IBM Center for The Business of Government

2023

Strengthening the Future of the AUKUS Partnership

Michael Cohen
National Security College,
Crawford School of Public Policy,
Australian National University

Chris Nott
Global Chief Technology Officer
Defence & Security, IBM

25TH ANNIVERSARY
IBM Center for
The Business
of Government

Strengthening the Future of the AUKUS Partnership

Preface by **Michael Cohen**

National Security College, Crawford School of Public Policy,
Australian National University

Report by **Chris Nott**

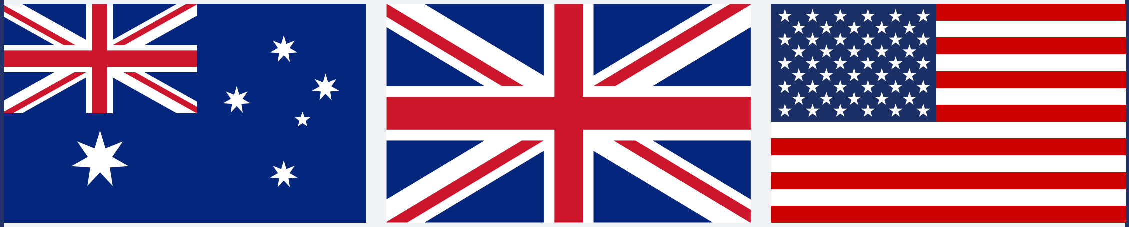
Global Chief Technology Officer
Defence & Security, IBM

SEPTEMBER 2023

IBM Center for
The Business
of Government

Table of Contents

AUKUS



Foreword

Daniel J. Chenok

On behalf of the IBM Center for The Business of Government, we are pleased to release this new report, *Strengthening the Future of the AUKUS Partnership,* by Michael Cohen with the National Security College of Australian National University, and Chris Nott, IBM global chief technology officer for Defence and Security.

This new report addresses how best to collaborate across government and industry among the three AUKUS nations—Australia, the United Kingdom, and the United States—in order to implement this historically important security agreement effectively. The authors focus specifically on how AUKUS stakeholders can leverage technology and innovation, from cloud computing and cybersecurity to artificial intelligence and quantum computing, to establish a sustainable and enduring strategy that enhances security, especially across the Indo-Pacific region.

The authors' work complements our Center's ongoing focus on how best to manage major global initiatives that promote security interests across nations. This includes our recent series of reports on visualizing information operations in defense settings with the Institute for the Study of War, as well as two recent reports on how Australian agencies are providing a model for other nations on how AI and emerging technologies can be implemented in a way that builds public trust.

We hope that AUKUS leaders and stakeholders find this report helpful in framing innovation that drives the path forward for implementing this vital partnership.

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

Preface

New threats and domains for warfare continually emerge. These include cyber and space along with disruptive technologies like artificial intelligence (AI) and quantum. Dealing with these threats necessitates an enhanced partnership across governments and within industry.

Achieving full mission readiness is becoming increasingly complex and requires dynamic defence technology solutions. Securing and protecting people, nations, and information is impacted by a multitude of challenges including COVID-19, climate change, and an increasingly hostile edge to global strategic competition.

On 15 September 2021, the leaders of Australia, the United Kingdom (UK), and the United States (U.S.) jointly announced the AUKUS partnership. They resolved to "deepen diplomatic, security, and defence cooperation in the Indo-Pacific region to meet the challenges of the 21st century."

Many would identify these three nations as partners in the strongest interstate alliances in existence today. The creation of AUKUS to help equip Australia with nuclear powered submarines and other technological upgrades should increase the already strong foundations that Australia, United Kingdom, and United States share.

To deter threats from China and defend allied interests throughout the Indo-Pacific, the U.S., UK, and Australia therefore require strong military strategy coordination processes and more operational regional and contingency planning mechanisms. To deter and defend against the full spectrum of threats in the region, the AUKUS partners need to develop integrated and combined approaches to these challenges. A recent report from Ashley Townshend and David Santoro[1] concluded that "the United States and Australia should gradually pursue collective deterrence goals by co-developing new warfighting concepts, enhancing technological development and experimentation, and advancing combined capability, interoperability, and force posture objectives." Increasingly sophisticated and resilient information sharing mechanisms will come to loom increasingly large in this mix.

Regarding AUKUS, most attention has focused on the Pillar 1 provision of nuclear powered submarines, but the spate of Pillar 2 technology and related components will be realised much earlier and "used" more frequently. How Washington, London, and Canberra go about conceptualisation, implementation, and data management will determine how they meet this challenge.

The AUKUS partners will face an unprecedented set of challenges and must find new and creative solutions to old and emerging problems. High technology bifurcation and decoupling between China and its partners and customers from the G7 and Quadrilateral Security Dialogue presents a need for new information access techniques and specific technological and knowledge solutions. AUKUS presents many opportunities to do this.

Putting information at the heart of decision making and collaboration offers important opportunities to meet these challenges. The post-9/11 homeland security agenda expanded intelligence sharing to also include counter-terrorism and countering violent extremism, cybercrime, encryption, and foreign investment in critical infrastructure.

[1] https://ipdefenseforum.com/2021/02/operationalizing-deterrence-in-the-indo-pacific/.

Meeting Challenges

Today, however, the AUKUS partners will have to meet the challenges ahead regarding undersea capabilities, quantum technologies, AI and autonomy, advanced cyber, hypersonic and counter hypersonic capabilities, electronic warfare, and further innovation.

What is needed, as Priya Chacko and Jeffrey Wilson[2] pointed out, are "functional cooperation programs in areas where the governments share both outlook and interests." Regarding AI, AUKUS partners need to continue discussing legal and oversight frameworks and potential future uses.

The AUKUS partners will need to develop and foster trilateral initiatives to pool research and development of leading-edge capabilities. As Rory Medcalf and Veerle Nouwens[3] have pointed out, this could also involve bilateral pilot programs in AI, quantum computing, new submarine detection technologies and/or unmanned underwater vehicles to galvanise trilateral AUKUS cooperation.

Sharing confidential sensitive cybersecurity intelligence raises challenges for organizations and states that stem from technological, organizational, institutional, and social challenges. Effective sharing of cybersecurity intelligence may therefore require the adoption of new technologies, and the development and implementation of organizational processes and new methodological applications or at least approaches to common problems.

This will likely require new infrastructure, tools, and technical elements to generate, consume, and share cybersecurity intelligence.[4] States and organizations need to strike a balance between leveraging and utilising their extant systems, processes, and technologies, and adapting and refining these to new and over the horizon threats and models.

[2] https://perthusasia.edu.au/getattachment/Our-Work/Australia,-Japan-and-India-A-trilateral-coalition/PU-175-AJI-Book-WEB(2).pdf.aspx?lang=en-AU.

[3] https://nsc.crawford.anu.edu.au/publication/19833/australia-and-united-kingdom-indo-pacific-security-agenda-revitalised-partnership.

[4] Kolini and Janczewski, https://aisel.aisnet.org/cais/vol50/iss1/2/.

Regarding technology, signature-based anomaly detection capabilities such as firewalls, proxies, and anti-malware fail to provide reliable detection or protection against new zero-day vulnerabilities that use multi-vector and multistage methods.[5] Active and effective sharing in effective cybersecurity intelligence offers cyberspace situational awareness and increases the probability that earlier successful adversary techniques and strategies will be less effective over time.

High quality and actionable cybersecurity intelligence tends to reduce uncertainty in cyberspace operations and looms large in effective cybersecurity intelligence sharing. The provision of such reliable and superior cybersecurity intelligence from more experienced organizations and government agencies can also incentivise less resourced and experienced organizations to participate in such intelligence sharing initiatives.[6]

Cybersecurity intelligence operational complexity related to data volume and variety, quality, intelligence enrichment difficulties, and automation complexities can also impede success. The challenge here is scaling and integrating different intelligence sources. Interoperability between cybersecurity intelligence platforms improves network quality and provides more reliable and timely intelligence. Given the different resources and foci of the AUKUS partners, much work is required to streamline these processes.

Organizational factors also offer robust and durable processes and procedures to create, consume, and/or share cybersecurity intelligence. Organizations and states operate in an increasingly interconnected environment where ultimate performance increasingly depends on cooperation with and success of others. Weaker or absent network nodes can increase the vulnerability of the network. Organizations orientations to collaborative cybersecurity intelligence will depend on which organizations have and have not already committed to participate. Organizations require confidence in interest convergence over the short and long run, and this may require scalable gains in cooperation between the AUKUS partners.

Collaboration Underpins Success

AUKUS partners need to build on the September 2022 Five Partners Ministerial commitment to contribute a whole-of-society effort to this endeavour with the private sector as a critical partner to strengthen collaboration on global, values-based data security within democratic frameworks. A continuous expansion of joint efforts to counter cybersecurity threats and ensure the security and resilience of emerging technologies and critical infrastructure and improve public awareness is required. This includes the implementation of domestic legislation on mandatory incident reporting.

Partners need to continue to develop and share lessons learned from “acute, emerging and chronic crises” to collectively improve resilience. As Five Eyes Law Enforcement Group Commissioner Reece Kershaw stated in May 2023, “We must be unapologetically proactive and innovative in how we identify and disrupt threats.” As National Crime Agency (NCA) Director Graeme Biggar stated, “We must continue to share information, intelligence, and best practices, enabling us to keep pace with the criminals and the technology they use to stay one step ahead of them both domestically and internationally.”[7]

[5] Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security.

[6] Robinson, N., & Disley, E. (2012). Incentives and challenges for information sharing in the context of network and information security. ENISA. Retrieved from https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing.

[7] https://www.acic.gov.au/media-centre/media-releases-and-statements/five-eyes-law-enforcement-group-meets-australia-combat-serious-crime.

Partners need to consolidate and create new forums for sharing ideas and consolidating harmonisation, extending research and development capabilities at reduced cost, minimising duplication, and strengthening interoperability.

It is vital that industry contributes to the goals and aspirations of AUKUS and its partners. Global public-private partnerships, built in a collaborative fashion and using company footprints in each of the partner countries, will underpin the success of the agreement. Ranging from the obvious to the subtle, there are three key pathways where support is needed:

1. **Knowledge Sharing.** At one level this is a simple case of raising awareness of programs delivered to each partner; at another level, it requires the removal of barriers that limit the transfer of that same work.

2. **Growth of Sovereign Capabilities.** Access to global supply chains is one aspect, but greater efficiencies may be gained by building industry capability to meet sovereign needs.

3. **Workforce Allocation.** Linked to sovereign capability, the ability to move talent between partner countries to improve the speed of technological innovation is vital.

In combination, these pathways will not only improve regional security—they can also drive transformational change across the partners' economies.

These challenges are substantial. AUKUS partners require decision superiority, systems commonality, innovation pull through, industry collaboration and skill building in undersea capabilities, quantum technologies, AI and autonomy, advanced cyber, hypersonic and counter hypersonic capabilities, electronic warfare, innovation, and information sharing. This report details how the AUKUS partners can best proceed to meet this spate of challenges.

Introduction

On September 15, 2021, the leaders of Australia, the United Kingdom (UK) and United States (U.S.) announced the creation of an enhanced trilateral security partnership called "AUKUS." The agreement committed the parties to significantly deepen cooperation on a range of security and defence capabilities to be achieved through deeper integration of security and defence-related science, technology, industrial bases, and supply chains.

The first pillar of the partnership is a UK-U.S. commitment to provide Australia with conventionally armed, nuclear-powered submarines. The three governments of Australia, the United Kingdom, and the United States announced more details for this pillar in March 2023.

The second pillar of eight advanced capabilities in the AUKUS partnership was laid out by the three governments in April 2022. This intent is oriented to providing capability that promotes security and stability in the Indo-Pacific region. This second pillar is the focus of this paper.

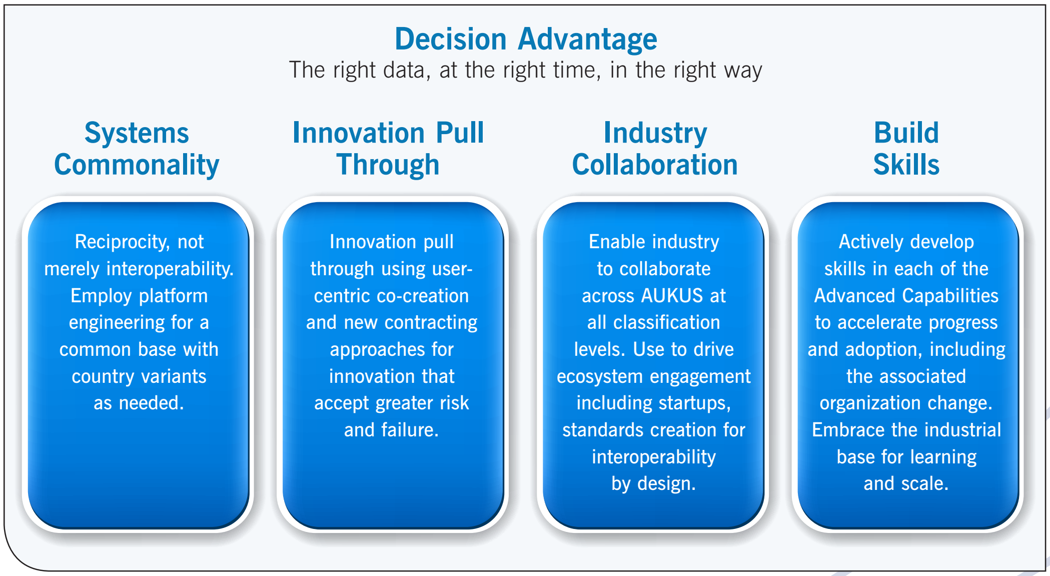
Beyond the enhanced security posture, there are substantial benefits to all three nations in combining the effort and resources of industry to accelerate innovation and adoption of these advanced capabilities. Sovereign requirements drive demand for new capability within the AUKUS nations. Nevertheless, the acceleration of innovation in emerging technologies offers widespread crossover opportunities benefitting other sectors, and more high value technical skills can raise economic productivity.

Overarching Imperatives

To achieve the core and secondary benefits of AUKUS, three imperatives—guided by an overarching principle of *powering decision advantage*—can accelerate adoption of the advanced capabilities.

- **Put data at the heart of decision making—**Put data assets, products, open industry standards, and sharing, including AI and machine learning (ML) models, across the AUKUS partnership at the heart of decision making while respecting data sovereignty.
- **Accelerated innovation and pull-through with deeper digital collaboration and skill development—**Strengthen individual nation efforts through collaboration and adoption of a digital ecosystem mindset, supported by commercial efforts and the coordination of AUKUS-wide exploitation and acceleration. AUKUS partners also need to make the defence and security technology sectors highly attractive as a career choice.
- **Harness and enable the AUKUS-wide industrial ecosystem—**Bolster and track existing and new investments by industry in leading technology advances. Reinforce existing AUKUS-wide industry structures and relationships, and identify and remove inhibitors to market growth.

Figure 1: Putting Data at the Heart of Achieving a Free and Open Indo-Pacific



Decision Advantage

The right data, at the right time, in the right way

Systems Commonality

Reciprocity, not merely interoperability. Employ platform engineering for a common base with country variants as needed.

Innovation Pull Through

Innovation pull through using user-centric co-creation and new contracting approaches for innovation that accept greater risk and failure.

Industry Collaboration

Enable industry to collaborate across AUKUS at all classification levels. Use to drive ecosystem engagement including startups, standards creation for interoperability by design.

Build Skills

Actively develop skills in each of the Advanced Capabilities to accelerate progress and adoption, including the associated organization change. Embrace the industrial base for learning and scale.

Powering Decision Advantage. Putting data at the heart of the AUKUS adoption of advanced capabilities is essential to achieving a free and open Indo-Pacific. Decision advantages can be sustained by exploiting unused data via data fabric endeavours across the three AUKUS nations and their partners.

Sound data management and governance is an essential foundation to the successful and responsible use of AI and automation. These efforts will need to recognise sovereign ownership and control of data, which necessitate appropriate frameworks, controls, and governance that enable effective sharing. The three imperatives discussed above reinforce how success will be achieved, implemented through the elements shown in Figure 1 and addressed further below.

Systems Commonality. Many standardisation efforts between nations and across NATO today facilitate interoperability. Indeed, open standards and architectures bring this benefit in the technology industry in general. AUKUS provides an avenue to achieve more by enabling reciprocal adoption of each other's systems without any reduction in security. This increases harmonisation of capabilities across the nations while platform engineering approaches allow nation customisation on reusable core functionality.

Innovation Pull-Through. User-centric, co-creation approaches increase the successful deployment of innovation. This requires strong representation and commitment by stakeholders for those who will make active operational use of the advanced capabilities. Users must directly participate rather than only by proxy. Contracting needs to be redesigned for innovation in ways that encourage experimentation and tolerate risk, failure, and learning. Development using advanced technologies is quite unlike acquisition of equipment, and is much more akin to digital ecosystem processes.

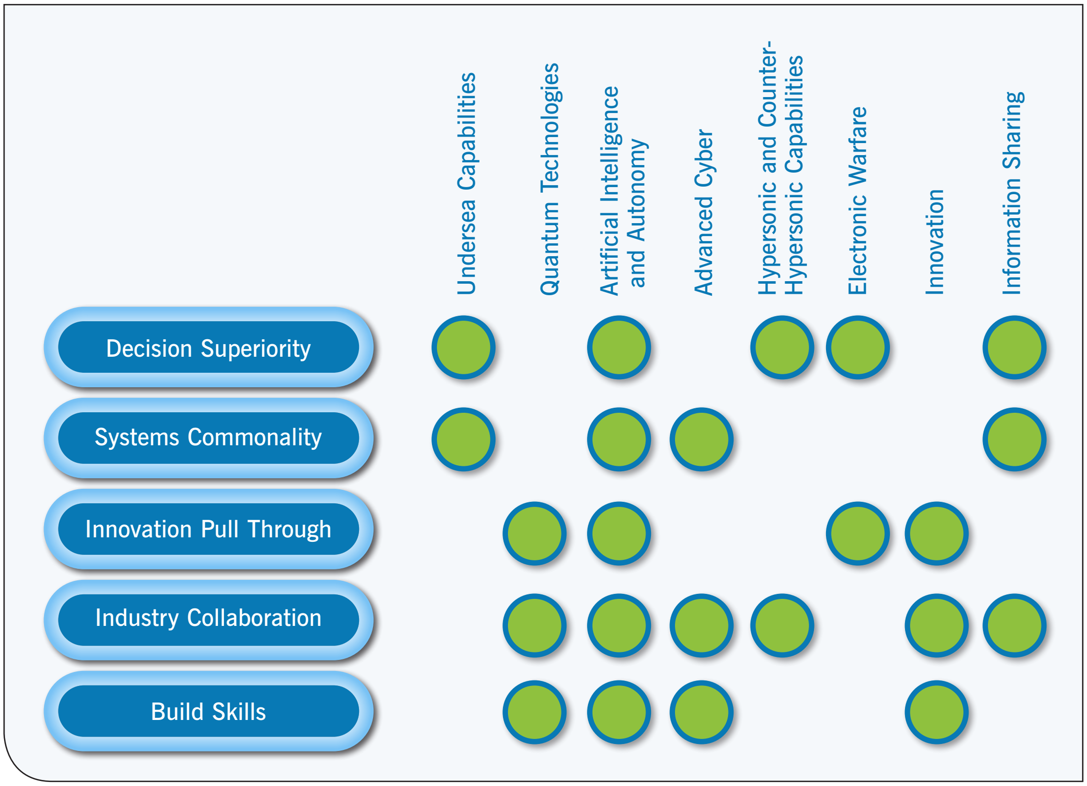
Industry Collaboration. Each AUKUS nation's defence agencies are fortunate to have an ecosystem of industry partners built around trust, credibility, and capability. AUKUS provides an opportunity to assess and augment both the span and scope of these ecosystems with technology partners who are digitally native, ecosystem minded, collaborative, and fast to evolve. AUKUS nations can also take meaningful steps to allow industry to more easily collaborate, share, and exchange assets and capability in support of the advanced capabilities between subsidiaries in the three nations. This important evolution in culture to share within defined guard rails can strengthen industry's support of the AUKUS partnership's goals.

Build Skills. The three nations of the AUKUS partnership can take active steps to build skills in advanced capabilities. These are required for research, innovation, experimentation, and learning, as well as adoption and deployment. Adoption includes associated organisational change to maximise value from the capabilities. Defence agencies can engage with their industrial bases to help with learning and building capacity with countries. There is a scarcity in many fields today and that talent can achieve more by moving between the nations.

Advanced Capabilities

Each AUKUS advanced capability maps on to the guiding themes in support of the imperatives. Understanding this mapping allows the first key step in knowledge sharing—what can be offered in support of AUKUS outcomes as shown in Figure 2.

Figure 2: AUKUS Advanced Capability Map



	Undersea Capabilities	Quantum Technologies	Artificial Intelligence and Autonomy	Advanced Cyber	Hypersonic and Counter-Hypersonic Capabilities	Electronic Warfare	Innovation	Information Sharing
Decision Superiority	●		●		●	●		●
Systems Commonality	●		●	●				●
Innovation Pull Through		●	●			●	●	
Industry Collaboration		●	●	●	●		●	●
Build Skills		●	●	●			●	

Undersea Capabilities

Harnessing data through interoperability across multiple platforms and operational systems is necessary for AUKUS to achieve the advantage offered by autonomous underwater vehicles as a force multiplier. Furthermore, AUKUS can ensure that flexibility is built into the vehicles themselves to re-task and update functionality, including deployed AI to suit changing conditions while adhering to navigation rules.

UK defence is leading efforts across the AUKUS nations to provide data services for remote and autonomous systems. This employs techniques, blueprints, and technology to integrate sensor data from across various platforms to increase situational awareness and improve vehicle performance. A data fabric can provide these data services as part of this effort.

This follows Australia's demonstration of open architectures and industry standards in Autonomous Warrior 22, with an implementation of a data fabric independent of platform providers. A data fabric offers real-time insights for decision advantage.

U.S. defence and some equipment providers are also making use of data fabric services to sustain and improve mission readiness and capability of vehicles. Implementations are optimising maintenance and supporting engineering resources as part of managing deployable assets. Greater platform reliability also protects their equity.

In 2022, the Mayflower Autonomous Ship successfully navigated the Atlantic from Plymouth in the UK, one AUKUS nation, to Plymouth in the U.S., another AUKUS nation. Artificial intelligence and machine learning algorithms, together with decision optimisation technology, provided the ship's real-time monitoring and decision-making capabilities. Several nations are actively exploring the application of this technology in defence. This includes experimentation in the U.S.

Many defence departments are standardising the application platform to run on any public or private cloud service and on premises, and from headquarters to the edge. The UK MOD is adopting open source technology to achieve this for its Defence DevSecOps Service (D2S). Recent advances have shown application containers scaling down, thereby opening up opportunities for defence at the tactical and disconnected edge. In addition, defence recognises that technology helps address the challenge of managing edge applications that scale across thousands of deployed platforms.

Open standards enable agility through interoperability. Many industry forums and consortia exist, such as OSDU (Open Subsurface Data Universe), SOSA (Sensor Open Systems Architecture), and trusted technology forums. Most significantly, FACE (Future Airborne Capability Environment) is developing vendor-neutral open standards to enable software portability, reusability, and interoperability in not only U.S. military avionics, but increasingly, maritime and land theatres. As of 2022, it was open to Australia, Canada, New Zealand, and UK.

Quantum Technologies

AUKUS will need to build quantum fluency to fully exploit the opportunities offered by quantum technologies. This is a combination of organisation and skills. For example, AUKUS can take steps to develop skills for quantum computing that are accessible to developers and data scientists with the tools and languages they use today.

The AUKUS partnership can begin building skills and hands-on experience in quantum computing today. Open-source software development kits with runtime services allow developers to use quantum with the same tools, languages, and code that they are using for classical computing. Extensive training and education programmes also exist. Much content is freely available. This is helping to make the adoption of this radical new technology as frictionless as possible, and engendering a new generation of quantum-literate developers.

The AUKUS nations can take further advantage of expertise in quantum computing with a quantum accelerator. Such a strategy can help the AUKUS partnership set priorities and identify new opportunities, which allows quantum teams to develop skills needed to build quantum fluency and provides direct access to the most advanced quantum systems.

Quantum computing also offers the opportunity for much faster ‘time to answer’ in the context of running complex algorithms with many dimensions. The pace of operations will only increase as data vital for timely and accurate decision making becomes both more available.

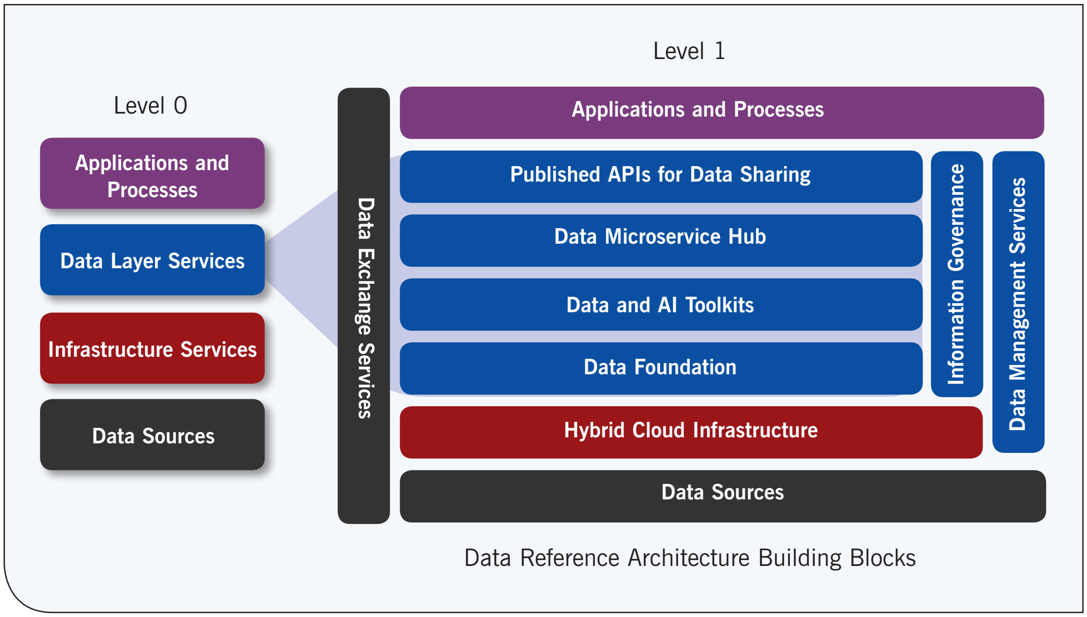
Finally, the opportunity that quantum computing offers also presents a challenge. Factoring algorithms are likely to be viable at scale on future “cryptographically relevant” quantum computers, posing major risks to encryption methods used in many current systems and communications. Quantum safe cryptography is addressed in the advanced cyber capability below.

AI and Autonomy

Successful use of AI is underpinned by sound data management and governance. Their absence presents risks to coherence, accuracy, reliability, and trustworthiness. AUKUS can take steps to facilitate data access through services, expose data lineage, and constantly monitor the performance of AI against goals when developing algorithms and through their operational lifetime. In addition, success requires exploiting data assets to improve systems resilience and mission capability. These together will help AUKUS build trust and confidence in the insights and behaviours afforded by such capabilities.

The UK Ministry of Defence published its data strategy in 2021, which forms part of the wider digital transformation for multi-domain integration to sustain decision advantage. The MOD data reference architecture provides a foundation for data management and governance within its strategy. This is shown in Figure 3 and offers the basis for consuming new data sources, easier access, and use of data, AI, and greater trust.

Figure 3: Data Reference Architecture Building Blocks



All three nations have been deploying data fabric. For example, the UK MOD has been using it on implementations of its strategy. This has included building a data factory on top of the data fabric to streamline the process of setting up and running data pipelines to ingest new data sources. It is underpinned by a catalogue that describes the data for ease of use while helping implement governance controls. UK MOD is now using these data pipelines to validate its data governance model and to help educate personnel with responsibility for data. Both are key to powering decision advantage.

This approach is being used by UK MOD to deliver data as a service for remote and autonomous systems. The open architecture avoids the pitfalls of approaches that have adopted a single, proprietary product. Furthermore, the architecture and data services APIs are reusable across the AUKUS partnership to promote cross-compatibility.

The use of AI with data fabric technology is enabling AUKUS to enhance situational awareness and improve the speed and accuracy of decision-making processes. Advanced machine learning algorithms in the data fabric accelerate the preparation of data for use and aid enrichment, and the identification of patterns and trends.

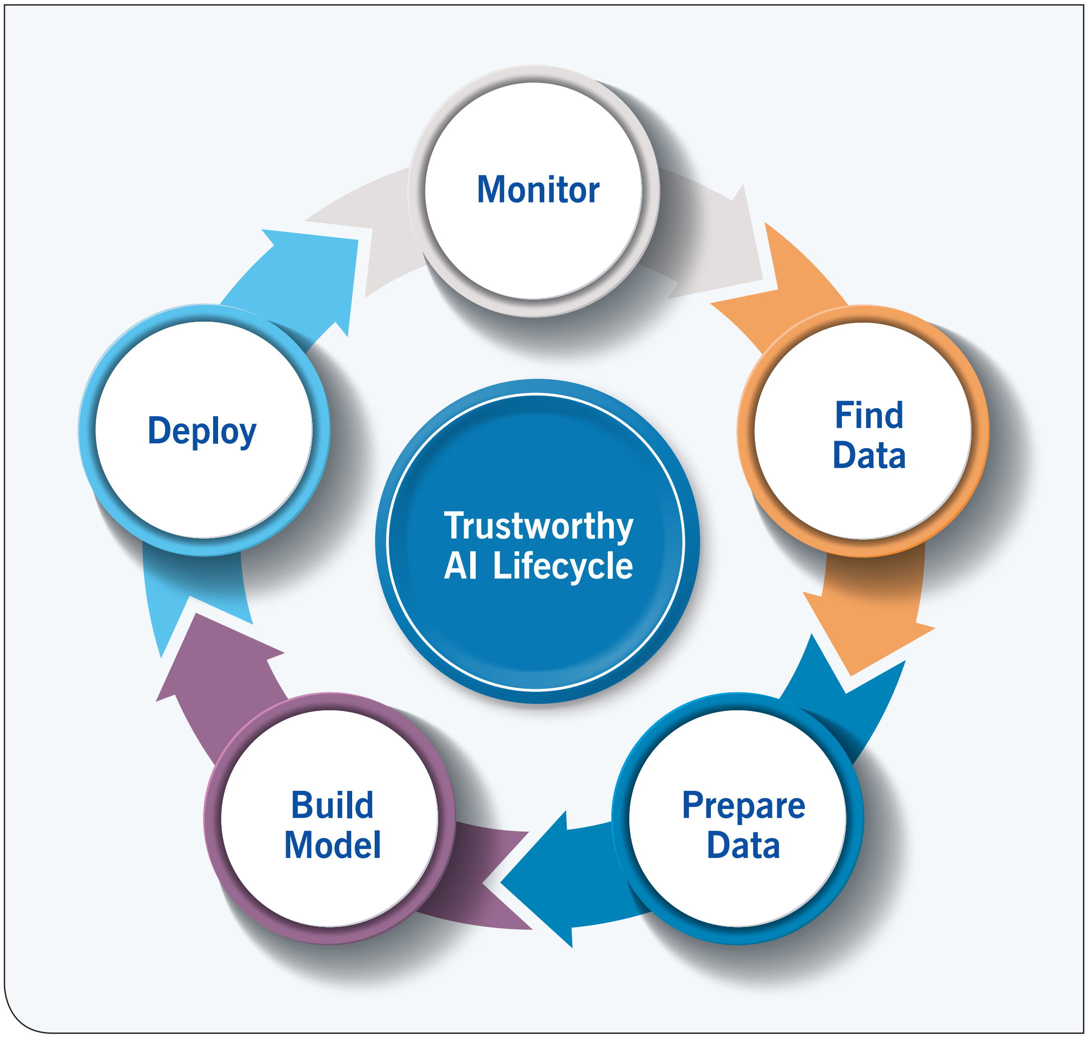
The UK MOD delivered its first operational deployment of AI with operation SPRING STORM in Estonia: AI on the tactical edge. AI is used to provide insights from open source and MOD data. It removes the cognitive burden of data processing on the human being and transfers it to the computer system to speed up and optimize decision making.

With the recent emergence of generative AI, considerable effort must be made to harness the power of this technology in the form of military function and specific Large Language Models (LLMs)—including understanding of the provenance for both the algorithm and the training data and methods—and then to apply the technology throughout the staff functions as they seek to “Prepare, Generate, Deploy, Operate, Sustain, Protect and Recover” force elements. A combined approach to determining where and how generative AI can deliver real value to the defence enterprise would serve to cohere the three nations both in physical technology and in concepts underlying military operations in the 21st century.

AUKUS nations can work with industry to build out the exploitation of open source intelligence with a minimum viable product (MVP) for multidomain operations that augments real data with synthetic data, employs AI to make recommendations to assist decision making in command, and utilises modelling and simulation tools from the defence ecosystem to evaluation courses of action. The real power of this MVP lies in its integrated workflow. This enables efficient management of the intelligence requirements management process.

Nevertheless, use of AI only endures if confidence is sustained. Trustworthy AI can be achieved using MLOps (Machine Learning continuous development Operations see Figure 4). This builds users' confidence in the AI and machine learning behind the results and recommendations they see; the data, technology, and algorithms being used assist and augment decision making through transparency, explainability, and monitoring.

Figure 4: Trustworthy AI Using MLOps (Machine Learning continuous development Operations)



In a recent collaboration, AI algorithms were updated on a UAS (unmanned aerial system) in flight from detecting a target emitter to recognition, thereby enhancing situational awareness with better ISR data. This is an example of dynamically managing AI algorithms on deployed assets.

In the undersea capabilities section above, several defence departments and equipment manufacturers used data for mission readiness. This includes drones and UAVs. Defence agencies are using data fabric technology and data science tools to optimise the use of engineering resources and cost. More generally, the integration of AI into existing systems and processes drives automation that enhances their performance.

The AUKUS nations can harness the power of data and AI technologies to improve their capabilities, sustain the resilience of their autonomous and AI-enabled systems, respond to emerging threats, and maintain advantage in a rapidly evolving environment.

Advanced Cyber

AUKUS nations can adopt zero trust and increase their cyber technical skills. In parallel, AUKUS should prioritise the implementation of quantum-safe cryptography in today's systems which will be operational in the medium term, as well as future capability. This will necessitate a review of risk, deployed cryptography, and architectures.

Scarcity of cyber skills is a challenge across our industry. UK Defence has successfully run cyber aptitude testing to identify those who can most easily reskill to pursue a new career in this field. Recognised industry standard digital-skills education and training platforms (such as at https://skillsbuild.org) could be adopted to accelerate the raising of baseline knowledge and competence in key cyber disciplines.

The AUKUS nations have been taking steps to increase security and resilience of critical infrastructure. Defence in depth and zero trust approaches can help protect systems and networks. In addition, technologies and practices can be employed to protect data so that once attacked, priority operations can be quickly resumed.

Defence departments are keen to detect unknown actors on deployed networks and capability for radio frequency device identification from signatures.

Despite this, a major and current challenge facing the AUKUS nations is making systems and networks quantum safe. Quantum computing offers the potential in the not-too-distant future to find the prime factors of large integers used for encryption keys. This presents considerable risks to our data today. Attackers will be able to:

1. Harvest data today and decrypt it later by cracking encryption keys (if they are able to access future, cryptographically relevant quantum computers)

2. Gain access to critical infrastructure through fraudulent authentication

3. Manipulate legal history by forging digital signatures

Quantum safe cryptography is needed. The National Institute of Standards and Technology (NIST) announced the first algorithms for protocol standardization consideration in July 2022 (with intent to publish formal standards in 2024). Furthermore, the U.S. National Security Agency (NSA) announced a new Commercial National Security Algorithm Suite (CNSA) 2.0 in September 2022. Goals for U.S. National Security Systems to transition to quantum-resistant algorithms to be CNSA 2.0 compliant for software, firmware, and cloud services have been set for 2025 and 2033.

The AUKUS nations can follow emerging quantum safe roadmaps to help them understand the risks to their systems and improve cryptographic governance, take steps to design better ways to consume cryptography, and simplify the migration to new quantum-safe cryptography.

Hypersonic and Counter-Hypersonic Capabilities

AUKUS can benefit from advances derived from scientific research conducted on high performance computing. Progress can result from improvements in algorithms as well as increasing scalability of systems.

The UK MOD's new Hypersonic Technologies and Capability Development Framework is specifically designed to bridge the gap between relevant research and development and useable capability. While still in its infancy, the Lot structure proposed under the framework emphasises the importance of a whole-of-industry effort to accelerate capability development. Key areas for support include:

Design and Integration—High-power and perhaps quantum computing to enable quicker time to value for the solutions to the numerous extant physics challenges. Hypersonics require and generate huge volumes of data. When coupled with the anticipated diversity and dispersion of the supply base, the need for effective data management and governance to enable timely and accurate decision making is significant.

Modelling, Simulation, Test, and Evaluation—The demand for high-power and perhaps quantum computing to enable more and more complex models to be built and scenarios to be simulated. Quantum computing can be applied to modelling acute engineering problems found in the aerospace industry.

Onboard Computing—High speed data buses which connect sensors, decision makers and effecters with extremely low latency are anticipated to be useful. The increased adoption of industry and open standards for data exchange will also be a key enabler.

Electronic Warfare

AUKUS will benefit from large scale data management and governance to derive insights across data sources including sensors, and apply advanced analytics and AI to identify signals and optimise spectrum usage. Such an approach helps AUKUS build trust in data exploitation.

The AUKUS nations will need to handle large volumes of data coming off sensors with a data platform to fulfill this capability. The data fabric described earlier in this paper is such a foundation for analytics and AI. It can be used to facilitate sharing, enhance situational awareness, recognise electronic signatures, improve electromagnetic spectrum management, and optimise its use. Robust workflows that are tightly integrated into data management systems will enable accurate and timely execution of decisions on spectrum management, and the effective continuity of key communications under sustained electronic attack.

Capabilities in this area are particularly sensitive. The UK has already demonstrated speed proficiency by quickly developing and maintaining applications for sensitive domains in less sensitive environments. Such an approach also widens access in the AUKUS partnership to the technology skills in the industry. Accredited implementations of techniques, technologies and automation with DevSecOps across security boundaries exist today. They verify components developed on the low-side for running in sensitive environments.

Innovation Through Collaboration

Strong leadership and sponsorship within the AUKUS partnership is a critical success factor for innovation. AUKUS can employ techniques and procurement approaches that have been shown to encourage and exploit innovation successfully. One contributing factor is taking a user-centric approach to co-creation by defence and industry. The research and innovation portfolio should be managed across AUKUS to embrace small and medium enterprises (SMEs), industry, academia, and defence, which should enable all to focus resources on high priority warfighting needs.

All three AUKUS nations have successfully delivered capability using military design thinking, to adopt new technologies and innovative approaches. The method takes a user-centric approach to co-creating minimum viable products. This is a quick way of deploying new capability, assessing value, and iteratively building out.

The International Technology Alliance in Distributed Analytics and Information Sciences (DAIS-ITA) is a collaborative partnership between the U.S. Army and the UK Ministry of Defence. It brings together researchers from U.S. Army Research Laboratories (ARL) and the UK Defence Science & Technology Laboratory (Dstl) to work alongside a consortium of universities and industrial research laboratories in U.S. and UK. The goal of the alliance is to foster collaborative fundamental research in both nations to enable secure, dynamic semantically aware distributed analytics for situational understanding in coalition operations. The DAIS-ITA consortium has operated for ten years, resulting in major research and development operations in both nations. Such an approach could be extended to AUKUS.

UK Defence has embraced novel contracting which specifically enables innovation: being descriptive rather than prescriptive in its approach. Defence has recently contracted its second programme in this way, based on the success of the first. This second programme has demonstrated a frictionless way to gather data from edge devices via a lightweight API into a data fabric. The focus is avoiding data loss in demanding operational situations. This is an important example of rapid experimentation to learn and advance.

The Mission Technology Integrator (MTI) model can integrate capabilities from SMEs for specific defence department challenges. Defence has successfully proven the value of several SME solutions using MTI. Again, this is a model that can be replicated.

The Mission Technology Integrator (MTI) model has proven the value of being mission led and integrating capabilities from SMEs into mission critical enterprise systems. In addition, the MTI model has driven solutions to business process related issues, like pace of onboarding into primes' approved procurement systems and the equitable handling and exploitation of IP. Defence agencies have successfully proven the value of several SME solutions using MTI. This model can be replicated and its impact amplified if coordinated with government innovation bodies such as the UK's Defence Innovation Unit and National Security Strategic Investment Fund.

Defence has been able to demonstrate an eight-times speed advantage in low-side innovation development versus high side using DevSecOps across security boundaries described in the previous section. It allows access to wider specialised skills and enables innovation to be pulled through faster.

As a parallel industrial example, the Open Group OSDU Forum delivers an open source, standards-based, technology-agnostic data platform for the energy industry that stimulates innovation, industrialises data management, and reduces time to market for new solutions.

This common data platform, which has an open source, cloud-native, subsurface reference architecture, is being used for energy industry collaboration, with usable common implementations across industry.

Other areas for the effective management of an innovation portfolio that spans the three nations' defence and technology industrial bases include the creation of focal coordination point offices in each nation's defence agency, reinforcing innovation offices that already exist and encouraging defence and technology industry partners with tri-nation presence to establish equivalent functions. Another opportunity to accelerate innovation involves leveraging the presence and expand the roles of nonprofit organisations such as Armed Forces Communications & Electronics Association International (AFCEA), which already contributes significantly to government, defence, industry, and academia collaboration in the U.S. and UK.

Collectively, these are examples of managing a mission-led innovation portfolio for AUKUS using a federated approach which embraces the defence ecosystem, SMEs, and academia. AUKUS would be able to accelerate defence innovation, foster collaboration, and quickly integrate commercial technologies to fulfill the partnership's warfighting needs.

Information Sharing Across the Industrial Ecosystem

As well as improving the sharing of information across the defence departments of AUKUS, the partnership should facilitate corresponding mechanisms for national industry sectors. AUKUS can define parameters that facilitate collaboration and reuse by industry across nations that help support and accelerate the adoption of advanced capability by the AUKUS partnership.

The AUKUS partnership should enable interoperability in industry and establish a common information sharing platform.

The partnership can benefit from collective access to industry skills from across the three AUKUS nations. Sharing expertise would help accelerate innovation and the adoption of advanced capabilities by allowing nations to take advantage of learning from one country in another as a minimum. While largely internal to industry, this is dependent on the governments enabling industrial interoperability. This includes allowing infrastructure and industry practice collaboration across the AUKUS partners at all levels of classification.

The current regulatory and export environment inhibits collaboration. Furthermore, opportunities may be lost due to an aversion to sharing information. Information sharing between nations depends on trust, security, and good governance. Coherence regarding how information sharing is implemented in terms of processes and supporting technology can help manage risk. A concept of 'share by design' could be applied to specific subjects that would unlock greater potential and increase the pace of speed to value from collaboration.

As an example of an enabling technology platform, consider a secure, EAL 5+ accredited system with KYOK (keep your own key). This infrastructure is protected with technical assurance rather than operational assurance. The keys are protected with a FIPS 140-2 Level 4 HSM (hardware security module) that allows compartmentalised Linux workloads to run on a single platform. This LinuxONE platform could be deployed in each nation to form the basis of secure infrastructure for information sharing across the AUKUS partnership and its defence ecosystem.

The LinuxONE platform is augmented by fully homomorphic encryption (FHE), a quantum safe type of encryption that allows data to remain encrypted even during computations. This makes it more secure than traditional encryption methods and protected against future cryptographically relevant quantum computers. Sensitive data can thus be shared and used for analytics without being decrypted and becoming vulnerable to human or cyber threats.

It is vital that the AUKUS partnership takes an architected approach to major transformation and ensures that the intended commonality of systems and industrial collaboration can be realised in deployment. A professional architected approach can ensure that good design intent is supported by architectural governance and design authorities. Such discipline is assured through professional certification and proven methods.

In addition, for both innovation and information sharing, industry would benefit from AUKUS enabling more collaboration, sharing, and reuse across sectors in the three AUKUS partners. This should consider parameters for information sharing and capability exchange as well as supporting infrastructure and mutual recognition of security clearances. It should also take account of the dynamic between information sharing and sovereign control of data. This would allow industry to better help accelerate adoption of the advanced capabilities prioritised in the AUKUS partnership.

Conclusion

The activity and needs of AUKUS show a strong alignment with hybrid cloud as an open, scalable, and highly flexible enabling platform for applications coupled with AI. This is woven through most of the AUKUS partnership’s advanced capabilities for innovation, insights, and automation. AUKUS nations can and should look to the future with quantum computing, enabling industry to reap the benefits of potential opportunities while offering practical action to address today’s risks.

Industry already has many implementations of the technologies in the scope of several of the advanced capabilities. This offers opportunity for reuse and exploitation across the AUKUS partnership to raise overall capacity and effectiveness.

Recommendations

This report concludes with the following recommends to the AUKUS partnership for consideration.

1. Adopt military design thinking to accelerate innovation and adoption of new capabilities. This user-centric approach to co-creation has shown a high success rate in defence.

2. Align a research portfolio to the AUKUS partnership's needs via a consortium that encompasses government, industry, and academic partners.

3. Facilitate technology sharing and reciprocity of capability across the AUKUS partnership, potentially to include exploring a reform of export controls.

4. Provide the capabilities and permission for industrial collaboration across the AUKUS nations at all levels of classification.

5. Speed up the security clearance process for experts in advanced capabilities in the three nations and promote cross-recognition of those clearances across the AUKUS partnership and its industrial ecosystem.

6. Establish an AUKUS quantum-safe crypto working group.

About the Authors

Michael Cohen

Michael Cohen is senior lecturer at the National Security College, Crawford School of Public Policy, Australian National University. He is the author of *When Proliferation Causes Peace: The Psychology of Nuclear Crises* (Georgetown UP: 2017), which was reviewed by the late Robert Jervis as a "significant contribution to our knowledge," and co-editor of *North Korea and Nuclear Weapons: Entering the New Era of Deterrence* (Georgetown UP: 2017). His expertise on the North Korean nuclear threat has been sought by and presented to the U.S. State Department, included in a United States Strategic Command Deterrence Symposium Special Edition and news media outlets in the United States, Canada, Britain, Australia, and elsewhere.

His research has been published or is forthcoming in scholarly journals *European Journal of International Relations, Journal of Peace Research, The Journal of Global Security Studies, Foreign Policy Analysis, Asian Security, International Relations of the Asia-Pacific, The Non-Proliferation Review, Australian Journal of International Affairs* and *International Security* (correspondence). His ongoing research addresses alliances in Europe and Asia, foreign policy decision-making and the sources of inter-state conflict.

Since joining the ANU in 2018, Dr. Cohen is (since 2020) convenor of the PhD program at the National Security College. Prior to joining the ANU he was senior lecturer at the Department of Security Studies and Criminology at Macquarie University (2016-2017) and assistant professor at the Department of Political Science and Center for War Studies at the University of Southern Denmark (2012-2015). In 2014 he was a visiting fellow at the Saltzman Institute of War and Peace Studies at Columbia University. He completed his PhD in 2012 at the University of British Columbia.

Chris Nott

Chris Nott is chief technology officer for Defence and Security at IBM. His expertise in digital transformation using hybrid cloud and AI and broad understanding of emerging technologies is sought by defence departments around the world. He influences strategic thinking by conveying complex technical concepts to senior officers and executives in an understandable way.

Chris sets the technical vision and strategy for the defence sector in IBM. He has applied his experience integrating systems that exchange information between headquarters and the edge, exploiting data to generate insight sooner for trusted decision making and constructing roadmaps for adopting cloud computing.

Since joining IBM, Chris has co-authored the seminal *Redbook* on service-oriented architecture and has become a Quantum Ambassador. He is also a chartered engineer and holds a first class honours degree in mathematics from the University of Durham.

Key Contact Information

Michael Cohen
National Security College, Crawford School of Public Policy,
Australian National University

Email: Mike.Cohen@anu.edu.au

Chris Nott
Global Chief Technology Officer
Defence & Security, IBM

Email: chris_nott@uk.ibm.com

Recent Reports from the IBM Center for The Business of Government

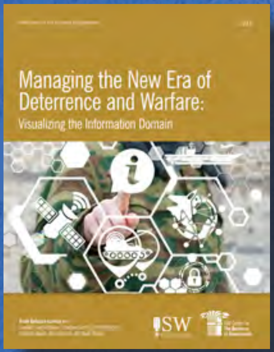
Government Procurement and Acquisition: Opportunities and Challenges Presented by Artificial Intelligence and Machine Learning
FEDERAL PROCUREMENT DATA
DEFINITION
AI

Government Procurement and Acquisition: Opportunities and Challenges Presented by Artificial Intelligence and Machine Learning

by Mohammad Ahmadi and
Justin B. Bullock

Preparing governments for future shocks: Collaborating to build resilient supply chains

by Robert Handfield Ph.D.



Managing the New Era of Deterrence and Warfare: Visualizing the Information Domain

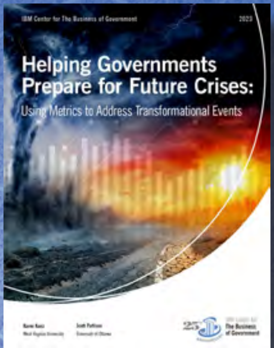
by Brian Babcock-Lumish

A Guide to Adaptive Government: Preparing for Disruption

by Nicholas D. Evans

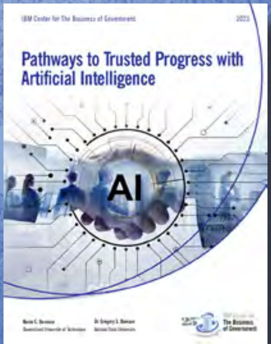
Preparing governments for future shocks: An action plan to build cyber resilience in a world of uncertainty

by Tony Scott


IBM Center for The Business of Government
Helping Governments Prepare for Future Crises:
Using Metrics to Address Transformational Events

Helping Governments Prepare for Future Crises

by Karen Kunz and
Scott Pattison


IBM Center for The Business of Government
Pathways to Trusted Progress with Artificial Intelligence
AI

Pathways to Trusted Progress with Artificial Intelligence

by Kevin C. Desouza and
Dr. Gregory S. Dawson

Mobilizing Cloud Computing for Public Service
PARTNERSHIP FOR PUBLIC SERVICE
The Business of Government

Mobilizing Cloud Computing for Public Service

by Amanda Starling Gould

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

IBM Center Research Announcement

Applying Design Thinking To Public Service Delivery
Scaling Evidence-Based Programs in Child Welfare
A Roadmap for IT Modernization in Government
Accelerating Government Innovation With Leadership and Stimulus Funding
EIGHT STRATEGIES for Transforming Government
Making Federal Evidence-B... The Key Role
Human-Centricity in Digital Delivery: Enhancing Agile Governance
Agile Problem Solving in Government: A Case Study of The Opportunity Project
Off to a State C...
Collaborative Networks

The IBM Center for The Business of Government connects research to practice, supporting work by scholars that benefits government through real-world experience and analysis. Our Center's reports are intended to spark the imagination—crafting new ways to think about government. We identify trends, new ideas, and best practices in public management and innovation.

We encourage applicants to review our research areas closely in selecting a topic, or a cross-cutting set of topics. We are looking for very practical findings and actionable recommendations—not just theory or concepts—in order to assist executives and managers to more effectively respond to mission and management challenges.

For more details on our latest proposal deadlines and application form, please visit: **https://www.businessofgovernment.org/content/research-stipends**.

We look forward to hearing from you!

25TH ANNIVERSARY

IBM Center for
**The Business
of Government**

Insights | **Conversations** | **Information** | **Action**

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**