally as important. A lack of cooling systems will not only stop the datacenter from operating properly, but it could also lead to the destruction of equipment and data. If an attacker were to stop cooling systems from working, systems will begin to overheat within the datacenter. When systems overheat, it can lead to damage of internal hardware. This could cause data to be corrupted or even destroyed. This type of attack is especially dangerous because attackers may destroy all data stored at a datacenter, not just the

information they were after. This can cause widespread damage and can cause many organizations and companies to lose valuable information. Limiting physical access to the building that stores the data is also of high priority.

Having a reliable and up to date security system is vital to the protection of information stored at a physical location. Being able to understand the capabilities of the security systems in place at data centers allows the Michigan National Guard to understand what data centers are well protected and which ones are more at risk of a physical attack.

Understanding which sites are more at risk of attack will allow the Michigan National Guard to better prepare response plans. Having response plans set up with different companies will allow for the mitigation of data that is lost and faster deterrence of the threat. Rapid response is one of the most important parts of cybersecurity. The contact list for data centers and internet providers will also assist with the rapid response strategy. Being prepared for an attack is vital to stopping it quickly, and the Traceroute tool we have created allows the Michigan National Guard to create simulations of potential data routes that could be destroyed or rendered non-operational.

Using the Traceroute program, the Michigan National Guard will be able to simulate random data routes and create scenarios where the route has been compromised. This will create a realistic scenario and allow the cybersecurity teams conducting the simulation to understand what systems, data centers, and infrastructure would be affected by attacks. This could allow them to simulate damage and see how they could use the information we have collected to contact internet providers and help with data recovery and protection.

Using the tools and systems we have created the Michigan National Guard can work to proactively defend it's internet infrastructure. Using contact information for existing data centers and internet providers, understanding current data center facilities and capabilities, and the

traceroute tool will allow the Michigan National Guard to work along side other agencies to build a more safe and secure internet.

Resources

Data Center News, events and information. Baxtel. (n.d.). <https://baxtel.com/>

Grand Rapids Data Center: Michigan colocation. Switch. (2022, October 13).

<http://www.switch.com/grand-rapids>

Letter from the Executive director. Connect Michigan. (2023, May 12).

<https://connectednation.org/michigan/>

Merit. (n.d.). <http://www.merit.edu/network/>

PeeringDB. (n.d.). <http://www.PeeringDB.com/>

Link to Our Google Drive for Additional Information:

<https://drive.google.com/drive/folders/1X5nWQPBnefwn7rF8Z8xeBU5N1XfiVgHq?usp=sharing>