FIU | Jack D. Gordon Institute for Public Policy

Policy Position Paper

December 2024

Artificial Intelligence and Critical Infrastructure: The Advent of the Future

Dr. Ratna Okhai

Summary

Artificial Intelligence (AI) and its impacts on cybersecurity has been a growing concern around the world, as increasing reliance on technology to support our advancements has created a space for a race to be better no matter the cost. In the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) has delineated processes to help guide how we prepare for, respond to and recover from these threats. This is the same in Florida, where we host critical infrastructures (CIs) that have the potential to be impacted (e.g., 21 military bases, 3 nuclear power plants, 67 counties' buildings). However, we are still at a disadvantage when it comes to the *why*. Why do we need concentrated efforts to address this issue? The reasoning is simple: It has the potential to derail entire nations. More specifically, it can derail our critical infrastructures. Critical infrastructure is a gold mine for cyber-threats due to the inherent value of information it holds, therefore its innate vulnerability and potential to lead to widespread harm and panic.[1] (Figure 1 identifies full list of these CI's). A comprehensive review of literature has highlighted the urgent need to develop guidelines that will protect from cyberattacks that are strengthened through AI. The State of Florida needs to leverage this extensive discussion surrounding this topic of AI and its impact on our critical infrastructure and follow suit of other states that have already proceeded with state-level legislation and regulations to better protect our critical infrastructure and citizens.

Background and Overview

Critical infrastructure has three major components for consideration, as it relates to cybersecurity, and the future of AI. First, a large part of cybersecurity has been thus far focused on responding to and recovering from breaches. As AI seamlessly becomes an innate part of our existing technologies (e.g., cars, phones, internet searches), we must look to ensuring our policies and practices are proactive rather than reactive. A large part of this integration of AI in cybersecurity will be to understand how the hosting hardware systems operate, the vulnerabilities exposed, and how to minimize them. According to the National conference of State Legislatures, at least 40 states across the U.S. and Puerto Rico have already begun to address this issue, whether it's through state-sponsored agencies created for cybersecurity, passing of legislation, or even incentivizing research and education programs for our future generations.

Second, smart cities are the future of the world, with increased connectivity, intelligence systems that can enhance efficiencies of how we run our communities, and machine learning capabilities that can promote better practices. However, these new age cities come with cybersecurity risks that are augmented with AI. For instance, with the number of remote workers increasing, we see an increased number of sensitive data more compromised. In December 2023, U.S. authorities intercepted an attempt by foreign actors to

[1] Critical Infrastructure sectors as defined by CISA: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors/Materials, Transportation Systems, Water/Wastewater.

infiltrate home routers, which was intended to target critical infrastructure (DOJ report). Preemptive efforts of governmental and private sector partnerships intercepted this attempt, but our expected and growing reliance on technology should be reflected with these cautions in mind. As the State of Florida sees a growing number of cities vying for this 'smart city' designation, the State needs to play a supportive role to ensure that critical infrastructure in these cities are insulated from such attempts.

Third, disaster response is something the State of Florida runs like a well-oiled machine. Adding to that the vulnerability of critical infrastructures could potentially derail this. This includes facets such as data breaches, system shutdowns and physical damage that hinder the ability to prepare, mitigate or respond effectively. Additionally, it includes the preemption or interception of any software-attacking programs (such as the one intercepted by DOJ last December). While many of the critical infrastructure sectors are prone to more secure systems, the symbiosis effect on each other must be emphasized to encourage more stringent training, detection and safety measures.

Impact

We believe that the State of Florida needs to place an emphasis on these three elements with the following:

1. Better understanding of hardware and software through funding of more secure hardware (and opportunities that engage this). We posit that partnering with universities that have subject matter expertise and centers that are already doing the work could address this. There are a significant number of Florida scholars that have already been at the forefront of this research to better understand protective measures we should take - leveraging and supporting their efforts will expedite the State's capabilities and efforts.

2. Engage universities to provide curricula that teach students about the unique nature of our critical infrastructure and potential threats that exist to them. The next generation of workers need to be able to utilize AI in their daily lives; more specifically, teaching about how potential critical infrastructure systems could be targeted can engage better prevention practices. Additionally, AI curricula should be focused on not just educating, but how to utilize it for the benefit and safety of our existing systems, and how to build AI capabilities to protect them.

3. Engage in discussions and invest in building standardized safety protocols for hardware hosting critical infrastructure systems and software that can protect existing systems. Utilize CISA's guidance for a framework, but then build a repository in Florida, engaging those critical infrastructures that have been attacked, so that better preparation measures can be built from experiences and best practices.

4. Regulate minimum safety requirements of critical infrastructure sectors because mandated compliance will ensure less vulnerability.

5. Build and maintain a list of critical infrastructures around the state, with a confidential host agency for this information. This encourages the repository, and more communication and contact with municipalities that host these infrastructures, to engage in standards' compliance for cybersecurity safety.

6. Engage critical infrastructure sectors to be connected to their municipalities through training and engagement. This aligns with encouraging preemptive safety measures in city ordinances that host critical infrastructure as they expand their technological footprint in the State and in Florida municipalities. This should also include requirements for more regular communication between municipalities and the State to reduce the likelihood of cyberattack through the use of

AI.

7. Leverage Florida's Department of Emergency Support Function #20. The State's active support of municipal efforts to strengthen their organizations from cyberattacks (through resources, grant funding, best practices) is beneficial to the State in the end, as cyber attacks on governments can have ripple effects. For those critical infrastructure that are private, the State should build in requirements for their policies to include "in the event of a disaster" plan, should they wish to utilize or leverage any State resources in the event of a cyberattack.

Impact

The primary impact of these measures is to have a state that is protected from having sensitive information leaked, protection from detrimental effect on the economy, or at its worst, potential for a much larger attack. As noted in the introduction, Florida hosts numerous critical infrastructures across the State, ranging from government agencies to those within military/nuclear capabilities. While there are sectors that have already emphasized fortification of their critical infrastructure, cybersecurity requires considerable adaptability, and constant updating. By engaging in the formalization of policies and preventative measures, the State of Florida has an opportunity to set a positive example for other states, and from an economic perspective, provide evidence for industries that want to bring their business to our state. Being able to showcase that our critical infrastructures are in active management and aware of cybersecurity measures has a positive long-term impact in this regard.

Author

Dr. Ratna Okhai is an Assistant Professor in the School of Public Affairs, University of South Florida, Tampa, Florida

Disclaimer