SPECIAL REPORT

IBM Center for The Business of Government

Delivering on the Vision of Multi-Domain Command and Control

Dr. David Bray
Distinguished fellow, Stimson Center & Atlantic Council

IBM Center for
The Business of Government
2022

Special Report

Delivering on the Vision of Multi-Domain Command and Control

Dr. David Bray
Distinguished fellow, Stimson Center & Atlantic Council

IBM Center for
The Business of Government
2022

Table of Contents

MDC2 is a strategy for integrating and coordinating command and control operations simultaneously across air, land, sea, space, cyber, and electromagnetic domains.

Foreword

Daniel J. Chenok

Daniel Munro

Across the defence and national security landscape, governments and partners are grappling with the speed of technological change and a deteriorating global strategic context. From capability development to planning to operations, leaders recognize that Western Allies no longer have a technological advantage over peer adversaries. To win the future battle, governments must focus on gaining situational advantage—making decisions better and faster than the enemy. Multi-Domain Command and Control (MDC2) addresses gaining that decision superiority. This strategy enables integration and coordination of command and control operations simultaneously across air, land, sea, space, cyber, and electromagnetic domains.

Dr. David Bray has expertly gathered the thoughts and insights of a diverse range of leaders from defence, industry, and academia, who joined a roundtable discussion in October 2021 on the effectiveness of MDC2 implementation.

By defining the need for MDC2 in context of the human flaws and irrationality in chaotic, uncertain, ambiguous circumstances—as well as the ability of the adversary to contribute to that uncertainty and the inherent flaws of any technological system and its processes—Dr. Bray elevates the discussion beyond any single challenge. This is vital because the modern battlespace is anything but homogenous. Today's military terrain involves a seething mass of digital infrastructure that includes edge assets, public/private clouds, embedded weapons systems software, and a host of Internet of Things (IoT)—all built separately, over a long period of time and for different purposes.

To solve for the challenges of MDC2, this paper outlines a range of action-oriented steps to be taken. Each step supports one or both of these top-line statements:

- **Strong and gifted commanders, at all levels, must remain at the centre of the solution.** They must learn, and continually relearn, how to take best advantage of available technology to inform development of the next generation of systems.

- **Only a hybrid cloud architecture can provide a consistent, standards-based approach to development, security, and operations.** This smarter architecture allows for workload portability, orchestration, and management across multiple environments.

For defence and national security—when the mission is this critical—agility and flexibility are paramount. Such a complex undertaking does not mean a lack of planning or unstructured implementation. It means taking the right approach to avoid being locked in and unable to respond to a changing environment. We hope this paper will help prompt deeper assessment about creating the capability needed for the future.

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com

Daniel Munro
Defence Global Markets
IBM
daniel.munro@ibm.com

Background

Multi-Domain Command and Control (MDC2), also referred to as Joint All-Domain Command and Control (JADC2), represents the operational vision of connecting sensors from all the military services into a single, interoperable, actionable data environment.[1] Though based on the earlier visions of Network-Centric Operations, modern day MDC2 differs in that it fundamentally represents data-centricity to include interoperability at the data-level across the different sensors, communication, and processing capabilities associated with all military services. As a result of this centrality of data interoperability, both analysts and operators across services—including human and artificially intelligent digital agents assisting humans—collectively can overcome the challenges of data overload, detection of weak signal-from-noise associated with important information, and information complexity of command and control spanning different domains of defence simultaneously.[2]

On October 19, 2021, several speakers from Australia, the U.S., and the U.K. assembled for a virtual conference as part of IBM SPADE 2021. This document represents a synthesis of the immediate realities each of the speakers see with regards to MDC2 as well the near-term action necessary to produce effective command and control capabilities to ensure collective defence in conflicts with either near-peer adversaries or faceless non-state terror organizations.

> War is the realm of uncertainty; three-quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty.[3]
>
> —*Carl Von Clausewitz*

1. https://crsreports.congress.gov/product/pdf/IF/IF11493.
2. https://www.16af.af.mil/News/Article/2421718/decision-superiority-through-joint-all-domain-command-and-control/.
3. https://www.globalsecurity.org/military/library/policy/usmc/mcdp/6/mcdp6_ch1.pdf.

Why the Future of Defence Requires Multi-Domain Command and Control

Australia is under near constant cyberattack. Such a reality represents both significant challenges as well as an exciting time for defence to better use data to uplift cyber defence and to unbalance Australia's rivals. This is just one example of the challenges nations like Australia, the U.S., the U.K., and others are facing. The post-pandemic world looks more dangerous than the decade that preceded it. There is no room for complacency in such an environment in which reengagement of near-peer competition is present.

The Five Eyes intelligence alliance comprising Australia, Canada, New Zealand, the U.K., and the U.S. is based upon exquisite data collection as well as crucial information sharing. It is also subject to disruption of communications, be it from electronic warfare, cyberwarfare, or traditional physical attacks. In such challenging environments, quicker and higher-quality decisions are paramount. MDC2 is essential for quality command and control decisions that require augmenting human intelligence as well as augmenting the synthesis of massive amounts of data to produce better intelligence. This includes MDC2 operating at timescales relevant to the operation-at times waiting for just the right moment to decide and execute to use temporal effects for maximum advantage.

> (1) Is the proposed operation likely to succeed? (2) What might be the consequences of failure? (3) Is it in the realm of practicability of materials and supply?
>
> *—Fleet Admiral Chester W. Nimitz*[4]

4. https://www.history.navy.mil/get-involved/essay-contest/2017-winners/additional-essay-contest-submissions/theater-jfmcc---back-to-the-future-.html.

What Implementing Multi-Domain Command and Control Will Achieve

Successful MDC2 requires quicker and higher-quality intelligence—noting that intelligence is not synonymous with more data. In many cases, the moderate era of defence confronts environments overwhelmed with data and underwhelmed with actionable intelligence. To produce both quicker and higher-quality intelligence from which to make superior decisions, military services must get control of their data in all the data environments in which operations occur. This requires command and control data that can act at the tactical edge, operational level, and across a strategic theatre. Achieving this requires connecting all battlespace sensors across domains; military services must break out of their data communication boxes completely.

Connecting all battlespace sensors across domains essentially means connecting all sensors since the modern battlespace essentially is an undefined environment wherein conflict and contestation can occur anywhere at any time. Nowadays tactical physical engagements can overlap with global cyber defence operations simultaneously in ways that significantly change the dimensions of the battlefield. For MDC2 to succeed, it is imperative to know what datasets are valuable to transport, assess, and synthesize at relevant timescales for quality decisions. Currently, knowing what datasets are relevant confronts again the modern-day challenge of an overwhelming volume of data relative to an underwhelming amount of actionable intelligence.

Solving the challenge of knowing what datasets are relevant for tactical, operational, and strategic multi-domain engagements requires artificial and augmented intelligence as well as automation—not to take the final decisions away from analysts, operators, or commanders, but rather to weed through all the initial data to convert the abundance of data into actionable intelligence by which humans can make quality decisions. It is important to note that MDC2 is not about removing the decision authority from

commanders. Rather, MDC2 is about providing a better command-level picture so that humans can make quicker and higher-quality decisions. These include recognizing the human limits that analysts and commanders need to sort through to get to the point where they can produce superior command and control decisions.

Alongside knowing what datasets are relevant and how complementing the data with technology tools can aid humans in sifting through data to produce intelligence and superior decisions, MDC2 also requires a better picture of the security of command and control. Military services must ensure their digital and physical practices place transportable and accessible data at the heart of decision-making. Transportable and accessible data requires a grand ecosystem of multi-cloud solutions that span different security domains. This includes zero-trust security baked into how data-centric activities occur. This also requires that command and control activities must recognize the possibility that some datasets are compromised, faulty, or intentionally deceptive to confound decision-making in times of conflict. It presents a requirement for MDC2 to incorporate a new security architecture that enables quicker and higher-quality intelligence, decisions, and operations despite compromised datasets. This new security architecture for effective MDC2 requires methods to perform real-time verification and retesting data of sources across domains.

Effective MDC2 also requires the capabilities for commanders to order, execute, and implement decisions at relevant timescales. This will include waiting for just the right moment to decide and execute to use temporal command and control effects across multiple domains for maximum advantage. Such capabilities require a connective digital network structure that permits multi-routing of actions with the assumptions that some aspects of communications will be disrupted or destroyed by adversarial actions. An effective MDC2 digital fabric must continuously reassess what are the best paths for certain times of mission data and actions. This includes autonomous assessments and routing across different communications modes—fibre optics, satellite transmission, 5G, high-frequency radio communications, and more—given contested battlefield environments.

Past military efforts at network-centric did not deliver on promised capabilities in part because of an absent focus on the data as well as a lack of maturing of digital technologies to operate at timescales relevant to employ artificial and augmented intelligence methods effectively. From a technological perspective, delivering successful MDC2 requires three crucial actions. First, technologies must transform how datasets are organized to test assumptions of both analysts, operators, and commanders. Second, technologies must achieve data-centric, interoperable activities across a vast number of sensors to best inform intelligence activities as well as command and control.[5] Third, technologies must augment the abilities of analysts and commanders to make superior decisions; achieving this requires both integration across different systems to produce multiple answers from different algorithmic platforms as well as continuous verification and retesting of security assumptions.

From an organizational culture perspective, delivering successful MDC2 will change depending on how humans are trained and operate together. For analysts, operators, and commanders, new forms of training to interact with MDC2 systems and avoid data overload will be necessary. Such training will include human-machine teaming with

5. https://asc.army.mil/web/news-stitching-the-armys-data-fabric/.

digital agents, whereby digital agents help augment some of the sifting through relevant data for analysts and help tip and cue commanders to relevant issues warranting their attention. Practicing and learning from these new ways of thinking will be essential to success. Military services must ensure human simulation and synthetic training occurs for personnel alongside assistive digital agents.

Given there are no boundaries to modern battlefields, even tactical commanders who might be experiencing immediate incoming advisal action will need to think and consider what's happening outside this immediate environment to include potential cyberwarfare, disruptive information operations, supply chain exploits, or other strategic actions impacting the commander's long-term success or failure. The U.S. saw some aspects of this in the Middle East where there were tactical cyber engagements on the Afghan Mission Network alongside a larger, global cyber battle occurring in parallel. Operating at tactical, operational, and strategic scales requires curated datasets and digital twins of physical environments and entities of interest.

Consequentially, MDC2 requires both new technologies and changes in how analysts and commanders scale their thinking, focus, and ways of operating. Analysts, operators, and commanders must practice with MDC2 technologies and iteratively learn by doing as they operate alongside artificially intelligent digital agents. Changes in how analysts, operators, and commanders train will ensure MDC2 successfully assists humans to translate data into intelligence and translate intelligence into actions at the speed of decision-making. Successful MDC2 also recognizes that necessary data will not always get through, either through disruption, modification, or human irrationality and flaws in a time of conflict. Most importantly, this means we must still rely on our commanders in the field and develop a command system that understands its own flaws and potential points of failure well.

> The commander in war must work in a medium which his eyes cannot see; which his best deductive powers cannot always fathom; and with which, because of constant changes, he can rarely become familiar.
>
> *—Carl Von Clausewitz*[6]

6. https://www.globalsecurity.org/military/library/policy/usmc/mcdp/6/mcdp6_ch1.pdf.

How to Start the Journey to Implement Multi-Domain Command and Control

Successful MDC2 also will require jointness across services—all military services as well as intelligence. Such effects will require robust scalability of command and control across domains as well as across tactical, operational, and strategic engagements. Such scalability will need to recognize the importance of decentralized capabilities that can come together and "appear" to be centralized by sharing data yet operate in a coordinated decentralized fashion should lines of communication become degraded. Decentralized MDC2 capabilities also permit superior coordination of actions across time, space, and domains.

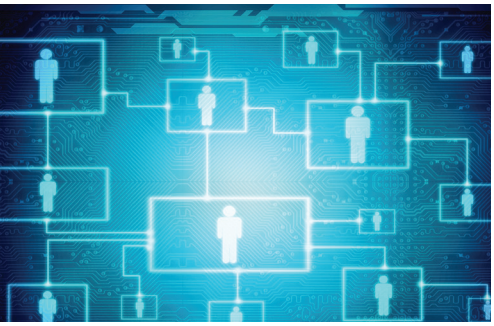
MDC2 requires adapting contracting and procurement of new technologies and services to match the speed of change in such capabilities. This means contracting and procurement must shift to outcome-driven delivery which can morph and adapt to support more hands-on pilots, prototypes, and experiments. The voice of the customer needs to be embedded at the very start and continue throughout the entire development and operations process. MDC2 contracting and procurement will require open standards and better integration with industry to develop MDC2 capabilities for the military services.[7] Successful contracting and procurement also require new methods of rapid experimentation to maintain the pace of technology development and adaptation, while openly building and innovating.

Starting the journey to implement MDC2 will require modernizing the military services—both in terms of technologies and operations. Strong and gifted leaders, focused on empowering their teams to collaborate and break out of the paradigm of doing things per the "old ways," are fundamental. Some circumspection about future command and control systems is warranted in helping to inform the design of future

7. https://www.af.mil/News/Article-Display/Article/1766202/industry-gets-schooled-on-mdc2/.

systems; no single communications procedure, method, or system is itself sufficient to guarantee success or even adequate conduct of command in war. Approaches come and go, yet the challenges of command and control remain.

Technology itself is not a cure-all. Data will not always get through due to disruption, modification, or human irrationality and flaws. Each new command system is a response to an evolving context and new set of problems—presenting new opportunities as well as potential new limitations. Not only do we seek new technological and data-centric capabilities, near-peer adversaries seek the same. As such, trusted team-based development of MDC2 includes experimentation, open-thinking, and bottom-up innovation—necessary to ensure what is developed remains relevant in a rapidly changing world.

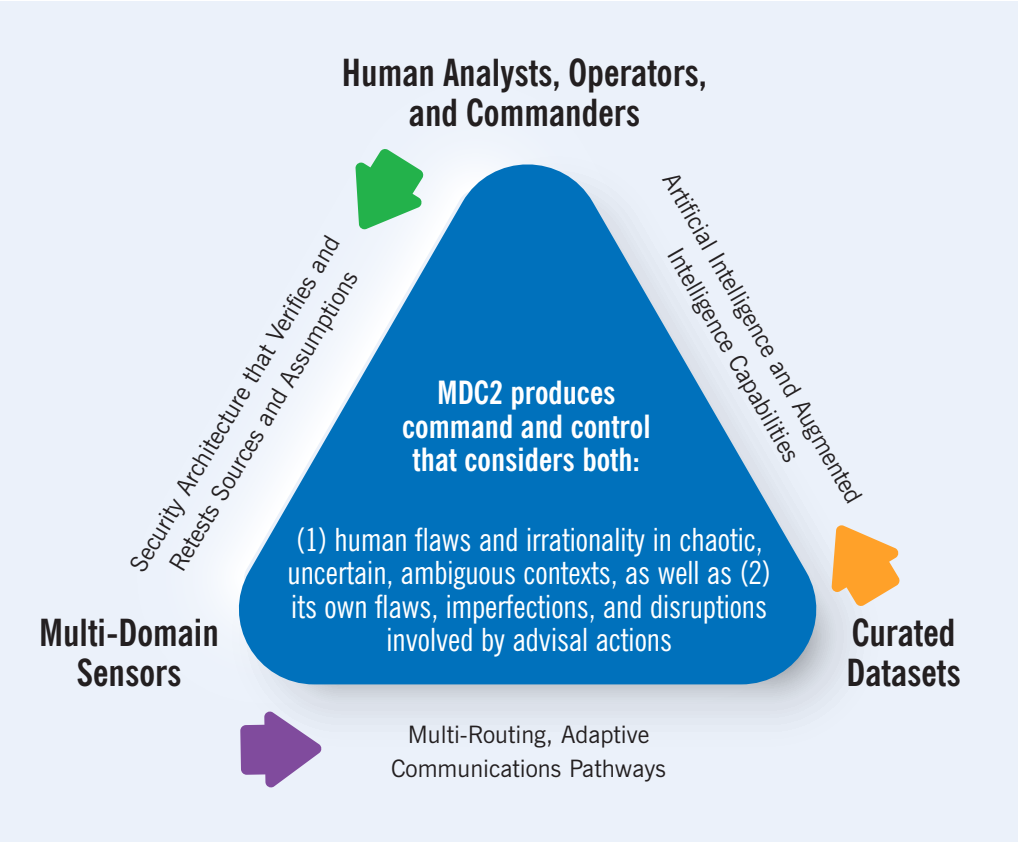


Such experimentation and bottom-up innovation must embrace, from the state, that the promise of ubiquitous data in future conflicts may not be an actual reality. The quintessential, idealized diagram of all of the "blue force's" tanks, ships, planes, satellites, and warfighters operating in perfect synchronicity with the "red force's" equipment and personnel may be only that—an ideal. The reality needs to recognize that loss of communications and data-centric capabilities might be lost from the very start of a conflict. MDC2 cannot be static, it must be adaptive, as adversaries will seek counters and workarounds. As such, MDC2 must always be adapting and exploring new methods and capabilities, as well as ways to overcome adversarial counters. Conflicts in cyberspace have already shown this dynamic of action and counteraction; we should anticipate the same for future multi-domain battlespaces.

A better diagram for how to proceed with MDC2 recognizes three crucial nodes essential for success: (1) multi-domain sensors, (2) curated, interoperable datasets, and (3) human analysts, operators, and commanders. Successful MDC2 connects these three crucial notes with:

- Multi-routing, adaptive communications pathways
- Artificial intelligence and augmented intelligence capabilities
- Security architecture that verifies and retests sources and assumptions

The strategic value when implementing MDC2 is to assist analysts and commanders in chaotic, uncertain, ambiguous space between the perfect function of command and control and its inevitable disruption, imperfection, and malfunction in the face of adversarial actions. Unlocking this strategic value raises the overarching goal of MDC2: to design and demonstrate a command and control that considers both (1) human flaws and irrationality in chaotic, uncertain, ambiguous contexts as well as (2) its own flaws, imperfections, and disruptions involved by advisal actions—such that the system can evolve and adapt. Such a command system would anticipate its own failures such that when it fails, it "fails well" amid contested environments.



The good news is there are already hints about how to achieve this overarching goal and unlock the strategic value of continuous and evolving implementation of MDC2 across military services. Decentralization, mission commanders' intent, and task-oriented teams already have been demonstrated and provide value in requiring adaptive, distributed efforts to operating disconnected from a main command system.

Successful MDC2 also will need to account for the great diversity of analysts and commanders who operate within the systems, to include their myriad strengths and weaknesses, preferences, and optimal presentation of data and intelligence for actionable decisions. MDC2 will need to identify when the risk of an analyst or commander drawing mistaken conclusions from the data presented is high, as well as to identify ways to help the human be aware and adjust for this. Similarly, MDC2 will need to reflect when its own digital agents providing artificial and augmented intelligence capabilities may have limitations, flaws, or gaps in their capabilities not readily visible to analysts, operators, or commanders. Again, such realities necessitate experimentation, open-thinking, and bottom-up innovation to hone and improve human-machine teaming for the purposes of MDC2.

Tactical forces with their own sensors and ability to effect actions on battlefields may in some circumstances overcome dependence on remote sensors and remote abilities to effect actions. When MDC2 permits coordination of these actions across time and

space, force multipliers occur in this coordination. These proof points point to an MDC2 that is not "one size fits all" or only operates in one way; rather successful MDC2 must account for different ways of operating, thinking, and effecting actions. Such realities include MDC2 operating both when data and connectivity is abundant, as well as when data and connectivity is scarce.

Ultimately, for MDC2 to provide superior decision-advantages, it must incorporate iterative codesigning of artificial intelligence with human systems. MDC2 must ensure its technological aspects incorporates both human psychology and doctrinal innovation to include learning by doing. In starting the journey to implement MDC2, it is essential to ensure a tightly coupled relationship between implementing new technologies and the necessary shifts in how analysts, operator, and commanders are trained.

> That is not to say that we can relax our readiness to defend ourselves. Our armament must be adequate to the needs, but our faith is not primarily in these machines of defence but in ourselves.
>
> *—Fleet Admiral Chester W. Nimitz*[8]

8. https://www.bartleby.com/73/409.html.

Six Action-Oriented Recommendations from SPADE 2021

As a result of the shared discussions on October 19, 2021, the collective set of points raised by a diverse group of speakers from Australia, the U.S., and the U.K. provided a set of action-oriented recommendations on how to advance and deliver the capabilities of MDC2, to include:

1. **Military services must break out of their data communication boxes completely.** This action includes changing how datasets are organized to test assumptions, ensure interoperable activities across a vast number of sensors, and providing integration to produce ensuring multiple answers from different algorithmic platforms.

2. **Military services must ensure their digital and physical practices place transportable and accessible data at the heart of decision-making.** To succeed, MDC2 efforts must assemble a grand ecosystem of multi-cloud solutions that span different security domains, with zero-trust security baked into the assumptions that data may be compromised, faulty, or intentionally deceptive to confound decision-making in times of conflict.

3. **Military services must ensure human simulation and synthetic training occurs for personnel alongside assistive digital agents.** This action recognizes that in addition to curated datasets and digital twins of physical environments and entities of interest, humans must practice and iteratively learn by doing as they operate alongside artificially intelligent digital agents assisting humans to translate data into intelligence and translate intelligence into actions at the speed of decision-making.

4. **Contracting and procurement must shift to outcome-driven delivery which can morph and adapt to support more hands-on pilots, prototypes, and experiments.** To succeed MDC2 requires the voice of the customer to be embedded at the very start and continue throughout the entire development and operations process, to include better integration with industry and new methods of rapid experimentation to maintain pace with technology development and adaption, while openly building and innovating.

5. **Strong and gifted leaders, focused on empowering their teams to collaborate and break out of the paradigm of doing things per the "old ways," are fundamental.** This action recognizes that MDC2 must recognize that technology itself is not necessarily a silver bullet; instead, trusted team-based development to include experimentation, open-thinking, and bottom-up innovation are necessary to ensure what is developed remains relevant in a rapidly changing world.

6. **We must still rely on our commanders in the field and develop a command system that understands its own flaws and potential points of failure well.** To succeed MDC2 must recognize necessary data will not always get through, either through disruption, modification, or human irrationality and flaws in a time of conflict. This means that for successful MDC2 to provide the superior decision-advantages, it must incorporate iterative codesign of artificial intelligence with human systems that ensure robust scalability, decentralized capabilities, and solution adaptability to evolving situations—both those that we expect to confront as well as the unexpected.

> If the leader is filled with high ambition and if he pursues his aims with audacity and strength of will, he will reach them in spite of all obstacles.
>
> —Carl Von Clausewitz[9]

9. https://www.goodreads.com/author/quotes/67848.Carl_von_Clausewitz.

About the Author

Dr. David Bray is a distinguished fellow at the non-partisan Stimson Center and a distinguished fellow at the Atlantic Council. He is principal at LeadDoAdapt Ventures, focused on how data and new technologies are changing the world. Dr. Bray has served in a variety of leadership roles in turbulent environments, including satellites associated with the Ballistic Missile Defence Organization in the mid-1990s, bioterrorism preparedness and response from 2000-2005, executive director for a bipartisan national commission on research and development, providing non-partisan leadership as a federal agency senior executive, work with the U.S. Navy and Marines on improving organizational adaptability, and with U.S. Special Operation Command's J5 Directorate on the challenges of countering disinformation online. He has received both the Joint Civilian Service Commendation Award and the National Intelligence Exceptional Achievement Medal. *Business Insider* named Dr. Bray one of the top "24 Americans Who Are Changing the World" under 40 and he was named a Young Global Leader by the World Economic Forum. For twelve different start-ups, he has served as president, chief strategy officer, and strategic advisor roles.

Dr. David Bray

Key Contact Information

David Bray, PhD

The Stimson Center
1211 Connecticut Ave
NW | 8th Floor
Washington, DC 20036

dbray@stimson.org

RECENT REPORTS FROM THE IBM CENTER FOR THE BUSINESS OF GOVERNMENT

For a full listing of our publications, visit www.businessofgovernment.org

Agility

Adopting Agile in State and Local Governments by Sukumar Ganapati

The Road to Agile GOVERNMENT: Driving Change to Achieve Success by G. Edward DeSeve

Transforming How Government Operates: Four Methods of Change by Andrew B. Whitford

Agile Problem Solving in Government: A Case Study of The Opportunity Project by Joel Gurin, Katarina Rebello

Applying Design Thinking To Public Service Delivery by Jeanne Liedtka, Randall Salzman

Digital

Artificial Intelligence in the Public Sector: A Maturity Model by Kevin C. Desouza

Aligning Open Data, Open Source, and Hybrid Cloud Adoption in Government by Matt Rumsey, Joel Gurin

Innovation and Emerging Technologies in Government: Keys to Success by Dr. Alan R. Shark

Risk Management in the AI Era: Navigating the Opportunities and Challenges of AI Tools in the Public Sector by Justin B. Bullock, Matthew M. Young

Financial Management for The Future: How Government Can Evolve to Meet the Demands of a Digital World by Angela Carrington, Ira Gebler

Effectiveness

Managing The Next Crisis: Twelve Principles For Dealing With Viral Uncertainty by Katherine Barrett and Richard Greene, Donald F. Kettl

Other Transactions Authorities: After 60 Years, Hitting Their Stride or Hitting The Wall? by Stan Soloway, Jason Knudson, Vincent Wroble

Guidance on Regulatory Guidance: What the Government Needs to Know and Do to Engage the Public by Susan Webb Yackee

Federal Grants Management: Improving Outcomes by Shelley H. Metzenbaum

Government Reform: Lessons from the Past for Actions in the Future by Dan Chenok, John Kamensky

COVID-19 and its Impact: Seven Essays on Reframing Government Management and Operations by Richard C. Feiock, Gurdeep Gill, Laura Goddeeris, Zachary S. Huitink, Robert Handfield, Dr. Rodney Scott, Sherri Greenberg, Eleanor Merton, Maya McKenzie, Tad McGalliard

Insight

Using Technology and Analytics to Enhance Stakeholder Engagement in Environmental Decision-Making by Jenna Yeager

Making Federal Agencies Evidence-Based: The Key Role of Learning Agendas by Dr. Kathryn E. Newcomer, Karol Olejniczak, Nick Hart

Improving Outcomes in Government through Data and Intelligent Automation by The IBM Center for The Business of Government, Partnership for Public Service

Silo Busting: The Challenges and Successes of Intergovernmental Data Sharing by Jane Wiseman

Integrating Big Data and Thick Data to Transform Public Services Delivery by Yuen Yuen Ang

A Practitioner's Framework for Measuring Results: Using "C-Stat" at the Colorado Department of Human Services by Melissa Wavelet

People

Sustaining a Distant Vision: NASA, Mars, and Relay Leadership by JW. Henry Lambright

Distance Work Arrangements: The Workplace of the Future Is Now by John Kamensky, Emily G. Craig, Michaela Drust, Dr. Sheri I. Fields, Lawrence Tobin

Preparing the Next Generation of Federal Leaders: Agency-Based Leadership Development Programs by Gordon Abner, Jenny Knowles Morrison, James Perry, Bill Valdez

Risk

The Rise of the Sustainable Enterprise by Wayne S. Balta, Jacob Dencik, Daniel C. Esty, Scott Fulton

Managing Cybersecurity Risk in Government by Anupam Kumar, James Haddow, Rajni Goel

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.

IBM Center for The Business of Government