Government Business Council

Community in the Cloud

Big Data and the IC

elastic

INTRODUCTION

As our world becomes ever-more digital, data management and protection are becoming more sophisticated and complex every day. While modern digital tools have opened up both novel communication channels as well as new ways of collecting and disseminating data, they have also created new potential threat vectors. As a result, good actors are working to increasingly identify, track and fight evolving national and international security risks in an effort to maintain and protect valuable data and communication channels. Caught in the middle of this evolving data landscape is the intelligence community (IC), whose work on a multitude of fronts require a data infrastructure that is equally adaptable and innovative. However, the legacy — and often siloed — systems of previous generations aren't equipped to deal with this new data frontier.

THE BIG ISSUE

The IC is in the midst of reimagining how it interacts with data. The era of big data has shifted focus from bilateral information sharing between siloed agencies to a macro vision that redefines data as a community-wide asset, with a reconfiguration of the data ecosystem to match. Intelligence agencies are pooling their knowledge around how to best go about this change while continuing to protect crucial data, but with massive amounts of unstructured data to contend with the question becomes: How are agencies adapting?

WHY IT MATTERS:

It’s imperative for the intelligence community to continue building this new ecosystem in order to maintain mission readiness in a rapidly evolving digital landscape. But the change does pose challenges to both technology and culture. Agencies must be able to leverage the value of their data effectively in order to make sure that any and all information that can protect American assets is going where it needs to go.

INTELLIGENCE COMMUNITY MEMBERS

Air Force Intelligence

Army Intelligence and Security Command

Central Intelligence Agency (CIA)

Defense Intelligence Agency (DIA)

Department of Energy Office of Intelligence and Counterintelligence

Department of Homeland Security Office of Intelligence and Analysis

Department of State Bureau of Intelligence and Research

Department of the Treasury Office of Intelligence and Analysis

Drug Enforcement Agency Intelligence

Federal Bureau of Investigation

Marine Corps Intelligence

National Security Agency (NSA)

National Geospatial-Intelligence Agency (NGA)

National Reconnaissance Office (NRO)

Office of Naval Intelligence

Office of the Director of National Intelligence

U.S. Coast Guard Intelligence

U.S. Space Force[1]

THE INTELLIGENCE COMMUNITY STRATEGY

The National Intelligence Strategy of 2019 and the 2017 Intelligence Community Information Environment (IC IE) Data Strategy both lay out both the challenges and opportunities that the intelligence community faces.

NATIONAL INTELLIGENCE STRATEGY, 2019

The NIS highlights the need for digital transformation and increased data analysis capabilities, moving toward tools that can quickly process and disseminate information from a vast and integrated pool of intelligence data across agencies.

> “Advances in communications and the democratization of other technologies have also generated an ability to create and share vast and exponentially growing amounts of information farther and faster than ever before. This abundance of data provides significant opportunities for the IC, including new avenues for collection and the potential for greater insight, but it also challenges the IC’s ability to collect, process, evaluate, and analyze such enormous volumes of data quickly enough to provide relevant and useful insight to its customers.”[2] **(NIS, 2019)**

THE INTELLIGENCE COMMUNITY STRATEGY

INTELLIGENCE COMMUNITY INFORMATION ENVIRONMENT DATA STRATEGY, 2017 - 2021

The Data Strategy focuses on “freeing data” — separating valuable information from its source and ensuring that information is available and searchable for other members of the community.

The IC Strategy further outlines two goals that specifically center on building and maintaining enhanced foundational IC IT capabilities and analytic technology.

STRATEGIC OBJECTIVE 4

Find, create, and deploy scientific discoveries and new technologies, nurture innovative thought, advance tradecraft, and constantly improve mission and business processes to advance the IC in a rapidly changing landscape.

STRATEGIC OBJECTIVE 5

Develop, enhance, integrate, and leverage IC capabilities and activities to improve collaboration and the lawful discovery, access, retrieval, and safeguarding of information.

Both strategies reimagine the way that the IC serves its customers, highlighting the strengths of integrated and collaborative data sharing when it comes to identifying and responding to threats as well as serving both the individual and collective mission of the community.

> “The environment must embrace a more disciplined approach to intelligence integration by ensuring that data is sharable, discoverable, accessible, retrievable, and protected.”
>
> **(IC IE Data Strategy)**

IT DECISION MAKERS

Thought leaders and decision makers within the IC IE are focusing on both building the IT environment and extracting what they need from it. Big data is not a new concept for this community, but with an increasing number of collaboration and data warehousing tools, decision makers have to balance the ability to triage the volume and velocity of big data, with the precision that allows intelligence analysts to draw conclusions about smaller data —

INTEGRATION

Decision-makers in the intelligence community understand that technological innovation is critical to mission advantage in a fully integrated and agile IC.

An integrated system allows fully accessible data across the IC environment, strengthening agencies' ability to rapidly identify and respond to threats. However, this also increases the volume and velocity of data accumulation, making it crucial to develop integration strategies that effectively engage both human analysts and machine analytics.

HYBRID COMPUTING ENVIRONMENTS

The IC is moving toward serving the various needs of its agencies by creating a hybrid computing environment that satisfies both the flexible and rigid requirements of data sharing and analytics.

The DNI Strategy notes that "IC leaders and managers have promoted a culture of collaboration and integration along with unification of intelligence activities to deliver shared IT services and capabilities across the IC [...] Information that is better organized and enriched by metadata will enable the transition to information-centered intelligence processes."[3]

CLOUD

The IC's critical need for rapid and secure data sharing has led to a particular investment in cloud solutions. The development of the Intelligence Community Information Technology Enterprise (ICITE), established in 2012, created the first collaborative program for intelligence analysts, with two cloud-based systems providing different services.[4]

- Multi-cloud solution is necessary for unclassified, secret, and top-secret networks to make sure that the right people are accessing the right information.

- Networks must be integrated and interoperable, with the goal of maximizing rapid reuse and sharing of data between systems.

THE FLEXIBLE: COMMERCIAL CLOUD ENTERPRISE (C2E)

C2E is an elastic computing environment that provides infrastructure as a service, allowing agencies to take advantage of cloud services only when needed.

Multi-cloud acquisition is intended to support the adoption of emerging technologies, including artificial intelligence and machine learning.

Developed by the CIA, C2E is one of the government's largest ever commercial cloud contracts. Hosted initially by Amazon Web Services, the community is now looking toward "best-athlete capabilities," moving into a multi-cloud environment that takes into account vendor strengths when choosing which platform best supports the mission.[5]

CLOUD

THE RIGID: GOVCLOUD

In addition to the C2E, the NSA is also looking to expand its on-premises hybrid computing initiative "GovCloud," which John Sherman, former CIO of the IC, described as a "high-performance analytics environment … an operation of massive scale where agencies can correlate their data at massive scale against NSA's very significant [signals intelligence] holdings."[6]

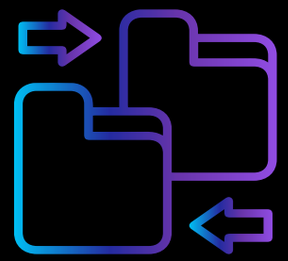
GovCloud addresses the more rigid signal intelligence needs of the NSA, functioning essentially as a warehouse for storage and analytics. "There is nothing elastic about what goes on with the mission at Fort Meade … and the software they have in GovCloud now needs to run, in some instances, on bare metal to be able to get that extra oomph of performance off of that," Sherman reported to FedScoop.

Both cloud systems address the disparate needs and customers of IC agencies and allow the community to tackle big data at scale. The first iterations of collaborative programs like ICITE built cloud systems that are multifunctional, secure, and adaptable. The new evolution of cloud systems must go deeper, equipped with the ability to assist analysts by asking questions of the data, noticing patterns, and reducing the time that analysts spend looking for individual pieces of information.

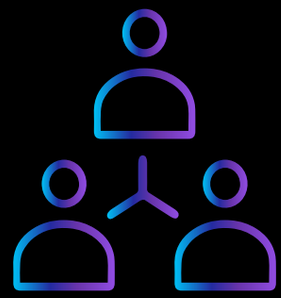
This cloud-based, communal environment has already seen successes, many of which likely remain unknown. A known victory: The National Geospatial Intelligence Agency (NGA) credits data from ICITE in its analysis that rapidly linked the Syrian government to the chemical weapons attack in August of 2013 that killed 15,000 people.[7]

THE CULTURE CHALLENGE

Intelligence agencies have been siloed for most of their history, creating “data empires” that can be difficult to share or reshape. This cultural shift — stressing the importance of **liberating data and sharing knowledge** — has been a major part of the NIS and IC IE Data Strategy.



Organizing, tagging, and transforming the data that agencies already have into usable and shareable quality is also a monumental task, requiring both machine and human analysis that must simultaneously absorb new information while working with backlogged information.



The **merging of the disparate agencies** of the IC into an interoperable system takes imagination and innovation that must evolve with changing priorities and capabilities.

WHAT'S NEXT?

CONTINUED CONNECTION: AI

Further modernization will certainly integrate artificial intelligence and machine learning tools to be able to interpret and extract critical information. The IC's 2020 Principles and Framework of Ethics for AI highlight the technology's ability to "analyze and connect disparate data, infer meaning and ultimately make analytic judgments based on all available data." Various arms of the IC have already implemented AI programs, including the DoD's Integrated Crisis Early Warning System (ICEWS) and the Mercury program developed by the Intelligence Advanced Research Projects Activity (IARPA) to continuously and automatically analyze foreign SIGINT data.[8] As with the development of collaborative cloud environments, the DoD is looking to create a "connective tissue" between silos through its Joint Artificial Intelligence Centre (JAIC). In September 2020, the JAIC awarded a $106 million contract to build out the Joint Common Foundation Artificial Intelligence and develop AI-as-a-Service, a move that will undoubtedly have implications for the intelligence community.[9]

Increased automation, collaboration, and data-sharing throughout the intelligence community will make it easier to detect patterns and threats, tag key information, and rapidly share data across silos, all in service of the core mission — protecting the American people.

> "Emerging technologies are already reshaping how the IC gathers, stores, and processes information, but will likely transform all core aspects of the intelligence cycle in the coming decades — from collection to analysis to dissemination."[10]

ELASTIC INDUSTRY PERSPECTIVE

Mike Kilrain | *Regional Vice President*, **Elastic**

The appetite for big data has not diminished. The challenge now is bringing together the right data to the right people at the right time to close the understanding gap: the gap between what you think and what is real. Whatever the adversary, whatever the threat or vulnerability, closing this gap is a necessity for decision makers and for mission success.

What's needed are tools and processes that support an iterative loop from data collection to insight to action. Speed is paramount. Legacy tools and manual processes are too slow and are barriers to multi-source correlations that provide a global view. We must simplify and speed up search and analysis for people and machines. We must break silos with secure, open, and programmatic interfaces to all data sources. And we must build an open enterprise that can be extended, improved, and customized when the mission demands it (and not just when a vendor gets around to it).

Delivering operational and mission data to analysts, operators, agents, ITOPS, and executives, is very much like running an efficient supply chain. Unlike our adversaries who can cut corners and are not bound by laws and due process, we must create strong policies and processes to secure and protect our data assets. We must continue to work to get this right while not impeding progress. The stakes are high and the risks will only increase if we fail to create a well-oiled and timely data supply chain.

Elastic is uniquely positioned to help close the understanding gap by building effective data supply chains. Searching at scale is the core of everything we do. Elastic is a software company that delivers three powerful solutions built on a single free and open stack. With Elastic Enterprise Search, you can connect and search across all your data repositories and easily add modern search experiences to your applications. With Elastic Observability, you can enjoy a single pane of glass to view, monitor, and understand your IT enterprise. And with Elastic Security, you can protect and respond to known and unknown threats across endpoints and networks with the help of machine learning. Operationalizing search has the power to minimize the gaps between data and understanding, and insight and action, for the community. Let's get it right together.

Government Business Council

ABOUT GBC

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research analysis. Email us for more information!

EMAIL GBC

elastic

ABOUT ELASTIC

From revealing insights into the economy to analyzing data from Mars in real time, Elastic helps government organizations bring the speed, scale, and security of free and open to their mission-critical projects. The Elastic Stack and related solutions are designed to run on premises, in public or private clouds, or in hybrid environments. Elasticsearch Service on Elastic Cloud is FedRAMP authorized and available on AWS GovCloud. Elastic products are fully compatible with legacy tools to facilitate IT modernization. Elastic also offers a full complement of consulting, development, technical audit, training, and support services to ensure government user success with cleared personnel who have experience in agency programs, standards, and requirements.

LEARN MORE

ENDNOTES

1. DNI. “Members of the IC.” https://www.dni.gov/index.php/what-we-do/members-of-the-ic.
2. Director of National Intelligence. “National Intelligence Strategy for the United States of America.” 2019. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf
3. ibid
4. FedTech. “The Intelligence Community Moves Towards a More Secure, Integrated Cloud Environment.” September 12, 2016. https://www.nextgov.com/sponsors/fed-tech/2016/09/intelligence-community-moves-toward-more-secure-integrated-cloud-environment/131453/
5. FedTech. “Where Will the CIA Go Next with Its New Cloud Contracting Vehicle?” December 10, 2020. https://fedtechmagazine.com/article/2020/12/where-will-cia-go-its-new-cloud-contracting-vehicle
6. FedScoop. “NSA plots the evolution of GovCloud in new acquisition.” February 19, 2020. https://www.fedscoop.com/hybrid-compute-initiative-intelligence-nsa/.
7. FedTech. “The Intelligence Community is Sharing More Data, and Making IT More Secure.” July 22, 2016. https://fedtechmagazine.com/article/2016/07/intelligence-community-sharing-more-data-and-making-it-more-secure
8. IARPA. “Mercury Program.” https://www.iarpa.gov/index.php/research-programs/mercury
9. Federal News Network. “DoD’s AI center striving to be connective tissue across all projects.” February 16, 2021. https://federalnewsnetwork.com/reporters-notebook-jason-miller/2021/02/dods-ai-center-striving-to-be-connective-tissue-across-all-projects/
10. CSIS. “The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for US Intelligence.” April 17, 2020. https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence