International Journal of Innovative Research in Education, Technology & Social Strategies
p-ISSN: 2465-7298 | e-ISSN: 2467-8163
Volume 10, Number 2 November, 2023
IJIRETSS

How the White House's AI Executive Order Could Increase U.S. Cyber Vulnerabilities

John Villasenor
Governance Studies, Center for Technology Innovation
Brooking Institution, Washington, D.C., United States

Article DOI: 10.48028/iiprds/ijiretss.v10.i2.12

Abstract

On October 30, the White House released its "Executive Order" on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." It is a lengthy document, spanning over 30 pages in the Federal Register. But two short portions of the Executive Order (EO) are of particular concern in terms of the cybersecurity vulnerabilities they will create: Under the EO, the government will institute mandatory reporting of information about the "physical and cybersecurity measures taken to protect" model weights associated with certain large AI models, as well as the location and computing power of "large-scale computing cluster(s)."

Keywords: W*hite house, AI, Cyber vulnerabilities*

Corresponding Author: John Villasenor

First Published: https://www.brookings.edu/articles/how-the-white-houses-ai-executive-order-could-increase-u-s-cyber-vulnerabilities/

Background to the Study

Cybersecurity Exposures

The very fact of requiring AI companies to report the "physical and cybersecurity measures taken to protect" model weights will itself undermine the utility of those measures. After all, one of the most basic principles of security is to avoid disclosing too many details of how an asset is protected. A well-protected jewelry store is secure in large part because would-be thieves are left guessing as to the full set of security measures that are in place. The most sophisticated AI models are the result of enormous investments in both dollars and human effort. Those models have extraordinary economic value and are therefore ripe targets for state-sponsored economic espionage. A U.S. government database describing the measures taken to secure those models will itself become a target for cyberattacks, as the information it contains can help provide a roadmap for people intending to hack into the computers storing the AI model information.

Another concern is exposure to cyberwarfare. Under the EO, the government will collect information from "[companies, individuals, or other organizations" regarding the "existence and location" and "the amount of total computing power" in reportable computing clusters. That information would be highly valuable for a geopolitical adversary planning to launch a large-scale cyberattack aimed at disabling American computing infrastructure. To maximize its options, a potential adversary will try to preemptively exfiltrate the information from the government's computing cluster database, as that information provides a target list for a future cyberattack.

One response to these concerns might be to argue that, knowing the economic and strategic value of this information, the government will succeed in protecting it accordingly. Unfortunately, history gives reason to be skeptical. In the mid-2010s, a nation-state was reportedly able to breach the computers of the Office of Personnel Management, making off with the information on tens of millions of people. A New York Times article at the time reported that "every person given a government background check for the last 15 years was probably affected".

To be clear, the government workers in charge of government computing systems do their best to secure them. But they are often hamstrung by a combination of antiquated technology, inadequate cybersecurity budgets, and the need to rely on insufficiently secure third-party tools and systems. The broader lessen is that government entities are not always good custodians of large computer databases of sensitive information. Of course, some government entities need to maintain such databases in order to execute their duties. The IRS, for example, needs to collect tax reporting information, and state motor vehicle departments need to collect information about licensed drivers. But there is no inherent need for the U.S. government to build databases of detailed information about privately held computing assets and AI models. It is worth asking whether the purported AI governance policy benefits accruing from the reporting are more than outweighed by the resulting cybersecurity risks.

Recommendation/Conclusion

The Department of Commerce should formulate the associated rules with the expectation that the reported information will be exfiltrated by nation-states seeking economic and geopolitical strategic gains. This means that it should be sufficient to report information that is highly generalized in nature, thereby providing fewer details that, once exfiltrated, could be used to inform potential adversaries about how to conduct cyberattacks.

It will also be important to ensure that the reporting obligation itself doesn't impede AI innovation. As noted earlier, the EO provides initial criteria (subject to modification by the Department of Commerce) that "any model that was trained using a quantity of computing power greater than 10 integer or floating-point operations" must be reported. But how is the total number of operations counted? If a company does five test training runs of an AI system before doing a final training run, should it count the total operations in all six training runs or only in the final one?

If the reporting requirements are too onerous, fewer U.S. companies will choose to develop innovations in the advanced AI models and systems that have such promise. Instead, that innovation will occur outside the U.S. The upshot is that while AI is rightly a key focus in current policymaking discussions, it is critical to ensure that AI governance frameworks are designed in light not of only potential AI harms, but also in view of the broader context of U.S. national security and global economic competitiveness.

References

https://www.brookings.edu/articles/how-the-white-houses-ai-executive-order-could-increase-u-s-cyber-vulnerabilities/