Accelerating Digital: Leveraging Innovation and Emerging Technologies to Modernize IT

Throughout history there have been inflection points that have tested the ability of governments to meet challenges and resolve issues for the greater good of their citizens. However, seldom has there been a convergence of multiple crises such as a global pandemic, economic upheaval, civil unrest due to social inequity and environmental instability due to climate change. Addressing these circumstances effectively requires research that helps government encourage and embrace technology innovation as part of the solution.

Accelerating the Pace of Change

Emerging and existing technologies have rapidly evolved to support digital transformation, and the pace of change is increasing. Digitization does not involve simply automating existing business or mission delivery models, but enables completely reimagining that model through digital platforms and tools.

Digitization harnesses technology to transform Government, while enhancing cybersecurity and maintaining the ability of agencies to focus on their mission. Governments are moving toward a "continuous improvement" model for IT modernization and technology delivery. Emerging technologies such as artificial intelligence and data analytics, and the power of digital platforms such as hybrid cloud services and quantum computing, allow for curating information to help government address pressing societal issues.

Managing and improving data quality will be fundamental to this overall transformation. Government can benefit from research on how to use digital tools to derive value from data. Deriving insights from data will assist in operating government well and measuring programs to determine if they are achieving their intended goals. At the same time, government must be cognizant of unintended consequences and build the important guardrails to protect privacy, ensure security and mitigate data bias.

Emerging Technologies and Digital Innovation Addressing Complex Issues -- Climate Change, Cybersecurity, Covid-19 Response and Recovery

Governments face many pressing and complex issues. Research can demonstrate how emerging technologies and digital innovation offer significant promise in addressing these issues and helping government agencies mitigate their impact.

Climate Change

Climate change represents one of the most pressing global issues that the Nation and the world face today. The impact on the global population is becoming more and more devastating. Research can highlight how digital innovation can help government address climate change.

Some clear examples have emerged of governments leveraging new technologies to affect trajectory of climate change. Technology, including predictive analysis, has long been used to forecast severe weather events and the early warning systems that allow governemnts to move populations out of harm's way. In October of 2020, the National Oceanic and Atmospheric Administration entered into a public-private partnership to use AI/ML to "enhance and amplify NOAA's use of satellite and environmental data to improve environmental monitoring, weather forecasting, climate research and technical innovation."[1]

Additionally, more frequent and stronger storms have an increasing impact on infrastructure and energy grids. Citizens sometimes lose power for months after a severe weather event; for those who need refrigeration for medication or power to run medical devices this can be a matter of life and death. The impact is often worse for the very young, the elderly, and the poorest of communities. Severe weather occurs more frequently now during all seasons, straining electric grids across the country and around the world. system in the state. According to a recent article in the Washington Post:

> As storms grow fiercer and more frequent, environmental groups are pushing states to completely reimagine the electrical grid, incorporating more batteries, renewable energy sources and localized systems known as "microgrids," which they say could reduce the incidence of wide-scale outages. Utility companies have proposed their own storm-proofing measures, including burying power lines underground. But state regulators largely have rejected these ideas, citing pressure to keep energy rates affordable."[2]

Energy production and use contribute to and are negatively impacted by climate change, making energy production less resilient. Transportation and agriculture also fall in this category. A report from arXiv.org, "Tackling Climate Change with Machine Learning"[3], outlines multiple areas of interest where technology can be used to combat climate change and improve the resiliency of infrastructure, including AI for simulation and modeling to balance outcomes. Approaches such as microgrid development and precision farming can leverage technology to optimize output from scarce resources.

The USDA/US Forest Service utilizes geospatial technology and analytics to identify areas where reforestation would have the greatest impact. In addition, urban planners use climate data analytics to integrate climate change principles into sustainable development approaches as a key mitigating strategy.

Technology can assist with meeting sustainability commitments by ensuring emissions are monitored, opportunities for action identified, and progress measured. With the advent of the internet of things, every step of the supply chain can be metered and monitored for emissions. Arial technology such as airplanes and drones can be used to gather emissions data.

---

[1] https://www.noaa.gov/media-release/ai-agreement-to-enhance-environmental-monitoring-weather-prediction
[2] https://www.washingtonpost.com/business/2021/10/24/climate-change-power-outages/
[3] https://arxiv.org/pdf/1906.05433.pdf

Sophisticated satellite imagery also gives governments an even broader view of emissions status.

Similarly, a planned United States-New Zealand space initiative, MethaneSAT, is due for launch in 2022. This observation satellite will monitor and study global methane emissions. Data will supplied to countries, industry and citizens in order to help identify the best places for intervention and investment to reduce methane emissions.

Cybersecurity

The adverse use of cyber tools by nation states and by other actors threatens national security, disrupts government service delivery, and our daily existence and supports criminal activity. And AI can both defend against nefarious activity, and also be an enabler. Research on areas where progress can be made is essential. Some of these areas were outlined in the Presidential Executive Order 14028 on Improving the Nation's Cybersecurity[4], and include:

- Improvements in threat information sharing between the government and private sector
- Government use of stronger cybersecurity standards such as zero trust architectures, encryption and multi-factor authentication
- Improvements in software supply chain assurance
- Improvements in detection, response to and recovery from cyber incidents

One recent cyber incident illustrated gaps in security in government, commercial enterprises, and critical infrastructure. The Solar Winds incident showed vulnerabilities in the software development lifecycle process and the global supply chain. In the area of software supply chain assurance, "DevSecOps" principles can drive ecosystems for developing software based on those principles. As a recent Center report highlighted[5], using DevSecOps supports a pre-approved software development environment where developers can experiment. Developers can code, test, prove or disprove initial hypotheses about how the code will work, adjust the software build according to what they learn, and then continue iterating. Capability and features are developed into viable products. Security is incorporated into the build, and continuously tested.

Another recent incident, the ransomware attack on Colonial Pipeline, illustrated another vulnerability. The White House has initiated international partnerships to accelerate cooperation on improving network resilience, addressing the financial systems that make ransomware profitable, disrupting the ransomware ecosystem via law enforcement collaboration, and leveraging the tools of diplomacy to address safe harbors and improve partner capacity. AI has emerged as a key tool to guard against such attacks.

---

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[5]

https://www.businessofgovernment.org/sites/default/files/Achieving%20Mission%20Outcomes%20Through%20DevSecOps.pdf

According to a recent article by the IEEE Computer Society, "The Use of Artificial Intelligence in Cyber Security,"[6] AI enables public and private sector organizations to improve the cyber posture of environments world-wide. AI can improve defenses in the areas of detecting new threats, recognizing bots, improving breach risk prediction and endpoint protection.
AI and machine learning help build a thorough understanding of website traffic and distinguish between good bots (like search engine crawlers), bad bots, and humans.

AI systems help determine the IT asset inventory, an accurate and detailed record of all devices, users, and applications with different levels of access to various systems. AI-based systems can predict likelihood of compromise to plan and allocate resources towards areas of most vulnerability.

Response and Recovery from the COVID -19 Pandemic

AI been critical to the COVID-19 pandemic response and recovery. The onset of the pandemic highlighted the lack of preparedness and flaws/gaps in the country's medical infrastructure, global supply chain, and policy and governance constructs.

Technology played a key role in helping the global community improve the speed to market for key therapeutics and vaccines, track the spread of the virus and the emergence of variants, and monitor the efficacy of medical and physical mitigation approaches.

According to an OECD Policy Response to the Coronavirus,[7] AI can help predict old and new drugs or treatments that might treat COVID-19, and can be used to predict the structure of proteins associated with SARS-CoV-2 (the virus that causes COVID-19). In addition, dedicated AI learning platforms can more rapidly share coronavirus literature to accelerate research, though access to datasets in epidemiology, bioinformatics and molecular modelling. Computing power for AI is also being made available by technology companies and by public-private efforts like the COVID-19 High Performance Computing Consortium and AI for Health.

Multiple opportunities now exist to leverage technology as the nation continues to recover from the pandemic and prepares for future health crises. AI can help identify emerging variants and track their geographic epidemiological path -- allowing governments to share scientific breakthroughs to accelerate the development of therapeutics and vaccines, and to improve logistics and supply chains for PPE and other critical medical supplies.

Conclusion
The next phase of digital government will advance with research showing how emerging technologies can help government and improve operations and address crises. Technology exponentially improves human ability to respond under rapidly evolving circumstances.

---

[6] https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity
[7] https://www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21/

Technology, analytics, and AI enable government to access curated data to derive insights, enhance decision making, model and simulate actions, perform predictive analyses, focus activities, and measure results.