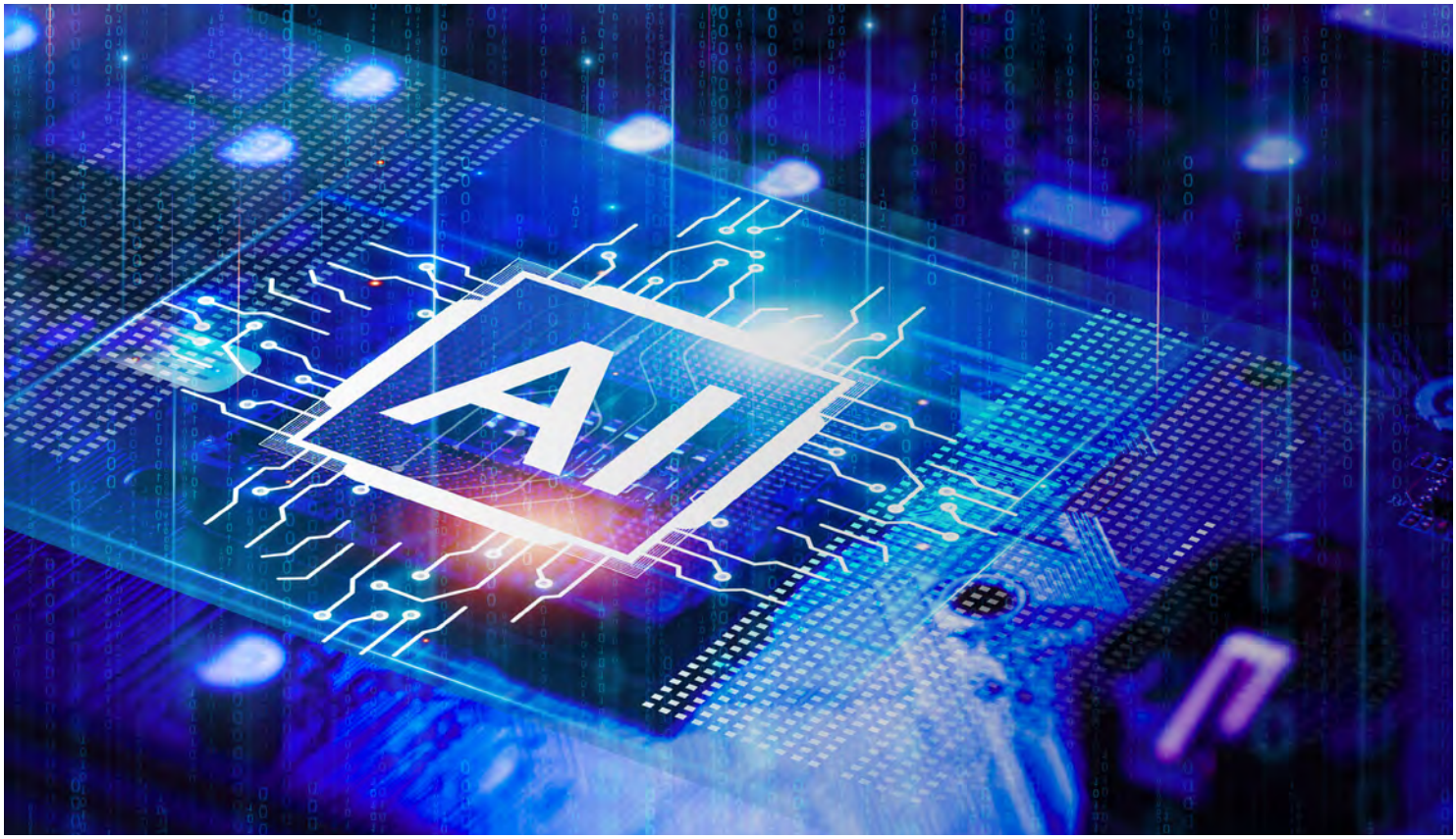
Nation-State Activity in the Age of Artificial Intelligence and Quantum Computing

Editor's Note: This article was originally published in *Domestic Preparedness Journal*, February 2024, Volume 20, Issue 2. Reprinted with permission from the Domestic Preparedness Journal https://www.domesticpreparedness.com/articles/nation-state-activity-in-the-age-of-artificial-intelligence-and-quantum-computing.

By Margaret Graves



Seldom has there been a simultaneous evolution of two powerful and complementary technologies—artificial intelligence (AI) and quantum computing (QC).

AI refers to machines programmed to mimic human intelligence. These systems use algorithms to analyze data, recognize patterns, and make decisions. Generative AI is a subset of AI that creates new content from learned data. It generates original material across various mediums (text, images, audio, etc.). Traditional AI analyzes existing data, but generative AI goes beyond by generating new content.

QC involves specialized technology, including computer hardware and algorithms, that harnesses the unique properties of quantum mechanics. Unlike classical computers or supercomputers, quantum computers can solve problems that are either impossible for classical machines to solve or would take an impractical amount of time.

Nation states are in a race to harness the power of these technologies for social good, economic advantage and growth, geopolitical influence, and cybersecurity. Many countries, whether allies or enemies, are investing in AI and QC capabilities and highlighting the adoption and use of these technologies in policies, legislation, and strategic imperatives.

"Staying abreast of the evolving landscape and remaining vigilant will ensure that organizations protect against unintended consequences and take the right pathway into the future."

Margaret Graves, Senior Fellow with the IBM Center for The Business of Government.

For example, in 2015, China published its "Made-in-China" strategy, which states the strategic objective of becoming dominant in specific technology markets, including AI and machine learning, the Internet of Things, and chip manufacturing. The U.S. and its allies have considered this objective to be a threat not only to economic growth but also to national security. The U.S. has responded by using trade policy to limit the incorporation of products from China and other unfriendly nation states in the national technology ecosystem.

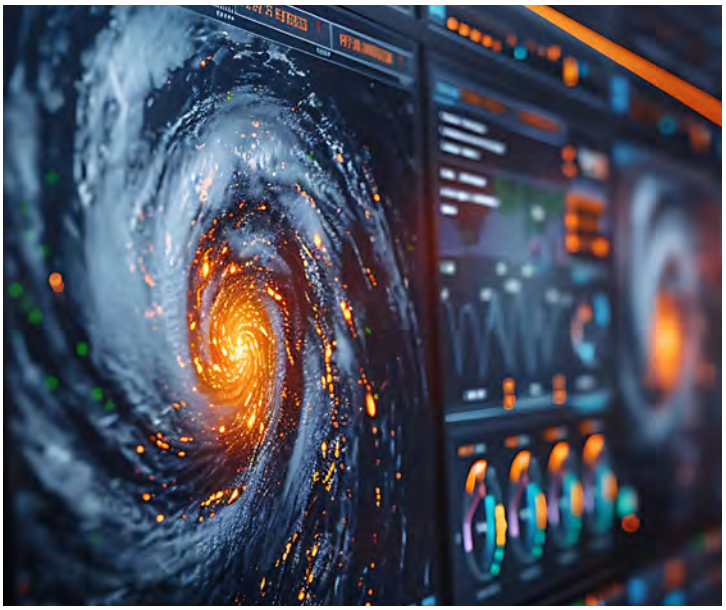
The CHIPS Act legislation addresses some of these challenges by offering approaches to reduce supply chain risk and investing in AI and QC technologies to increase the country's competitive edge. There also is an emphasis on strengthening the protection of intellectual property created in research and development centers. Aside from these measures, significant policies solidify the importance of effective adoption, appropriate use, and vigilant cyber protection of AI technology, as evidenced by a comprehensive executive order.

Benefits of AI and QC

AI and QC offer significant benefits for executing private-sector business and government missions. The combination of AI and QC gives companies and governments the ability to curate large amounts of unstructured data, find the "signal in the noise," and perform pattern recognition in such rapid computational timeframes that the outputs from the algorithmic analyses can help make strategic and operational decisions in real-time. In addition to providing powerful analytic support for decisions, AI and QC also offer organizations the ability to use predictive analytics to continuously improve resilience, especially during a crisis. A few of the most powerful use cases include:

Medical research—AI and QC can assist in medical diagnostics for rare or critical illnesses, biomedical and genetic research, and pharmaceutical development. During the first phases of the COVID-19 pandemic, the Organization for Economic Cooperation and Development (OECD) tracked and published on its website the use of AI in addressing the crisis. More recently, the Cleveland Clinic has deployed a QC capability, the first of its kind solely dedicated to biomedical research.

- **Climate resiliency and emergency preparedness**—According to the National Oceanic and Atmospheric Administration (NOAA) Center for Artificial Intelligence (NCAI) website, "NOAA has a long history of using AI in weather forecasting, climate modeling, and environmental monitoring," and the NCAI is its "conduit for artificial intelligence and machine learning for mission science initiatives." The Federal Emergency Management Agency (FEMA) is using AI to conduct geospatial damage assessments after a natural disaster relief suppliers of goods and services use AI to optimize their supply chain and transportation networks to ensure rapid delivery.



- **Fraud risk reduction**—AI can identify patterns of fraud in benefit transactions. The Department of Health and Human Services uses AI to identify fraudulent pharmaceuticals and Medicare or Medicaid fraud. FEMA is using AI to identify fraudulent disaster relief applications.
- **Cybersecurity**—AI can enhance the effectiveness of cybersecurity operations and defense by identifying attack patterns, recognizing anomalous activity, performing predictive risk analysis that can help expand defenses and train cyber defenders, and automating a matching response based on defense approaches that have worked against past cyberattacks.

Dual-Use Technologies

Unfortunately, knowledge of these technologies leads to a point-counterpoint argument in which each capability that can be used for good can also be used by criminals or nation-state actors for nefarious purposes. Nowhere is this point-counterpoint phenomenon more evident than in the national security realm. For example, there is understandable excitement about the ability of AI to accelerate and enhance the development of valuable computer code. However, at the same time, an attacker could use this capability to create stronger self-healing malware in which multiple strains of malware are fed to an algorithm, thus creating strains that are harder to detect. This malware could subsequently be used in disruption or exfiltration of sensitive national security data.

Another risk arises by the very nature of AI's fundamental principles. AI uses massive amounts of data to feed machine learning. Having such a large amount of data in one system could present an attractive attack surface to adversaries. Designing and building these systems with that risk in mind is imperative. Generative AI also poses an emerging threat as it enables adversaries to create more dangerous phishing attacks by creating emails that are convincing in their content. Finally, developing deep fake identities provides an opportunity to create civil unrest and influence political outcomes.

Protective Steps That Organizations Should Take

Organizations should define practical steps that private- or public-sector organizations can take to ensure they derive the most good from these technologies while protecting their vulnerabilities. To that end, in the 2022-23 timeframe, the National Academy of Public Administration and the IBM Center for The Business of Government conducted a series of roundtables with eminent executives from government, industry, and academia to openly discuss strategies for improving nation-state government resiliency in the face of "future shocks" in the areas of emergency management, cybersecurity, supply chain, climate resilience, and workforce development. These roundtables helped produce individual reports, a compendium, and a book with recommended actions for executives. These publications were released in November of 2023 and are referenced in this article.

Several reports indicated that thoughtful implementation and appropriate use of AI and QC can bring tremendous benefits. However, those implementations must be underpinned by a structure that at least recognizes the importance of the following elements:

- Governance structure – There should be recognition that AI and cybersecurity are risk factors to include in C-suite discussions. They are not simply technology issues. The appropriate implementation of AI includes ensuring that it is comprehensive, inclusive, unbiased, and secure. Proper use is the responsibility of the highest level of the organization.
- AI literacy and workforce development – All levels of the organization should know how to leverage these technologies to improve the mission and what risks they present. Role-based training is critical, from C-suite executives to practitioners.
- Public, private, and academic partnerships – There should be a constant exchange of information regarding the risk and threat landscape, successful use cases and implementations, and evolving research and development.
- Investment in innovation and transformation – Chief information officers, chief data officers, and AI executives must work together to address all elements of quality AI implementations, including infrastructure, tools, and data strategies supporting mission- or business-driven use cases.

Conclusion

Using AI and QC for business and mission results presents promise and peril. Critical missions such as national defense and public health and safety will benefit from real-time enhanced situational awareness and the ability to optimize predictive analysis, defense, response, and recovery. Additional benefits include the support of fair trade and commerce by creating economic stability in global markets to reduce the possibility of geopolitical destabilization. A business result is providing services to the population that are delivered in a more transparent and accelerated fashion, thereby enhancing the customer experience. Staying abreast of the evolving landscape and remaining vigilant will ensure that organizations protect against unintended consequences and take the right pathway into the future.