Forum for American Leadership

AI is Critical for Cyber Defense

October 19, 2023

ChatGPT and other forms of generative artificial intelligence have reinvigorated policy conversations about the future of AI and how the technology should be regulated as it enters the mainstream.

The large language models that underpin tools like ChatGPT represent a class of AI known as generative AI—because they ingest large datasets and hundreds of billions of parameters to generate new content. This content generation has limitless potential for societal benefit from diagnosing diseases to detecting fraud in the financial system. Malicious actors can also leverage it for nefarious purposes. Cybersecurity leaders across government and industry have expressed concern about generative AI being leveraged to create malware, enhance the scale and sophistication of attacks, and make social engineering schemes—like phishing emails—more believable.

Recognizing these divergent forces, nascent AI policy debates have focused heavily on "risk," particularly the risks that AI systems can have on individuals. However, any discussion of the risks associated with AI must also consider the risks of not deploying these tools, where restrictive approaches could impact the security of the very individuals we aim to protect. Cyber defense is one of these arenas—where it is more risky for society to *not* deploy AI-enabled tools.

Network defenders leverage large amounts of security data—malicious IP addresses, vulnerability information, and other telemetry—to spot malign activity in real time and to automate response and remediation activity. Maximizing AI/machine learning and in-line learning for this critical cyber defense activity will inevitably support both national security and privacy imperatives, as both of these interests cannot be served until the systems upon which they operate are secure. Deploying the most up-to-date and capable tools to protect the nation is exactly what the American people should expect, and there is an obligation to leverage the relentless American innovation in the AI space to stay ahead of increasingly emboldened cyber adversaries.

The benefits of AI-powered cyber defense are far from hypothetical. For years, the cybersecurity industry has been successfully deploying a range of AI and ML tools. These include AI-driven malware detection, inline ML to stop never-before-seen "zero day" attacks, AI-driven anti-phishing tools, and ML-backed asset discovery and cataloging across the public-facing internet.

Looking forward, large language models like ChatGPT, which have seen widespread public availability and adoption as a low-cost and accessible generative AI tool, could make it even more difficult to defend networks and systems from AI-driven attacks, as these tools may empower less sophisticated threat actors to scale their attacks. This new reality places heightened importance on leveraging AI for *defensive* cyber purposes.

Recommendations

Congress and the Executive Branch find themselves at a critical moment when it comes to AI policy. There's an opportunity to assess international trends in AI policy space—especially

Europe's demonstrated eagerness to regulate AI—and evaluate where these existing actions are helpful and where they are counterproductive. From there, U.S. policymakers can more surgically pull domestic policy levers by aligning regulation to areas where these AI tools present actual risks to individual rights versus use cases where these tools may instead be essential elements of our comprehensive security posture.

- **Prioritizing that deliberative approach now will minimize unintended consequences in the future.** For example, in the EU Artificial Intelligence Act, broad sectors and capabilities are characterized as high-risk, with proposals to even further expand this categorization to include more general purpose AI systems. This unbalanced approach that focuses on just one side of the risk equation. Alternatively, we are encouraged to see the flexible, adaptable, and risk-based parameters included in the NIST AI Risk Management Framework. That is a more reasonable piece of AI doctrine to build upon.

- **Cyber defense use cases demand dedicated policy protection**. As several U.S. legislative proposals consider algorithmic design review requirements, we urge lawmakers to avoid unintended consequences that will negatively impact national security. We must carefully evaluate use cases like defensive cybersecurity much in the same way network cybersecurity can be considered a permissible purpose for processing personal information under various privacy frameworks. Cybersecurity is ultimately an enabler of privacy, and AI will increasingly become an essential element of cybersecurity defense. Recognizing this interdependency under the terms of any proposed legislation would not undermine or undercut the protections offered to individuals but only help secure those interests.

- **Recent precedent for legislation to explicitly encourage the deployment of AI-powered cybersecurity capability.** The EU's Network and Information Security (NIS2) Directive, which is currently being implemented through the member state regulatory process, includes the following article: "Member States should encourage the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks, enabling resources to be diverted towards cyberattacks more effectively."

Cyber adversaries just need to be right once to wreak havoc. This represents a fundamental challenge for network defenders—with sprawling digital infrastructure, being "pretty good" at cybersecurity simply isn't good enough. AI-backed automation, both for visibility and response, helps solve this misalignment. Our cyber defenses need more AI, not less. We urge policymakers to recognize this reality now before we see unintended consequences of these policies.

This paper is a product of FAL's Technology and National Security Innovation Working Group.
