MITRE | Intelligence After Next

Intelligence After Next

SERIES # 26

CREATING INTEROPERABLE AND ANTIFRAGILE DIGITAL PLATFORMS: A NEW PARADIGM FOR SENSEMAKING

by Randy Howard and Geralyn Blossom

© 2024 MITRE # 24 2265 7 26 2024

The Imperative to Create a Better Technology Intelligence Infrastructure

The United States' whole-of-nation capabilities are severely hampered by the government's outdated approach to discovery and harnessing the collective intelligence resources that could enable our Intelligence Community (IC) and its domestic and international partners to have a decisive understanding of the operational picture. The technology gaps that most adversely affect decision makers' ability to understand their options and to take informed actions are interoperability, antifragile[1] baseline capabilities specific to IC missions, and enabling timely actionable sensemaking to benefit all partners.[2] Many non-technical factors, such as budgets and authorities, burden-sharing, and process development, contribute to this situation as well—which will be addressed in a subsequent paper.

These technology gaps have been recognized for more than a decade, and warfighters, analysts, and data specialists are delivering amazing results by creating a plethora of tools and data for their specific needs. However, the data and tools:

- Are stovepiped and fragmented, are hard to discover and learn to use, and do not work seamlessly together—that is, they do not interoperate
- Are fragmented across technology infrastructures, causing a great deal of manual preparation and stitching together results to deliver conclusions based on data sources that can be accessed and managed across our communities
- Are too fragile[3] and brittle, and the tools are not easy to extend, modify, and deploy—which does not support timely delivery to unanticipated user inputs and changing needs
- Address known patterns but provide limited ability to explore and make sense of unknown patterns

These gaps force decision making at all levels with partial or differing insights that may not include all relevant data the United States has collected. As our whole-of-nation efforts advance and data availability improves, data specialists and analysts will increasingly need tools that automates dynamic integration and amplifies sense making of the ever-increasing stores of data to meet ever-changing conditions. As a nation, we need to find continuously increasing means to improve the efficiency of our analysis by automating where we can; creating general and shareable models and simulations whenever possible; and customizing our applications, programs, and systems only when necessary.

This paper provides a technical approach to greatly improve our intelligence operations by moving to engineered production lines to enable dynamic discovery, integration, and access to harness the value invested and build unanticipated solutions. To do so, the IC should invest in commercially developed proven approaches (e.g., cloud platforms) to create a data and analytic infrastructure engineered to support sensemaking, or a sensemaking infrastructure framework (SIF). As shown in Figure 1, a SIF consists of three inter-connected layers:

- Federated Sensemaking Digital Platform
- Analytics Interoperability Services Suite
- Data and Analytics Factory

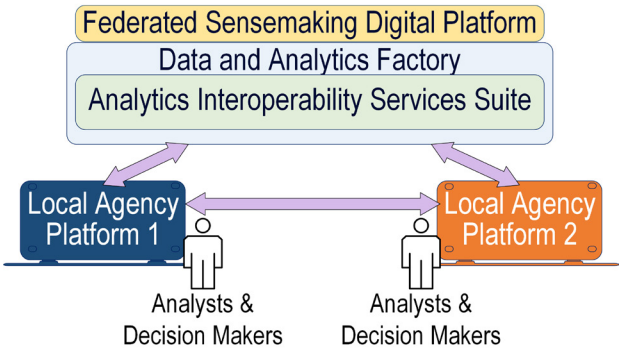

Figure 1. Sensemaking Infrastructure Framework

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

Across the IC, a SIF would enable dynamic enterprise sharing across disconnected and disparate workflows, validation, and protection, as well as ensure results across agencies. This infrastructure can help manage risk, ensure credit is given to contributors in collaboration efforts, and expand awareness of information critical for our tipping capabilities (i.e., tipping involves the ability of intelligence agencies to provide timely and actionable information that can alert or "tip off" decision-makers or operational units about potential threats or opportunities). Although the technology can still provide for local agency autonomy, policy enforcement will be needed to ensure appropriate access across the whole-of-government. This infrastructure would be tailorable for local platforms with minimal impact to an organization's existing environments.

The Federated Sensemaking Digital Platform, as the flagship capability, surpasses current analytic capabilities by enabling the dynamic framing and exploration of possible concepts, theories, and insights; augmenting human associations and interpretations; and optimizing the anticipatory user experience. The Analytic Interoperability Services Suite enables seamlessly connecting capabilities across the IC through the Sensemaking Digital Platform without disclosing sensitive information. The Data and Analytics Factory scales antifragile capabilities across the IC and its domestic and international partners' data and tools for non-technical end users as well as technical data engineers and scientists. The engineers and scientists can innovate and create new capabilities that are robust, scalable, adaptable, and resilient[4] so investments can remain valued.

A SIF provides the equivalent of a production line of discoverable, reusable, and composable capabilities specific to the IC's common and new unanticipated patterns of analysis. These capabilities must be standardized and understood to be interpreted and packaged into commonly accessible functions for non-technical end users to leverage across the IC. Current cloud infrastructures provide similar capabilities for generic commodity functions that typically involve software engineers modifying software or data scientists developing new algorithms.

Allowing analysts to compose capabilities themselves increases their throughput; provides analysts more time to evaluate, produce, and leverage one another's source data, processed data, and analytic results; and advances analytic tool capabilities. It also allows scarce technical staff (e.g., software engineers, data scientists) to focus on more advanced capabilities and reduces duplicated efforts to develop the same functionality in different siloes across the Intelligence Community.

Lastly, a SIF allows intelligence resources to deliver higher quality finished intelligence at the speed of relevancy.

Current Analytic Landscape

The enduring challenge highlighted by the findings of the 9/11 Commission and subsequent studies underscore the critical need to bridge the gap between recommendations and practical implementations. Despite recognizing the imperative for enhanced data sharing and intelligence fusion to support comprehensive national and strategic endeavors, progress remains hindered. Information sharing depends too heavily on trusted personal affiliations or point-to-point organizational agreements and solutions that are untenable to scale.

A central obstacle to realizing these data sharing and intelligence fusion objectives lies in the archaic functional infrastructure prevalent within our government agencies. Another significant challenge hindering the achievement of these goals stems from the outdated operational framework entrenched in government agencies, coupled with reluctance or incapacity to share information due to stringent need-to-know and classification limitations. This piecemeal structure perpetuates the use of disjointed tools and fragmented data systems, hindering smooth cooperation among our military personnel, analysts, and data experts. Although certain data may

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

necessitate compartmentalization for security reasons, the methodologies and tools for extracting insights from data should be openly shared across the IC, with an emphasis on adaptability for various scenarios.

Operating within this fragmented environment necessitates extensive manual effort to synthesize insights from disparate data sources, often resulting in a piecemeal approach to decision making. Such limitations impede timely access to comprehensive data insights essential for informed decision making across all levels of the IC.

As the nation's collective efforts coalesce and data integration and availability improve, the demand for agile and adaptable solutions becomes more pronounced. Data specialists and analysts must be equipped with prebuilt capabilities that facilitate seamless end-to-end life-cycle workflows. These capabilities should enable swift deployment, repurposing, or adaptation to accommodate evolving operational requirements with minimal technological modifications.

Moreover, the evolution of our data infrastructure must prioritize interoperability and scalability to ensure seamless integration across diverse systems and domains, while still adhering to authorization and legal authority protocols. By modernizing our technological frameworks and empowering personnel with advanced sensemaking platforms, we can overcome the constraints imposed by stovepiped tools and fragmented data systems. Doing so will not only enhance collaboration and information sharing but also enable personnel to navigate the burgeoning volume of data and dynamic operating conditions effectively, thereby bolstering our national security posture and strategic competitiveness.

These challenges, and this proposed path forward, emanate from U.S. National Intelligence Strategy and other intelligence-related studies. Additional insights come from decades of the authors' and their colleagues' empirical hands-on work as data specialists and analysts who experience these situations daily. This paper focuses on the below functional gaps, as they are likely to have the most impact in addressing the core themes found in IC strategies and studies:

- Interoperability
- Antifragile Properties
- Sensemaking

The ultimate capability needed is sensemaking to help inform decision makers. However, sensemaking relies on cross-organizational interoperability to connect disparate inputs and perspectives for a whole-of-nation impact. As this interoperability increases, sensemaking is needed even more because the amount of information exponentially increases. Portable and antifragile properties are essential to sensemaking in that they enable solutions to innovatively scale consistently and uniformly across the interoperating organizations and adapt to unforeseen threats and challenges.

Interoperability

Interoperability across the IC has been an elusive objective to achieve; however, it is vital to connect and harness our collective organizations' and our partners' strengths at scale. Data sharing still depends heavily on a plethora of disconnected point-to-point data-sharing agreements, memorandums of understanding, and so forth. Standards are a prevalent approach to address interoperability, but they are also disconnected across isolated topics covering data, policy, classification, jurisdiction, and so on. Additionally, complying with standards has two major impediments. First, local organizations often must continually modify their platforms to comply with constantly changing standards. Second, compliance depends on developers interpreting and integrating multiple standards, which incurs duplicated efforts and inconsistencies across the IC. Additionally, smaller, geographically separated, and forward-deployed organizations along with partner forces often have insufficient resources to seamlessly connect with advanced enterprise capabilities. They must use disparate systems and data to achieve the analytic insights needed for commanders' decision making.

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

RELIANCE ON DISJOINTED CAPABILITIES AND INABILITY TO DYNAMICALLY MAKE SENSE OF THE EVER-CHANGING THREAT LANDSCAPE POSE SEVERE RISKS OF NOT KEEPING PACE WITH OUR ADVERSARIES AND OUR NATION'S NEED FOR THE HIGHEST QUALITY, MOST TIMELY INTELLIGENCE TO COUNTER EVER-INCREASING GLOBAL THREATS.

Antifragile Properties

Gaining antifragile properties has gained traction recently for both organizational[5] and architectural[6] purposes. Antifragile is defined as "becoming more robust when exposed to stressors, uncertainty, or risk."[7] Antifragile solutions[8, 9] entail characteristics such as reliability, fault tolerance, and resilience.[10] However, a SIF also emphasizes scalability and adaptability so solutions can dynamically adjust to ever-changing threat conditions, which is analogous to offensively being prepared to handle contingencies in battles to outpace the operational tempo of our adversaries. Regardless of the architecture, solutions can have inherent limitations in becoming antifragile. Large, centralized architectures that require a massive infrastructure to operate are not easily transitioned, or portable, to other organizations. Container technologies facilitate capabilities operating in different environments; however, they do not necessarily facilitate the containerized capabilities integrating with other capabilities within the different environments. These systems can be hard to sustain because functions are tightly coupled such that failure of one function causes others to fail. Other solutions are built for single bespoke purposes, and their internal structures are too fixed and rigid to be adapted and scaled to similar functions across different missions. Some solutions intended to serve multiple user bases and missions impose constraints where users must find workarounds to meet their local mission needs.

Cloud solutions are built on reusable components; however, the components require tailoring to meet specific mission needs. Therefore, the common functions are unnecessarily developed multiple times across the IC despite using common reusable components. Also, reusable components are geared toward developers and not non-technical end users, preventing these users from taking advantage of them.

These limitations are indicators of fragile systems because they break often or fail under the stress of being extended beyond their single bespoke purpose or dynamically adjusting to meet specific local mission objectives. Fragile systems are not able to readily engage in a dynamically changing threat environment.

We are missing an opportunity to package mission-specific functions that users can discover and repeatably perform into composable mechanisms that can be dynamically configured by end users without involving developers.

Sensemaking

Data specialists and analysts charged with developing timely key insights are continually inundated with fragmented information that is difficult to navigate. For example, Common Intelligence Picture (CIP) and Common Operational Picture (COP) capabilities provide intelligence and operational indicators of the operational theatre to help inform the decision space. However, CIP/COP solutions typically have limitations that emanate from such constraints as pre-engineered biases that focus on certain aspects (e.g., maritime versus space) of the theatre, not being able to adapt to unforeseen situations, or inability to accept new data feeds. As a result, decision makers struggle to make informed decisions because they do not understand their

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

option space. Additionally, data latency is an important consideration, as this process hinders analysts from heavily influencing operations and requires them to utilize disparate systems to establish the most current, updated battlespace view for decision makers. Operators and commanders need data in near real time to make decisions at the speed of relevancy.

Restructuring data requires a substantial amount of manual intervention to collect, clean, and prepare the data. A common statement from analysts is that they spend 80 percent of their time munging data and only 20 percent of their time performing analysis. In other words, analysts spend too much time merely triaging data and artifacts to determine what is useful and depend too heavily on informal relationships to facilitate information sharing. Analysts need to have data delivered straightaway that can be used across multiple systems and models.

Intelligence reporting and data exist in disparate systems across multiple domains. Efforts have been underway across the Department of Defense (DoD) to improve system interoperability. While some systems have enabled these efforts through Application Programming Interface (API) pulls, degradation can easily occur if analysts are not coordinated with one another or do not have real-time developer support to adjust API filters to reflect updates of the source database. This can lead to latent or stale data, hindering analysts' ability to trust the data being received.

For example, the Intelligence Community has embraced Object Based Production (OBP) to restructure intelligence data in an ontology to easily share and align intelligence information and develop insights into data sets. As efforts continue to scale OBP across the DoD, it will also need to be easily shared across systems and domains to extract insights from the data using advanced analytical models with artificial intelligence and machine learning (AI/ML).

Relying on external contractors for data management poses significant long-term financial implications for the government, as it often entails substantial investment in sustaining and enhancing the functionality of acquired tools. Moreover, such reliance may compromise the government's unfettered access to data and result in receipt of data tailored to the specific requirements of the contracted tools. By establishing an internally owned digital platform, the government can harness the full potential of its data, facilitating seamless integration with external tools to derive advanced insights (although vendor lock-in will have to be considered). This approach affords the government greater flexibility in contracting arrangements, enabling procurement based on genuine necessity rather than alignment with individual contractors. Furthermore, internal ownership ensures enhanced data security, accountability, and long-term cost-efficiency, thereby optimizing the government's data management capabilities while safeguarding against dependency on external entities.

The aforementioned factors result in uninformed decisions due to analytic products being made on partial or incomplete data. Analysts must have sufficient sensemaking capabilities to separate signals from the noise,[11] and must be able to dynamically explore, analyze, and package the endless "what-if" scenarios into cogent courses of action for decision makers. This necessitates analysts and data specialists have the tools to make better sense of signals in real time. Additionally, our current tool base struggles to properly depict situational awareness to better understand what is happening in theatre. Some efforts to enhance situational awareness through intelligence data have been underway, such as the Air Force's response to Joint All Domain Command and Control through implementation of Advanced Battle Management Systems to enable integrating data for sensor to shooter capabilities. However, fully incorporating signals with other intelligence indicators remains a fragmented and time-intensive process.

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

IF WE WISH TO REALIZE OUR STRATEGIC OBJECTIVES OF SOLUTIONS MEETING NEEDS AT THE SPEED OF MISSION, THEN WE MUST INVEST IN A NEW SENSEMAKING INFRASTRUCTURE TO CONNECT OUR COLLECTIVE CAPABILITIES AS A WHOLE-OF-NATION APPROACH.

Getting Unstuck

Core Considerations

Establishing core and common frameworks is hard to achieve due to the many disparate organizations that have different missions, objectives, standards, data and data structures, and "languages" (i.e., use of terms and concepts). IC strategies have important concepts and principles (e.g., data-driven, interoperability, speed of mission) that are essential to addressing threats and challenges. However, these initiatives are struggling, even failing, to make substantive impact in achieving their goals and objectives. Despite the many solutions that have been developed to address these challenges, users and developers continue to struggle.

To get out of this conundrum, we should pursue the following options, where some of these actions draw from fundamental systems engineering, but they bear emphasizing for this effort:

- Define more concrete pathways to realize goals and objectives.
- Provide architects and engineers with more specific guidance to better convey the intentions of the objectives, how many resources can be expended, and when the return on investment is not worthwhile.
- Share tools, capabilities, insights, and knowledge—our collective sensemaking of the environment. Leaders need cross-organizational operational, intelligence, and logistics data to make the most informed decisions.

These efforts would provide more in-depth insights gained by leveraging broader collections of data. Machines would then identify patterns and allow humans to dynamically adjust their user experience (UX)[12] per mission need at any given time so they can have better context, interpret new data in real time, and draw key insights. For example, a single threat report may not suffice for an analyst to consider further action; however, an analyst tracking a threat stream utilizing many sources of multiple intelligence reporting could better determine the next actions to take. If some of this reporting contains information outside the scope of a specific analyst's subject area, being able to adjust UX allows analysts to filter down to their specific mission area and pull only the relevant information from an ever-increasing amount of intelligence data.

Commercial software development practices have long embraced these principles to encapsulate commonly used functions into reusable and tailorable capabilities. Data mesh principles support this by providing reusable tailored data capabilities for specific domains. These principles are rapidly gaining traction because they decentralize the control and ownership of data to address the limitations and challenges faced by traditional centralized data systems that often lead to bottlenecks, lack of agility, and scaling challenges.[13] The IC and DoD need to embrace this approach to encapsulate the common capabilities, features, and functions used to address their unique challenges that are not found in commercial spaces.

This proposal is rooted in a case study of commercial success from Hadoop. Hadoop, which emanated from papers on Google File System and Map Reduce,[14]

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

encapsulates the many complexities related to distributed computing, allowing developers to leverage the power of distributed computing with ease. There are many similar complex functions being handled redundantly and inconsistently by developers across the IC. The approach of leveraging the power of distributed computing would allow for packaging complex and redundantly coded capabilities across the IC a similar manner, where a relatively small number of developers create solutions that can be reused across the community. IC Common Data Services[15] and Services of Common Concern[16] apply this approach and need to be extended much further in practice and resources.

We need a common set of tools or utilities that can be bolted onto existing platforms to promote faster throughput and consistent compliance across organizations. The below additional considerations are incorporated into the framework:

- Interoperability expands data concepts and approaches to include analytics. For example, configuration management and provenance and lineage are applied to analytic models, training data, results, and the like. The principles of findability, accessibility, interoperability, and reusability (FAIR)[17] are applied to the analytic capabilities throughout the platform, especially interoperability and reusability.
- Antifragile includes portability and is considered offensive as well as defensive, similar to cybersecurity having offensive and defensive uses,[18] because an antifragile approach entails solutions having scalability and adaptability engineered into their fabric to maximize their impacts.
- Scalability is expanded beyond just handling volume and capacity to include repurposing data and analytics[19] and across domains, organizations, and purposes.[20] The Cross-Domain Interoperability Framework[21] provides a set of patterns and recommended practices for research infrastructures servicing cross-domain research areas to support broad reuse of FAIR data offerings only within a given community and between communities. Portability of solutions and capabilities across organizations and environments expands portability beyond what container technologies such as Docker and Kubernetes provide for technical portability across platforms.
- Adaptability is also expanded beyond development and operations; development, security, and operation; or agile software development methodology to include engineering into solutions the ability to handle unforeseen conditions without engaging developers. This feature results in self-service and no-code/low-code approaches. Part of this adaptability is the ability to dynamically compose and configure solutions from capability "building blocks," which is prevalent in cloud platforms for developers. However, a SIF expands this composition capability to non-technical end users. For example, no-code/low-code solutions[22] allow users to compose and execute complex algorithms with minimal technical knowledge or coding experience necessary.

To gain traction with this novel approach, we can escalate these considerations to officials above the individual agency level to approach it with a whole-of-nation urgency. At the same time, we must convince stakeholders that a collective approach is needed. We can also identify existing examples of technologies and organizations that demonstrate elements of this approach and build pivotal proofs of concept that exemplify the benefits and considerations of such an approach.

The Platform's Framework

A SIF can be realized in many forms. Using prevalent cloud solutions, it could be an additional layer of capabilities riding on existing service platforms (e.g., Platform as a Service, Infrastructure as a Service, Software as a Service), where this additional layer simply follows the model of existing cloud services that provide reusable and composable capabilities that can readily be transferred across platforms. The key addition to these commodity

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

cloud capabilities is that this layer provides functionalities tailored to address IC-specific needs, which are then further tailored for end users versus technical developers as ready-to-use components and building blocks.

This framework addresses typical roadblocks because it is positioned as a lightweight, bolt-on apparatus to existing platforms. This allows both large and small organizations to take collective action without having to refactor their existing technology solutions. Providing an overarching and unified framework enables these existing solutions to consistently work better together, or possibly even extends their usefulness by making them more portable across different domains.

The framework's description is based on what it provides functionally, along with the rationale and justification for the framework, while leaving such details about how, who, when, budget, authorities, and organizational challenges for subsequent endeavors.

The first layer of the framework is a Federated Sensemaking Digital Platform positioned within a simulation and modeling environment, where personnel can navigate countless "what-if" scenarios, tailor information down to only what is relevant, and make sense of complex situations to gain necessary insights and provide the necessary explanation of the possibilities of leveraging models built for similar use cases. The capabilities depicted in Figure 2 (which are representative and not exhaustive) are capabilities that better inform more comprehensive decision making in a timelier manner compared with typical CIP and COP solutions.

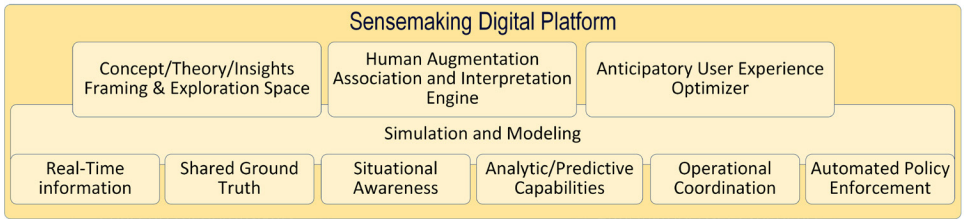

Figure 2. Sensemaking Digital Platform Capabilities

Analysts need to create space for "listening, reflection and the exploration of meaning beyond the usual boundaries, allowing different framings, stories and viewpoints to be shared and collectively explored." They need to "develop a set of insights with explanatory possibilities rather than a body of knowledge or plan of action."[23] Digital platforms "cut across traditional organizational structures, silos, policies, and technology investments to enable the new operating model. They force a different organization, a different talent model, a different mindset, and a different set of policies and processes."[24] This structure augments human domain knowledge to identify, connect, and interpret complex but relevant data points and information (and tools) that may be connected using AI/ML (and non-AI/ML) capabilities. Additionally, it is automatically tailorable for users to adjust their expanded information sets to manage unexpected conditions without developers having to intervene.

The next layer is an Analytic Interoperability Services Suite, depicted in Figure 3, that knits together disparate organizations' infrastructures to meet both community and local organization mission needs across data, workflow, and visualization dimensions. The suite allows the framework's capabilities to be portable and easily

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

integrated with existing environments of both large and small organizations across the intelligence, operations, and logistics communities to enable interoperability across the policy, data, workflow, visualization, and access dimensions of solutions.[25] This facilitates cross-organizational, whole-of-nation solutions, while still allowing local organizations the autonomy they vitally need to perform their missions and enhance enterprise-wide data correlation. An Interoperability Broker mediates between local organizations and enterprise languages, thus allowing local organizations the autonomy to conduct their mission without requiring massive changes to their infrastructure.

This suite is an expansion of an effort at an IC agency to connect analytic platforms through common metadata services of catalog/registry, pedigree and lineage, and tethering. By connecting these common services to each platform, the platforms could interoperate regardless of how disparate their backend infrastructures are. Additionally, the authors have designed architectures to forge the path.

The suite's portal links the various aspects of interoperability, such as policies, data, workflow, visualization, access, AI/ML, and others as needed, depending on the extent the organizations can and wish to work together. Some commercial off the shelf vendors are doing some portions of this already, but the technologies are not comprehensive or fast enough to meet today's need.

Humans can interface either at the suite level or at the higher sensemaking platform, and non-person entities can also interface at either point to augment the human efforts.

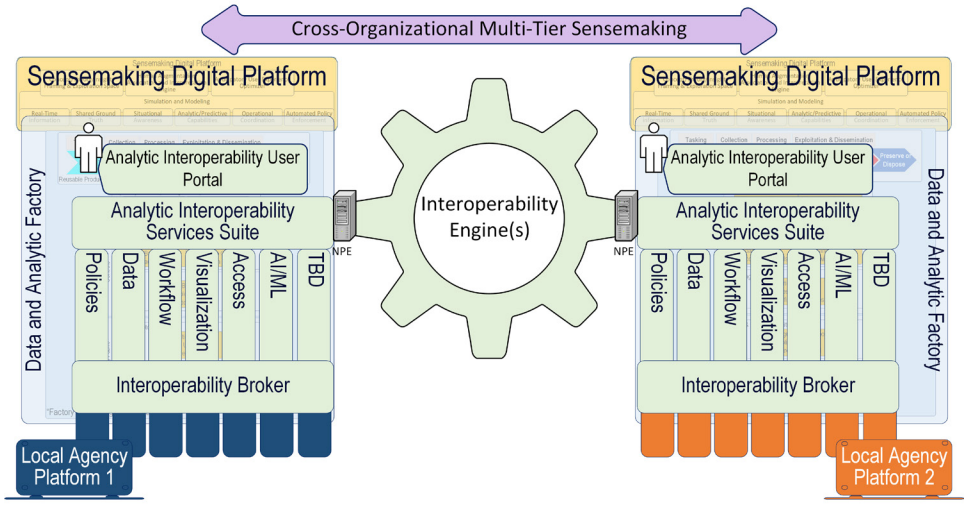

Figure 3. Sensemaking Digital Platform Capabilities

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

The suite works with a network for portable microservices and agents that can be deployed across organizations, where interoperability engines choreograph, and where choreography allows more autonomy and independence than orchestration[26] of the traffic. The suite is easy to replicate (and sustain)—and is portable—across disparate environments and organizations to provide a robust and common baseline of functionality, especially for smaller organizations that do not have the resources to develop such capabilities. Enterprise-level resources should be appropriated to support these smaller organizations to take advantage of the suite of services.

The JavaScript Object Notation-Linked Data specification fits within the data interoperability services by allowing organizations' data to be interoperable with other organizations' data through a lightweight linked data format at web scale. Linked data provides a network of standards-based, machine-readable data across websites.[27]

The last layer is a Data and Analytics Factory (as shown as part of Figure 3 and shown in greater detail in Figure 4) that conveys a majority of the antifragile properties of the framework and provides the utilities to help analysts with triaging data.

The Data and Analytics Factory mimics the production line of any factory manufacturing goods and materials in that the product line can be rapidly configured in multiple forms for each result as needed. The base product line depicts the IC data management life cycle and Tasking, Collection, Processing, and Exploitation and Dissemination in terms of functions processing data, producing analytics, and recursively iterating on the same. As in a physical factory where machinery, robots, staging stations, and the like provide the components to reconfigure the lines, the Capability Toolbox provides composable purpose-built tools and utilities for reusable functions such as federation, interoperability, workflow, analysis, sensemaking, and decision making. Controls in the forms of guards (e.g., routing, load balancing) and monitoring (e.g. metrics, notifications when tolerances are exceeded) ensure the components operate within acceptable tolerances. The Capability Toolbox can take the form of:

- Containerized software to crunch data into common, sharable intelligence products (e.g., Cursor on Target message, Geojson objects) that allow analysts to visualize and report on relevant phenomena
- Composable and scalable deployment mechanisms (e.g., Ansible, which is compatible with secure cloud computing)
- A suite of browser-based Graphical User Interface tools that allow analysts to compose capabilities for themselves rather than developers

Using a transportation infrastructure example, this architecture would enable analysts to rapidly report weather, status of transportation systems (e.g., runways, pipelines, rail lines, ports, highways), and results from in-transit visibility systems for managing day-to-day and surge operations. On the Intelligence Preparation of the Battlefield front, the architecture would allow for all conventional enemy order-of-battle and threat information, plus estimates of fuel stored in areas that are hostile or where the political landscape is volatile. Having the flexibility within the architecture allows for compilation or flexibility in retooling depending on the mission space and analyst need.

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

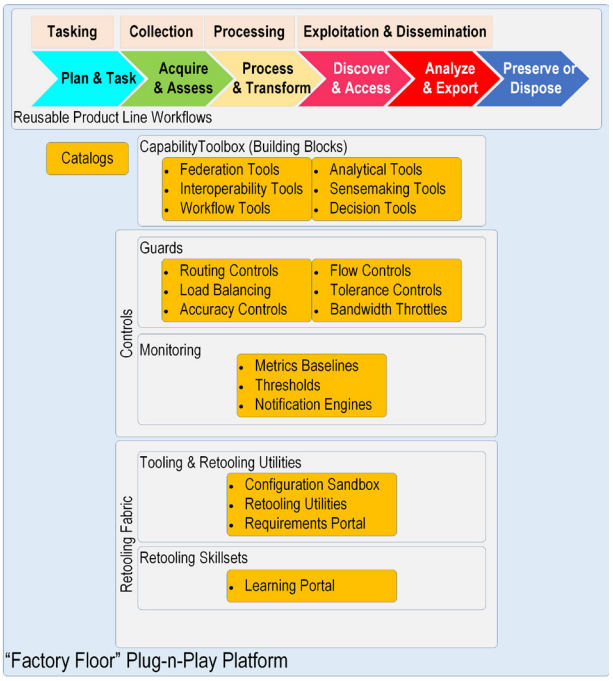

Figure 4. Data and Analytics Factory

Retooling is essential in the IC's ever-changing environment due to factors such as newer technologies, budget changes, emerging threats, partner landscapes, access, and availability (e.g., networks, authorities). A Configuration Sandbox allows for impromptu experimentation on new or updated capabilities that provides automated transition to the rest of the factory's functions. Catalogs across the IC enable discoverability and access. Requirements must perpetually drive the retooling to keep the machinery current. Last, but by no means least, is the needed investment in analysts' skillsets within the Intelligence Community to develop, train, and cultivate a more data driven analyst. The factory mandates continual learning to keep up with this constant change.

Investing to Bolster U.S. Competitiveness

This framework defines baseline functional structures, capabilities, and components specific to the IC's mission that can be easily replicated, or portable or reused, across analytic platforms to allow these platforms to interoperate so analysts can share data and analytic progress and results, while still allowing organizational autonomy to meet local mission objectives in an offensive operational manner.

We propose a suite of portable and antifragile microservices that interoperate across the policy, data, workflow, visualization, and access dimensions of solutions. The microservices need to facilitate the common elements that can be made portable and scalable across platforms and missions. The platforms must also easily adapt to ever-changing conditions and uses.

To ensure cross-community consistency, the platforms should be collaboratively engineered across stakeholder communities. It is essential to consider all tiers together, as opposed to addressing only isolated parts of the framework. Otherwise, a fragmented approach will result in fragmented capabilities. Key components of a collaborative approach exist across Intelligence and Operations communities (e.g., CIP and COP solutions, digital platforms, cloud platforms). This approach provides the vision and essential mechanisms for components to take collective action.

While this paper focuses on a technical approach, non-technical aspects must also be considered. For instance, a community-wide champion and key stakeholders are needed to ensure equities across the community are represented. This champion will need to tackle such realities as budget, assignments, and schedules. The champion will also need to be sufficiently empowered to influence significant changes in authorities and lines of business.

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

The capabilities provided by the framework, when fully realized, will provide analysts more time to evaluate, produce, and leverage one another's results; reduce their time collecting and preparing data; and ultimately allow them to make better sense of situations with more complete and comprehensive information. Additionally, access to this information reduces the amount of duplicated work from developers across the Intelligence Community who are likely working on similar capabilities in inconsistent and disjointed manners and allows them more time to focus on delivering functionality for their specific missions.

If we wish to realize our strategic objective of solutions meeting needs at the speed of mission, then we must invest in a new functional infrastructure that focuses on sensemaking with inoperable capabilities and antifragile properties to connect our collective capabilities as a whole-of-nation approach. Doing so will bolster our strategic competitiveness. Finally, investing in any new capability requires time to learn, experiment, evolve, and adapt to solidify what is predictable to better handle the invariable—we cannot do this in the heat of a crisis.

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

References

1. Nassim Nicholas Taleb, Antifragile, Penguin Books, 2013.
2. Department of Homeland Security, National Strategy for Information Sharing and Safeguarding, December 2012. Available: https://www.dhs.gov/sites/default/files/publications/15_1026_NSI_National-Strategy-Information-Sharing-Safeguarding.pdf; Government Accountability Office, COUNTERTERRORISM, Action Needed to Further Develop the Information Sharing Environment, June 2023. Available: https://www.gao.gov/assets/830/827084.pdf
3. Bilgin Ibryam, From Fragile to Antifragile Software, July 20, 2016. Available: https://developers.redhat.com/blog/2016/07/20/from-fragile-to-antifragile-software
4. Albert Munoz, Jon Billsberry, and Véronique Ambrosini, Resilience, Robustness, and Antifragility: Towards an Appreciation of Distinct Organizational Responses to Adversity, International Journal of Management Reviews, 24, 10.1111/ijmr.12289, 2022. Available: https://onlinelibrary.wiley.com/doi/full/10.1111/ijmr.12289
5. Albert Munoz, Jon Billsberry, and Véronique Ambrosini, Resilience, Robustness, and Antifragility: Towards an Appreciation of Distinct Organizational Responses to Adversity, International Journal of Management Reviews, 24, 10.1111/ijmr.12289, 2022. Available: https://onlinelibrary.wiley.com/doi/full/10.1111/ijmr.12289
6. Daniel Russo and Paolo Ciancarini, Towards Antifragile Software Architectures, Procedia Computer Science, 109, 929–934, ISSN 1877-0509, 2017. Available: https://www.sciencedirect.com/science/article/pii/S1877050917311079
7. Dictionary.com. (n.d.). Antifragile Definition & Meaning. Available: https://www.dictionary.com/browse/antifragile#google_vignette
8. Bruce Powel Douglass, Real-Time Design Patterns: Robust Scalable Architecture for Real-Rime Systems, Addison-Wesley, 2003. Available: https://box.cs.istu.ru/public/docs/other/_New/Books/Software%20Development/Real-Time%20Design%20Patterns.pdf
9. Sanjoy Kumar Malik, Defining Architecture and Design Principles for Robust Solutions, LinkedIn, November 12, 2023. Available: https://www.linkedin.com/pulse/defining-architecture-design-principles-robust-solutions-malik
10. Daniel Russo and Paolo Ciancarini, Towards Antifragile Software Architectures, Procedia Computer Science, 109, 929–934, ISSN 1877-0509, 2017. Available: https://www.sciencedirect.com/science/article/pii/S1877050917311079
11. Claude Elwood Shannon, A Mathematical Theory of Communication, Bell System Technical Journal, 27, 379–423, 1948. Available: http://dx.doi.org/10.1002/j.1538-7305.1948.tb01338.x
12. Interaction Design Foundation, What Is User Experience (UX) Design? The Interaction Design Foundation, October 19, 2023. Available: https://www.interaction-design.org/literature/topics/ux-design
13. Micha Horner, The Ultimate Guide to Data Mesh, Data Empowerment, February 26, 2024. Available: https://medium.com/data-empowerment-with-timextender/the-ultimate-guide-to-data-mesh-b25b54276f74#:~:text=This%20novel%20approach%2C%20centered%20around,by%20traditional%20centralized%20data%20systems
14. GeeksforGeeks, Hadoop History or evolution, GeeksforGeeks, January 18, 2019., Available: https://www.geeksforgeeks.org/hadoop-history-or-evolution/
15. Lori Wade, IC Data Strategy 2023-2025. (n.d.). Available: https://www.dni.gov/files/ODNI/documents/IC-Data-Strategy-2023-2025.pdf
16. Daniel R. Coats, Services of Common Concern. (n.d.). Available: https://www.dni.gov/files/documents/ICD/ICD-122.pdf
17. Mark Wilkinson, Michel Dumontier, Ijsbrand Aalbersberg, I. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018 (2016). https://doi.org/10.1038/sdata.2016.18FAIR Principles. (n.d.). Available: https://www.nature.com/articles/sdata201618#citeas

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

18. Pfortner, A Comparison Between Offensive and Defensive Cybersecurity Strategies, May 15, 2023. Available: https://www.linkedin.com/pulse/comparison-between-offensive-defensive-cybersecurity

19. Mingsheng Long, Jianmin Wang, Yue Cao, Jiaguang Sun, Philip S. Yu, Deep Learning of Transferable Representation for Scalable Domain Adaptation, IEEE Transactions on Knowledge and Data Engineering, 28(8), 2027–2040, 2016, doi:10.1109/TKDE.2016.2554549.

20. Robert Vane, What Is Scalability in the Enterprise Information Domain, LightsOnData, March 18, 2020. Available: https://www.lightsondata.com/scalability-enterprise-information-domain/

21. Simon Hodson, The Cross-Domain Interoperability Framework: Coordinating Standards for Scalability, Dublin Core™ Metadata Initiative, October 4, 2022. Available: https://www.dublincore.org/conferences/2022/sessions/panel-cross-domain-interoperability-framework/

22. Chris Johannessen and Tom Davenport, When Low-Code/No-Code Development Works - and When It Doesn't, Harvard Business Review, June 22, 2021. Available: https://hbr.org/2021/06/when-low-code-no-code-development-works-and-when-it-doesnt

23. Centre for Public Impact, What Is Sensemaking? January 13, 2022. Available: https://www.centreforpublicimpact.org/insights/what-is-sensemaking

24. Cognizant, (n.d.).What Is a Digital Platform? Available: https://www.cognizant.com/us/en/glossary/digital-platform#:~:text=What%20is%20a%20digital%20platform,for%20operations%20and%20customer%20engagement

25. Randy Howard and Larry Kerschberg, A Framework for Dynamic Semantic Web Services Management, International Journal Cooperative Information Systems, 13, 441–485, 2004. Available: https://www.semanticscholar.org/paper/A-Framework-for-Dynamic-Semantic-Web-Services-Howard-Kerschberg/32df75d3956edee9a191b567c8ff51f8fa1004ab

26. Hemesh Thakkar, Microservices Orchestration vs Choreography: What should you prefer? Accion Labs Group, January 5, 2023. Available: https://accionlabs.com/blogs/microservices-orchestration-vs-choreography-what-to-prefer]

27. JSON for Linking Data. (n.d.). Available: https://json-ld.org/

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.

Authors

Dr. Randy Howard, PMP, CSM, is Principal Enterprise Data Architect/Engineer/Scientist at The MITRE Corporation and is also an adjunct professor at George Mason University and Liberty University, author, researcher, and international speaker. He is a pragmatic and versatile engineer who blazes trails for organizations to realize their strategic objectives to overcome intractable challenges. He is codifying methodologies in a book titled "Navigating Wicked Problems: Going Where Traditional Systems Engineering Fears to Tread."

Ms. Geralyn Blossom, PMP, is a Division Operations Lead for the Air and Space Force Center's Operations in Contested Environments Division at The MITRE Corporation. She has 18 years of experience with the DoD and IC in military, private sector, and government civilian capacities. She holds a master's degree in Intelligence Studies and currently serves as a U.S. Navy Reserve Intelligence Officer for United States Central Command J2.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

©2024 The MITRE Corporation. ALL RIGHTS RESERVED.