Using GIS to Explore Cyber Attacks and Natural Disasters in the U.S.

By Carson Buffalow, Graham School of Business, York College of Pennsylvania
Faculty Mentor: Dr. Jennifer Pomeroy, History & Political Science Dept.

Introduction & Background

Cyber attacks are considered as a top risk to a country, along with natural disasters. Being a cyber security major, once I saw the abilities of GIS systems, I wondered how I could use these systems and data analysis methods to benefit the world of cyber security. This research project used Geographic Information Systems (GIS) to map out the spatial distribution pattern of cyber attacks from 2016 through 2019 in the United States. This was done to understand any patterns and processes that would help cyber security analysts secure information systems better and help understanding disaster recovery.

Research Questions

1. What are the patterns regarding cyber threats in the U.S. from 2016-2019?
2. Are such patterns correlated to natural disasters such as tornado patterns and hurricanes? If so, how are they correlated?

Methodology and Data

GIS was used for data visualization to discern the underlying patterns and processes. Data used include (i) Cyber Attacks by Sector; (ii) Tornado Hotspots; and (iii) Hurricane Michael Path 2018. All datasets come from ArcGIS.com.

Study Area

The US is the study area and is also the third largest country in the world. It is a major mid latitudinally located country with a population of 328 million (Census). As shown on the map, the major surface water features are the Great Lakes and the Mississippi river system that is located in the low flat mid- west region. The Sierra Nevada in the west, the Rockies in the mid-mountain, and the Appalachians on the east raise the terrain to much higher elevations. The Tornado Alley refers to the Great Plains' low elevated sizable region. In addition to tornados, the Gulf states and the southeastern region are subject to annual hurricane season.

Figure 1
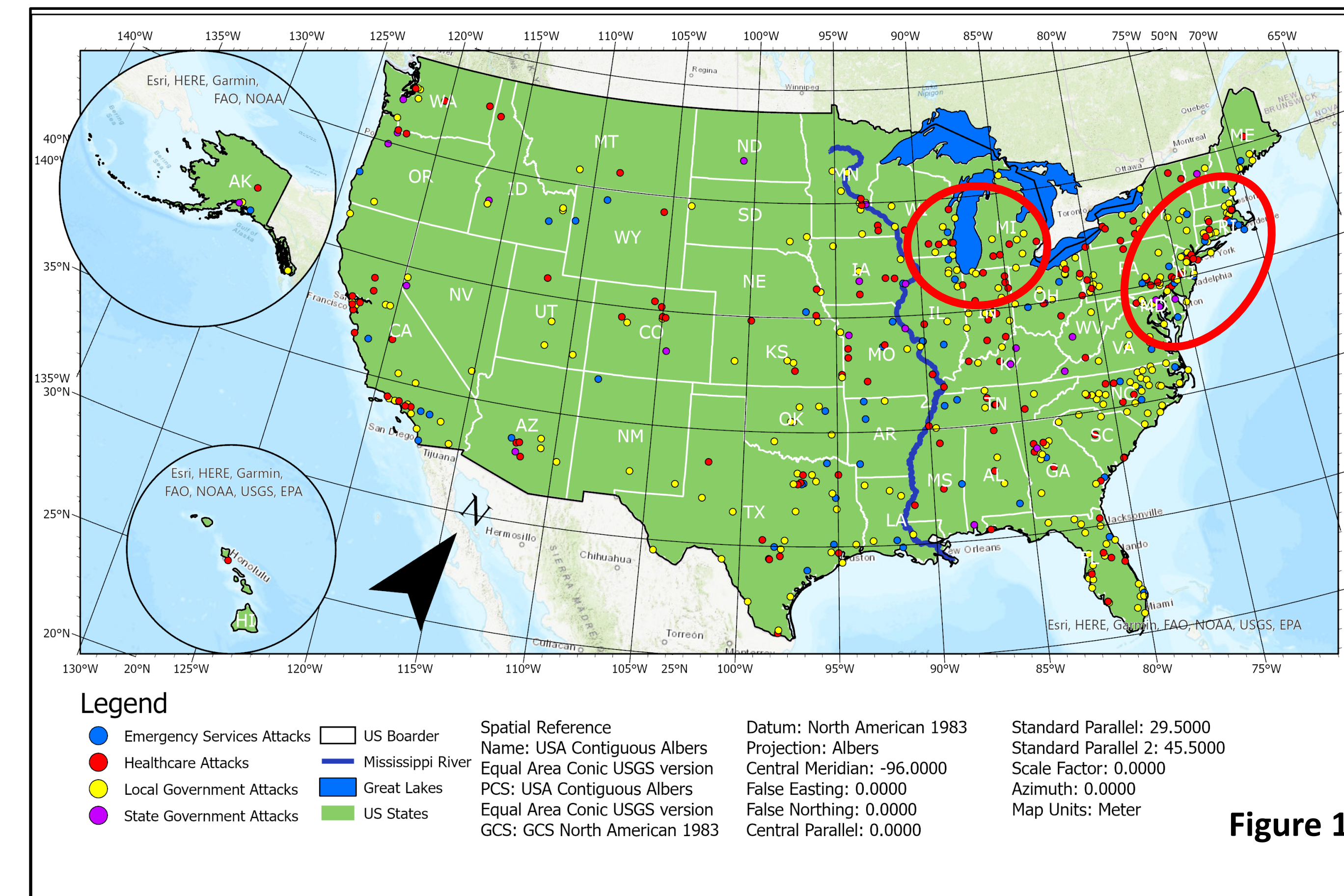
Figure 2

Figure 3

Mapping & Analysis

Figure 1 shows the spatial distribution pattern of all cyber attack events 2016-2019 by targeted sector. Of all sectors, 232 cyber attacks were launched on Local Government; next is Health sector with 172; then, Emergency Services at 87; the attacks launched on State Government sector was the last with 66. In terms of attack type, the most common attack types are ransomware and phishing which extensively targeted Local Government. Healthcare organizations also see a lot of ransomware and phishing style attacks as well. As shown, the BosWash Megalopolis is the spot of all cyber attacks for its highest density. The Chicago Urban Region is another hot spot, but slightly more dispersed. Figure 2 shows the cyber attack events were correlated to the tornado hot spots in the central part of the country. Local government is represented in yellow and emergency services in blue which are found on the brown colored areas which are hot spots with 90% confidence about the correlation.

In Figure 3 on which only Local Government received cyber attacks are visible, it confirms that cyber attacks correlate to natural disaster, in this case, hurricane Michael in 2018. By attack types, both ransomware and phishing were the major attack types. Those yellow points located right on the path of Hurricane Michael of 2018 confirms such correlation. Particularly vulnerable local government include the concentrated cluster in the northern FL, Georgia's Atlanta, Griffin, and Winder regions that are in high risk to cyber attacks.
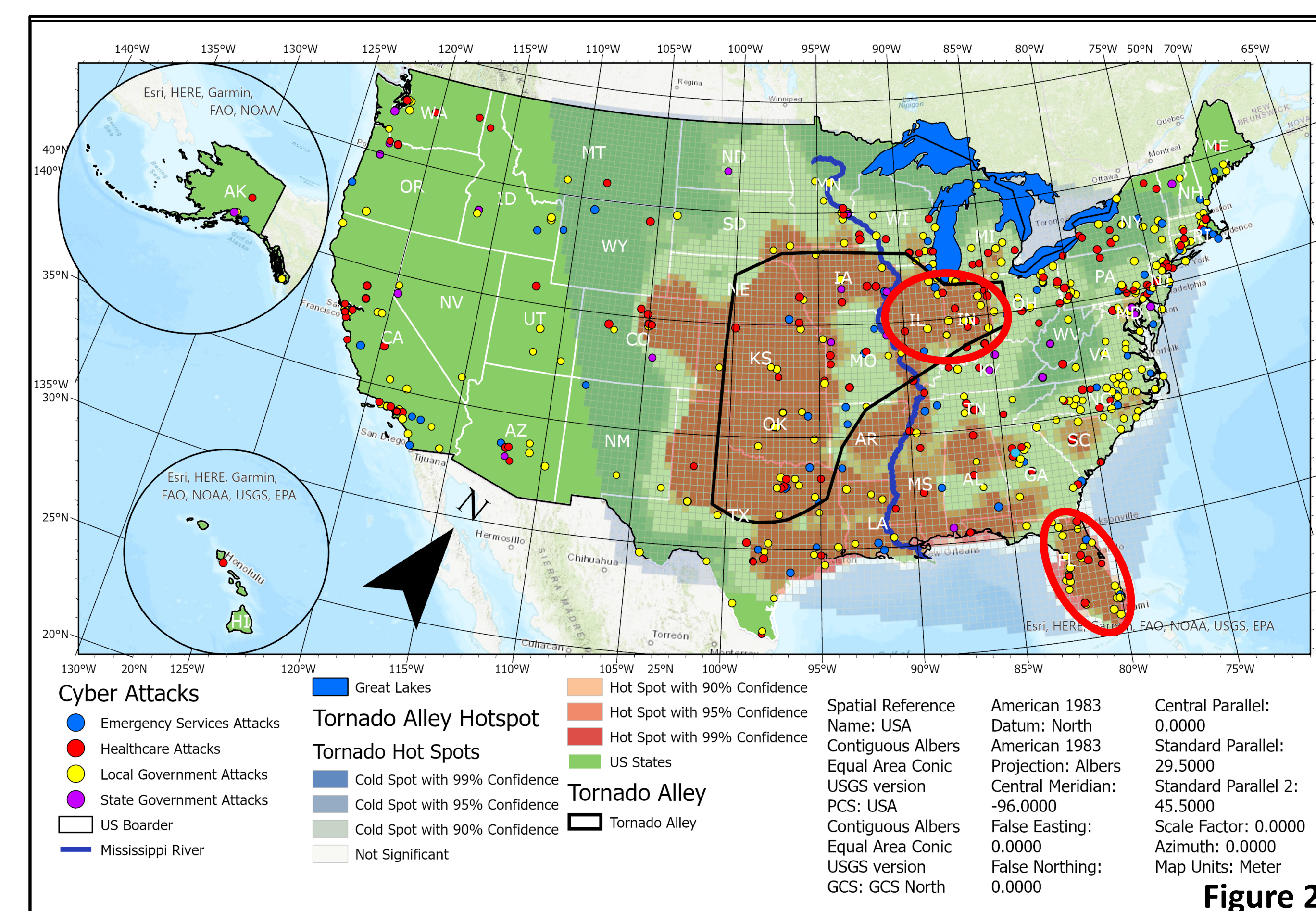
Conclusions & Future Directions

Cyber attacks from 2016-2019 were more concentrated in the east than west. The eastern seaboard and the southern tip of the Lake Superior experienced the densest attacks in all sectors. Cyber attacks are correlated to natural disaster events such as tornadoes and hurricanes. Future directions of this study would be assessing local government cyber security policy and assessing health and emergency sectors' preparedness in the natural disaster seasons.
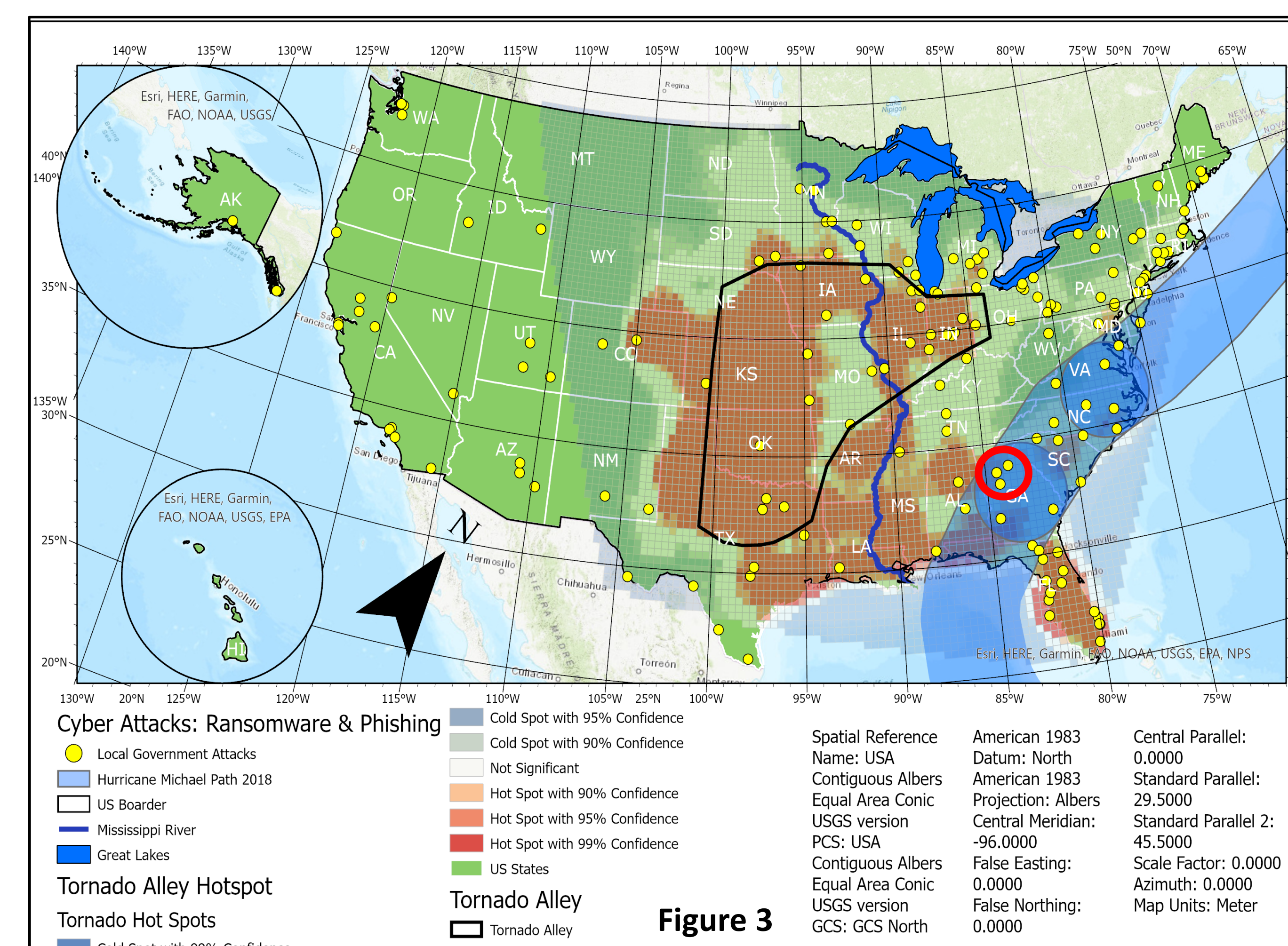
United States Department of Justice (USDOJ). (2019). *Department of Justice Reminds the Public to be Aware of Fraud When Disaster Strikes and Report it to the National Center for Disaster Fraud.* https://www.justice.gov/opa/pr/ Federal Communications Commission (FCC). (2020). *After Storms, Watch Out for Scams.* https://www.fcc.gov/consumers/guides/after-storms-watch-out-scams