Envisioning the Future of Government

How Emerging, Secure Technologies and Data Flows Can Enable Anticipation and Action that Improve Performance

Editor's note: Adapted from chapter 14 in *Anticipatory Governance: Shaping a Responsible Future*, edited by Melodena Stevens et al, World Scientific Publishing, forthcoming.

By Daniel Chenok

How can governments secure implementation of advanced technologies and enable government to use data to make more informed decisions, promote transparency, and improve outcomes in an increasingly complex and uncertain world?

This article draws on recent publications and other IBM Center research to demonstrate how secure implementation of advanced technologies, such as cloud computing, artificial intelligence (AI), and quantum computing, can enable government to use data to make more informed decisions, promote transparency, and improve outcomes in an increasingly complex and uncertain world. Such capabilities support greater transparency through which the public can understand and engage with government, and ultimately increase performance and public trust.

Key Technologies: Cloud, AI, and Quantum Computing

Public and private organizations are moving through a significant period of inflexion given the rapid evolution of a suite of technologies. Artificial intelligence, and more recently generative AI and the development of initial quantum capabilities, all gain strength when building on a foundation of cross-boundary networking enabled by cloud platforms. Implemented properly, these technologies can transform how people work. Each of these emerging intelligent technologies offers a set of capabilities that can enable government to improve anticipatory governance and resilience in the face of change.

"By leveraging innovation responsibly, governments can act with agility to anticipate the future and make choices that best serve the public."

Daniel Chenok, Executive Director, IBM Center for The Business of Government.

Cloud Computing

Cloud computing has long been defined by the U.S. National Institute of Standards and Technologies[1] (NIST) as "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Agencies can adopt secure, scalable cloud solutions to transform government operations and deliver effective digital public services. Cloud networks can provide the building blocks for technology-enabled service improvement in agencies anticipating and addressing a wide range of issues, including weather prediction, agricultural development, veterans benefits, emergency management, federal personnel, and national defense.

Three stages of cloud computing can strengthen agency capabilities:[2]

Stage 1: Cloud infrastructure for mission-specific needs: In this first stage, early adopters and innovators within subagencies and offices independently move to the cloud to support their mission-specific needs.

Stage 2: Agencywide cloud enablement: To handle everyday essential processes like billing, data-sharing and collaboration, agencies often move towards centralized platforms, applications and infrastructure, in a process known as cloud enablement.

Stage 3: Cloud technology for future transformation: The stability and security provided by cloud services and business-oriented solutions allow agency innovators to focus their efforts on developing more ambitious programs and ideas.

In moving through these stages, governments should strengthen cloud networks against security threats, and operate cloud networks to optimize planning and performance.

Cloud Security. Threats to federal data, software applications, and digital infrastructure, including cloud-based technologies, are growing exponentially. NIST reports on new cyber vulnerabilities daily[3] that, if unaddressed, could result in large-scale security breaches that can weaken government resilience. To safeguard the systems and services agencies rely on to serve the public, government must adopt a security-first mindset, maintain a responsive, agile approach, and implement cybersecurity best practices.

Cloud Optimization. As agencies implement best practices to maintain accountability while exploring and expanding cloud use, they can implement multiple strategies:

- **Build cloud financial operations into cloud planning:** Cloud migration projects, like any complex IT initiatives, can experience excess costs and time lags. Agencies can track their cloud usage and spending so that cloud operating decisions are data-driven and outcomes-based.
- **Develop flexible and scalable partnerships with an ecosystem of mission-aligned cloud service providers:** Pay-as-you-use cloud computing, runs counter to the annual and often multiyear government budgeting cycles. Agencies can strengthen resilience through multi-cloud ecosystems that leverage diverse services and platforms.
- **Account for ROI:** Agencies can quantify the dollar value of migrating workloads to the cloud for transparency and accountability.

Artificial Intelligence

The advent of artificial intelligence has moved rapidly in government. As agency use of AI evolves, leaders will look for pathways to capitalize on opportunities, and the workforce will need new technical and social skills to assess AI-based data for improved anticipatory governance and decision making.

More specifically, AI could enable agencies to fulfill numerous roles efficiently and effectively by reducing or eliminating repetitive tasks, revealing new insights from data, driving analytically-based actions, improving service, and enhancing agencies' ability to achieve their missions.

As a series of reports[4] from the IBM Center and the Partnership have described, AI can help government employees focus on core responsibilities related to their agencies' missions and spend fewer hours on administrative duties. They are likely to have more time to plan for multiple scenarios, make choices among complex options, deliver services, and perform other mission-related tasks. Specific strategies for implementation that these reports cite include efficient decision making, risk management, and AI literacy.

AI can increase efficiency and improve decision making. Automating administrative tasks has been one of AI's initial benefits. Over time, federal employees are spending less time on repetitive administrative work and more of their workday on tasks that are core to their agencies' missions, from mitigating hazards in workplaces to following through on complicated applications for grants or other government services.

AI can adapt to address risks in a changing world. Questions about effects AI technologies may have include concerns about data privacy, security, and safety. Similar risk factors have affected public perceptions when other technologies were introduced; and similarly, today's leaders need to address these concerns to foster trust as agencies rely more on AI to carry out missions. As governments adopt AI, they should enable agencies to buy tested and trusted AI products, and create effective ways to identify and manage potential risks,

AI can increase focus on technical and data skills. Agencies need to enhance their digital and data literacy and learn how best to use AI and related technologies. As AI becomes more ubiquitous, government employees need new skills to succeed in an AI-enabled world, emphasizing expertise in technical, digital, and data skills. Indeed, governments cannot implement AI to improve foresight and anticipate future events in a world of risks without a skilled workforce that can implement strategies such as those listed above.

Quantum Computing

As defined by IBM, "quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers."[5] Quantum has significant potential to driven improvements in operational efficiency across government, and the capacity to address previously intractable problems. The technology can foster immense potential benefits for the public. As a tool to enhance anticipatory government, agencies must protect against risk in using quantum computing, Developing "quantum-safe" capabilities is crucial to maintaining data security and integrity for critical applications.

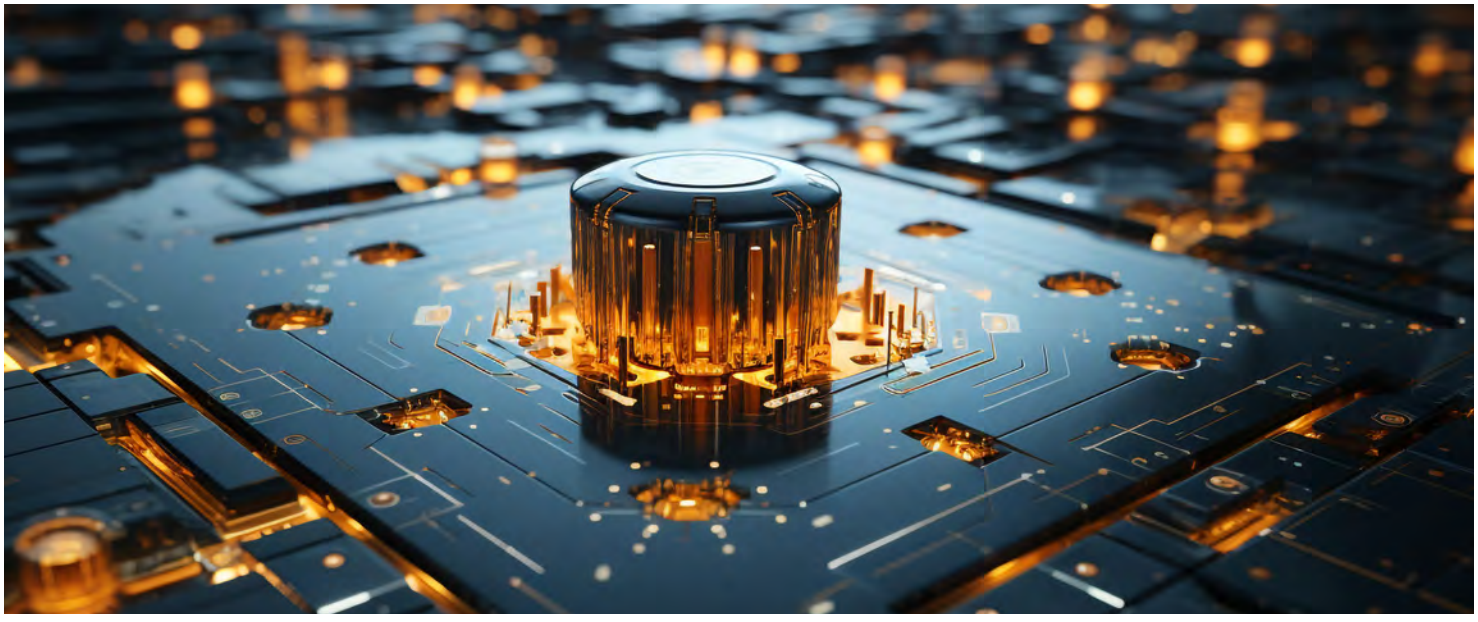
In the U.S., the National Quantum Initiative[6] brings together "a whole-of-government approach to ensuring the continued leadership of the U.S. in QIS [quantum information science] and its technology applications." Such an enterprise strategy is key to enabling government to tap into the potential for quantum to improve performance across a range of issues and use cases, including materials science, pharmaceuticals, finance, and energy.

Paula Ganga, a Stanford University fellow, notes that quantum computing has significant potential for improving agility and analysis across government, as well as enabling more sustainable computing environments given quantum's efficiency relative to traditional computing.[7] However, quantum introduces a number of risks that must be addressed in order for government to best capitalize on its potential, including cybersecurity. Quantum-safe cryptography is a burgeoning area to stay ahead of quantum-based attacks from adversary, and its integration with AI.

Recommendations for Quantum Adoption by Government

1. Outline the quantum computing possibilities and the ambition appetite.
2. Design platforms to orchestrate the quantum computing ecosystem to advance public value.
3. Leverage strategic international partnerships to accelerate and scale quantum computing discoveries and capabilities.
4. Invest in creating a public workforce that is quantum computing literate and skilled.
5. Establish an office to coordinate quantum computing initiatives across the public sector.
6. Publicize use cases on quantum computing in the public sector.
7. Identify risks and disruptions to digital systems across the public sector.

Source: Desouza, & Fatima (2023).



How Can Agencies Tap Emerging Technologies to Use Data for Greater Anticipation and Improved Performance?

Governments face an enormous and increasing barrage of information that drives content to enable anticipation and inform choices, in areas ranging from citizen interactions and business regulation to law enforcement, national security, and responding to major national and cross-border threats.

Technologies such as those discussed here enable governments to tap into data stores with previously unimaginable speed, scale, and accuracy. In anticipating future complexities, cloud, AI, quantum, and related intelligent automation technologies provide decision makers with tools to view the state of the world today, scenarios and probabilities for what may come tomorrow, and opportunities to redefine how governments can take action and improve outcomes for the public. Box A summarizes the kinds of mission capabilities that these technologies can support to help government build readiness for future shocks, leveraging these and similar technologies.

Box A: What practical steps can governments take in the near term to better prepare for and respond to future shocks?

Since the turn of the millennium, pandemics, heat waves, wildfires, floods, cyberattacks, supply chain interruptions, and other crises have deeply stressed governments, communities, businesses, and individuals around the world. This cascade of catastrophic events raises fundamental questions about how governments can anticipate, prepare for, and respond to these and other shocks yet to come.

The IBM Center for The Business of Government, IBM Institute for Business Value, and National Academy of Public Administration have launched an initiative to help governments identify core capabilities critical to building resilience.

Based on the common themes that emerged from the roundtable discussions, the following recommendations can assist governments at all levels to anticipate, prepare for, and respond to shocks of virtually any origin.

1. **Steer clear of complacency.** Many governments made great strides toward building resilience during the COVID-19 pandemic. However, it is risky to pull back on these investments, especially as the probability of major disruptive events in the future remains high.
2. **Identify risks inclusively, with systemwide thinking.** The greatest threat isn't the unknown crisis—it's failing to recognize that interlinked and compounded risks could destabilize the entire system. Government leaders and stakeholders should adopt holistic risk identification approaches, including diverse stakeholder inputs that capture a wide range of perspectives.
3. **Explore and strategically invest in data-driven technologies.** With the importance of making data-driven decisions growing every day, it is vital for governments to transition beyond maintaining legacy systems and invest strategically in more advanced cloud, AI, automation, and other platforms to protect government assets, boost workforce productivity, and take advantage of new opportunities to connect with and serve constituents. Technology investments should support this goal.
4. **Leverage cybersecurity as a capability multiplier.** Bolstering the security of all government platforms can improve the performance of these systems and boost confidence in their operations, an especially important consideration as generative AI takes on more functions and powers more workflows.
5. **Collaborate with and expand cross-sector partnerships.** Government can leverage the expertise and resources of private industry, academia, and other sectors to source and share best practices and avoid reinventing the wheel. Government leaders and stakeholders can work with industry to invest in technology-driven platforms and solutions that enable remote collaboration across public and private sectors.
6. **Build trust with citizens and employees.** Governments can use transparency and inclusiveness to address the trust deficits incurred by many governments, recognizing that trust is foundational for building and maintaining organizational resilience.
7. **Plan for human-centric resilience.** Infrastructure may survive a disaster, but how will constituents fare? Resilience plans that don't accommodate human needs will fail. Government leaders and stakeholders can invest in localized models to simulate the real-time impact of disasters on communities to inform targeted interventions.

To learn more about the Future Shocks initiative, please read the compendium report: https://www.businessofgovernment.org/report/future-shocks-roadmap.

Conclusion

Cloud computing provides significant scalability, and cloud platfoms provide for flexible and cost-efficient ways to store, process, and share data across computing siloes and organizations. AI, which strengthens cognitive understanding, can help public sector officials examine large datasets, and find patterns quickly and reliably to draw key insights, foster predictive analytics and optimize resource allocation. Quantum networks support using data to make findings and reach decisions at previously unthinkable speeds, holding immense promise for solving problems once considered insurmountable. By leveraging innovation responsibly, governments can act with agility to anticipate the future and make choices that best serve the public.

Endnotes

1. National Institute of Standards and Technology (2011). The NIST Definition of Cloud Computing. Special Publication 800-145 (p. 2). Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.
2. Gould, A. S. (2023). Mobilizing Cloud Computing for Public Service. IBM Center-Partnership for Public Service. Available: https://www.businessofgovernment.org/report/mobilizing-cloud-computing-public-service.
3. For more information see: https://nvd.nist.gov/vuln.
4. IBM Center and Partnership for Public Service. (2019). More Than Meets AI, Parts 1-2. Available: https://www.businessofgovernment.org/report/more-meets-ai-part-ii.
5. IBM (2023). What is Quantum Computing? https://www.ibm.com/topics/quantum-computing [Accessed 27, December 2023].
6. National Quantum Initiative. (nd). https://www.quantum.gov/about/, accessed December 2023.
7. Gangn, P., 2023. The Quantum Technology Challenge: What Role for the Government. In Chenok, D. & Keegan, M. J. (eds). Transforming the Business of Government, Chapter 9. IBM Center. Rowman and Littlefield. Available: https://www.businessofgovernment.org/blog/quantum-technology-challenge-what-role-government.