

Orchestration: A Key Framework for 21st Century Government Action

By Daniel Chenok



The collective response to COVID-19 over the last two years—and the emerging pattern of recovery from this unprecedented global pandemic—reveals little to no value in a sole actor response to twenty-first century challenges. Only through leveraging a mosaic of interests can most modern complexities be addressed by governments, often working with their partners in civil society, academia, and industry.

A strategy and roadmap to orchestrate players and systems now stands as one of the pillars of successful modern governance—orchestration similar to leading a great symphony from the conductor’s podium, but with far more players and higher stakes. The orchestration needed for a digital age involves multiple levels of action, which fall into three categories: organizations, systems, and technologies. Here are key elements of this strategy, based on recent research from the IBM Center.

Organization

Many government programs involve supply chains for the production and distribution of goods, services, data, funds, and other public benefits. The national response to the COVID pandemic has included hundreds of federal, state, local, and private sector entities in the exchange and distribution of information, personal protective equipment, testing, and vaccine administration. The administration of these programs can be transformed by leveraging a “whole of government” scope and industry-leading supply chain management, as well as shared services business models to their delivery.

Through such a networked effort, individuals who step outside assigned roles and designations and join with others can bring their collective talent to bear on urgent problems. Greater networked response capacity will be necessary to improve future response capability. Expanding this capacity



“To win on the future battlefield, governments must focus on gaining situational advantages—making decisions better and faster than the enemy.”

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

will require improved transparency and information sharing across levels of government and throughout the private sector.

In the context of national defense, a recent IBM Center report discussed how orchestration across organizations in the air, sea, land, space, and cyber domains—referred to as “Multi-Domain” or “Joint” Command and Control—enables governments and partner organizations to meet the challenges of twenty-first century engagement. To win on the future battlefield, governments must focus on gaining situational advantages—making decisions better and faster than the enemy.



MDC2, also referred to as Joint All-Domain Command and Control (JADC2), represents the operational vision of connecting sensors from all military services into a single, interoperable, actionable data environment. Following on the foundations of network-centric operations, MDC2 leverages data-centricity to include data interoperability across different sensors, communication, and processing capabilities, to produce effective command and control capabilities to ensure collective defense.

Data

Data gathering, analysis, and dissemination across multiple levels of government, and among international governments, can enable information sharing to enhance threat prediction and prevention in a global context. International stakeholders can increase the understanding of effective ways to leverage channels involving technology, human capital, organizations, and private sector coordination that meet strategic, mission, and operational needs. Governments can leverage data integration and analytics to support better decision-making around a range of mutual challenges, especially in cyber and homeland security.

Technology

To start, the application of artificial intelligence (AI) to address government challenges is a team sport. For example, AI can help predict and prevent harmful behavior and identify at-risk communities in real time. However, even with the most effective and accurate algorithms, only human actors can determine how to turn AI insights into action and identify a valid intervention that would not cause residual problems.

Other examples of this need to orchestrate AI strategies include leveraging data gathered by drones to narrow down the path of hurricanes, managing the influx of cybersecurity events and reviewing logs, and applying natural language processing (NLP) to analyze public comments in regulatory proceedings. AI can even predict where floods or saturation might occur and help manage levees, locks, dams, and critical infrastructure waterways. The application of this technology in the real world, however, requires an orchestrated action plan.

A particular technology that can strengthen supply chains involves blockchain, which enables a shared ledger to record the history of transactions with consistency and certainty across a network. In a blockchain business network, all parties to a transaction must give consensus



before a new transaction is added. Once recorded in the blockchain network, a transaction cannot be altered. Blockchain eliminates or reduces paper processes—speeding up transaction times, increasing efficiencies, and building trust among participants to a transaction.

Finally, a hybrid and multi-cloud architecture can provide a consistent, standards-based approach to orchestrate development, security, and operations. This smarter

architecture allows for workload portability, orchestration, and management across multiple environments.

Orchestration Relies on Open Strategies

Orchestrating across “open” systems that rely on data sharing can yield broader and deeper positive outcomes than “closed” systems that restrict access to internal data. But some question the security of open systems.

For example, in a world that has already witnessed the inadvertent exposure of sensitive military sites by technology as mundane as fitness apps, there is concern around how public data sources may be used by foreign adversaries to harm U.S. interests.

But the benefits of an open approach are clear. For example, analysts now leverage commercial data to understand changes happening at U.S. military bases and how that could affect national security. And there is a cost to not sharing data or working collaboratively. Because the resources of any single organization are inherently limited, pursuing responsible partnerships represents a viable path to realizing objectives that would otherwise be impossible. At a 2021 Roundtable that the IBM Center helped to drive, one government leader commented:

“Are we losing things by not collaborating or putting a choke or a governor on collaboration? I think the answer is yes. . . . I think you’re starting to see a shift in organizational culture. There are use cases and considerations where opening up access to closed data is becoming common. We’re starting to implement those mechanisms.”

A Path Forward

An action-oriented strategy can help governments orchestrate across functional communities—including mission leaders, engineers, and end-users—as well as reach out to their nonprofit, industry, and academic partners. An IBM Center report recently emphasized the importance of building partnerships with key organizations in the public, private, and nonprofit sectors. It focused on managing networks needed to drive such partnerships to overcome challenges by improving operations and service delivery. It also discussed steering outcomes across networks that lead to well-understood and measurable improvements in the health and well-being of the public.



Governments should consider these specific recommendations to orchestrate across networks:

- **A new organizational model** to effectively leverage state, local, and industry resources in a unified national response capability—for example, in combating national crises like Covid-19
- **A robust and well-integrated planning and governance framework** that would align and coordinate these interests throughout the lifecycle of response activities
- **Addressing data challenges** through cross-agency and intergovernmental data standards and integration
- **A cultural shift** to tackle issues on a whole-of-nation basis