CYBER-ATTACKS AND THEIR IMPLICATIONS FOR EMERGENCY MANAGEMENT

To the editor:

Emergency management has rightfully given attention to a variety of emergencies and disasters that have occurred throughout the United States over the past few years and months. Foremost among them is COVID-19, which underscores the need for improvements in public health preparedness and response. But the country has also been impacted by major hurricanes/tropical storms, damaging Derecho windstorms, devastating urban-wildland fires, significant floods, notable social unrest/riots, extreme winter temperatures and accompanying loss of electricity, and many other costly and deadly events including a disturbing building collapse in Surfside, Florida. This list is not comprehensive, of course. It excludes other concerns regarding rising social vulnerability, shortsighted development decisions, a degraded environment, and our inadequate and decaying infrastructure. It is understandable, therefore, that we are focused on the pressing issues of the day and needed changes in our policy priorities. Unfortunately, this may cause us to possibly overlook other potential risks.

A possible technological hazard that may not be sufficiently recognized is cyber-attacks—whether they emanate from hackers, activists, criminals, terrorists, or enemy nations.

The recent Colonial Pipeline incident is a visible example of the disruption that may be caused by such attacks. On May 7, 2021, nefarious foreign actors—with or without the knowledge and support of the Russian government—targeted the information technology systems of Colonial Pipeline, a company which is based in Alpharetta, Georgia. The digital attack affected the 5,500-mile pipeline running from Texas to New York, and it was disabled and shut down as a result. This situation created numerous complications for many states since roughly 45 percent of the East’s coast’s fuel was immobilized as a result. Thousands of gas stations quickly ran out of fuel and there were fears about the availability of heating oil and jet fuel. The daily activities of life were altered and even the stock market was impacted on a temporary basis. The stoppage lasted days and was only reversed once the CEO Colonial Pipeline paid the DarkSide group $4.4 million dollars in cryptocurrency.

The Colonial Pipeline incident was a serious wake up call for the nation. But it was not the first cyber-attack. Nor will it be the last.

Corporations, government leaders and national security agencies recognize this fact and are working feverishly to address this growing problem.

This brings up an important and consequential question for emergency management scholars and practitioners: should they also give attention to future cyber-attacks?

If cyber-attacks are deserving of a fully developed emergency management research agenda, possible questions for emergency management scholars and practitioners may include:

- How serious is the threat?
- Where are the attacks coming from?
- Who is launching these attacks?
- Why are they occurring?
- What are the potential targets?
- What physical consequences can be expected?
- What are the social impacts of these
events on the nation, communities, organizations, businesses, and individuals?

- To what extent can attacks be prevented?
- What changes in technology or processes will be required to reduce the threat?
- Should the nation prepare further for these types of attacks?
- What is the appropriate reaction to cyber-attacks? For instance, should ransoms be paid? What are the consequences of doing so? Could retaliation lead to a never ending tit-for-tat cyber war? How can everyday citizens, businesses, government leaders and multi-lateral partners successfully deal with this problem?
- How will people react to and in these types of intentional disasters?
- Are response and recovery operations for cyber-attacks similar or different than other disasters?
- What new partners should be engaged by emergency managers because of this apparent challenge?
- Are new organizations and plans needed?
- Should cyber-attacks be a priority for emergency managers?
- If so, how can emergency management professionals confront this problem without jeopardizing all of the other vast responsibilities the profession has already?
- What other questions must be considered in light of the threat of cyber-attacks?

These are not pleasant inquiries to consider and yet another hazard could distract us from our key mission. But, scholars and practitioners may need to explore them nonetheless. Cyber-attacks are not likely to dissipate anytime soon. In fact, they will likely pose an aggravated and vexing problem to our society for years and decades to come.

All of this suggests that emergency management will become an increasingly important profession. Once again, we must rise to the occasion.

Keywords: cyber-attacks, emergency management, planning

David A McEntire, PhD
Utah Valley University
Orem, Utah