One of the core tenets of these reports and legislation was the need to share information across the IC, as well as with the larger interagency and state and local authorities, necessitating investments in IT networks, as suggested by this image of technicians working in a server room.

Driving IT Integration

Patrick Gorman

Patrick Gorman is the CEO of Cynomiq, an AI-driven cyber security posture-management platform. Previously he served in various executive roles at Booz Allen, Bank of America/Merrill Lynch, Bridgewater Associates, as well as the acting chief information officer in the Office of the Director of National Intelligence.

At the core of the intelligence cycle of collection, processing, analysis, and dissemination is information which over the years has relied upon sophisticated information technology systems to manage an increasing volume, variety, and velocity of data from the various intelligence agencies. Both the 9/11 and WMD Commissions focused on the need to better share that data, while protecting security and privacy. This article looks at the evolution of information technology in the Intelligence Community, IRTPA's role in driving transformation, and the way ahead as new technologies around AI and quantum take hold.

Since the modern national security enterprise emerged in the mid-20th century, the US IC and the Department of Defense have been at the forefront of digital technologies, including having had a significant role in early innovation in Silicon Valley. As the Cold War advanced, the need for advanced microelectronics and data processing systems were critical for early signals-intelligence and electronic-warfare capabilities.

In that era, the IC drove many innovations in mainframe telecommunications, computing, data storage, and analytic tools, followed by a wave of digital technologies of mainframes, minicomputers, microcomputing, and finally internet technologies.

More importantly, given the sensitive nature of the information collected, the IC took the lead in critical areas of cryptology and what would later be called (after iterations of computer security and information assurance) cyber security. The establishment of the US Communications Security Board in 1953 was an interdepartmental effort to protect US national security systems. In 1967, the DOD-commissioned Ware Report established the foundation of a broader set of computer security controls, including information labeling, encryption, access controls, auditing, secure systems development and accreditation, and storage segregation.[a]

These recommendations became the basis of the Trusted Computer System Evaluation Criteria (often referred as the "Orange Book"), which set standards for protecting classified information and were developed by the National Computer Security Center at the NSA in the early 1980s. To better drive policy and adoption, in 1990 the White House issued National Security Directive 42, which created what is now known as the Committee of National Security Systems to better align DOD and the IC.

As the internet expanded and commercialized with MOSAIC browsers in the early 1990s, DOD and the IC modernized their networks through layered infrastructures based on varying classification levels (e.g., NIPRNET, SIPRNET, and JWICS).[b] Other innovations in the 1990s include Intelink, which leveraged internet technologies to improve information sharing and collaboration across all three layers of classified networks: top security, secret, and unclassified.

Catalyst for Change

In the wake of the 9/11 terrorist attacks and US invasion of Iraq, the resulting review commissions provided recommendations that led to the Intelligence Reform and Terrorist Prevention Act becoming law in December 2004. One of the core tenets of these reports and legislation was the need to better share information across the IC, as well as with the larger interagency and state and local authorities. Two organizations were created within the Office of the Director of National Intelligence to address this: a chief information officer of the IC and a program manager for the Information Sharing Environment.

The IC Chief Information Officer (IC CIO) was deemed so critical to Congress that the position is a presidential appointment subject to the advice and consent of the Senate, one of only a handful of positions to be so designated. IRPTA gave the DNI (and IC CIO) authorities to establish enterprise-architecture and security requirements and standards, to direct all enterprise architecture related procurement for the IC, and to drive integration and develop multi-level security capabilities.

The ISE program manager was established in 2005 to improve terrorist-related information sharing across federal, state, and local government; the private sector; and foreign partners. The ISE shared space was designed as a decentralized, distributed repository of connected systems with a federated query system to provide greater access to terrorism related data. Congress later added WMD and homeland-security information into the mandate.

From Mandate to Action

ODNI sought to further clarify roles, update laws and directives like Executive Order 12333 and the Foreign Intelligence Surveillance Act, and translate mandates into action through

a. Willis H. Ware, Security and Privacy in Computer Systems (RAND Corporation, April 1967).
b. MOSAIC browsers were pioneered by the National Center for Supercomputing Applications in the early 1990s.

a series of initiatives that were designed to quickly drive outcomes and field new capabilities. The initiatives around information technology and information-sharing fell into three categories: policy and directives, architecture and standards, and technology solutions.

The policy and directives work focused on striking a balance between need to know and need to share ensuring that data discovery and access was supported by improved cyber security efforts to protect critical national security data. Intelligence Community Directive 501 established the roles of collection and analytic production stewards in each element whose role was to ensure that all intelligence could be "discovered" through the use of meta data with enough detail so that analysts and operators could find information that was relevant to their mission and request further access. An exemption process was established to ensure that sources and methods were protected if deemed so by the data steward and approved by the DNI.

The other policy bookend was ICD 503, "Intelligence Community Information Technology Systems Security Risk Management," which established the rules for security assessments and security authorizations of new information technology systems. This work was further expanded through the Committee on National Security Systems, a joint DOD-IC effort to ensure greater standardization and harmonization on IT systems that resulted in the National Institute of Standards and Technology Publication 80053A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans." This work helped enable the concept of reciprocity to better facilitate authority to operate across different agencies. Moreover, the NIST 800-53A standard and its revisions have become the bedrock for the broader cyber security community in the commercial and federal organizations, protecting critical information and national security information and continuing the impact of the IC outside of the national security community.

The increasing importance of big data required greater leadership and direction on data interoperability and standardization so it could be better integrated and analyzed in support of various missions. To that end, ICD 504, "Intelligence Community Data Management," established the IC Chief Data Officer to oversee this effort. The IC CDO was responsible for working with the agency CDOs to implement data tagging, to include legacy electronic data, for the purpose of improving discoverability, accessibility, and usability while protecting security and privacy.

The second role of IC CIO is to drive overall strategy, architecture, and information technology roadmaps for the enterprise. Beginning in 2008, a series of initiatives were folded into what became the IC Information Technology Enterprise. IC ITE was based on a framework of a common platform infrastructure, common back-office design, an applications mall, and a single IC desktop. At the core of this was the adoption of an IC cloud architecture and IC data center that leveraged commercial cloud provider systems (e.g., Amazon Web Services and Microsoft) to ensure that the IC technology base kept pace with commercial innovations.

The third role of the IC CIO was to ensure that real capabilities were being fielded and ensure oversight of major enterprise IT programs and projects (mission-systems acquisition was provided by a separate ODNI office with the IC CIO in a supporting role). These programs fell into four areas: common cloud infrastructure, cross-domain solutions, incident response, and collaborative tools:

- The common cloud infrastructure was started in 2008 with the IC Data Center initiative and detailed out the IC ITE program resulting in an award to Amazon Web Services in 2014. This innovative approach moved from a more traditional siloed infrastructure toward a community-wide cloud that

leveraged best of breed technologies and commercial best practices, greatly accelerating technology adoption, and providing services that more resembled what commercial enterprises and consumers were accustomed to in terms of data access and apps.

- The Unified Cross Domain Management Office (UCDMO) was established in July 2006 as a joint DOD-IC effort for the creation of secure connections between different network domains (e.g., top secret, secret, and unclassified). Before the UCDMO, various multilevel security tools were developed by various services and agencies, creating duplication of effort and inefficiencies.
- The IC Incident Response Center was created to ensure better cyber security operational coordination across the various intelligence agencies who ran their own security operations center and incident response teams. As networks, systems and data become for available across agencies, the IC CIO wanted a mechanism to better understand threats and vulnerabilities, improve shared situational awareness, and synchronized and coordinate actions in the event of a cyber security incident.
- Intellipedia was established in 2006 to create an analytic collaboration environment with the functions of the popular Wikipedia and consisted of three wikis: Intellipedia TS, Intellipedia-S, and Intellipedia-U that were hosted on their respective networks. This provided a space for analysts to collaborate on shared missions and topics.

Looking Forward

The IC has made significant progress in improving the basics in place in terms of policy, strategy, architecture and standards, solutions, and shared infrastructure. However, the next wave of technologies is challenging IT leaders to harness the power of AI, leverage automation for greater speed and efficiencies, and ensure the IC gets the benefit of quantum technologies, both in terms of new capabilities and protecting national security systems.

Artificial intelligence, particularly the domains of generative AI and large language models, presents a significant opportunity for the IC to generate insights from vast amounts of data, both structured and unstructured, and other forms of media. The ODNI established the Augmenting Intelligence Through Machines (AIM) Innovation Hub and developed a strategy in 2019 to guide the community's efforts in AI. However, like previous technology waves of mainframe, client-server, and cloud, AI presents new risks (e.g., data poisoning, evasion, extraction) that must be addressed through new policy guidance, procedures, technology, and training. AI will reshape the information technology landscape, architectures, security and budget in the same way that the cloud transformed how we delivered technology.

Another technology that can help the community become more agile and efficient are business process automation tools. BPA helps to better define, streamline, and orchestrate critical processes in core areas of collection, processing, analysis, and dissemination, as well as in back-office functions. Combined with AI, BPA is a transformational technology that should be harnessed with the AIM Innovation Hub.

While practical applications are still some years out, quantum computing will significantly alter the IC technology landscape over the next decade. It has the potential to solve complex problems and address modeling and simulation challenges that are difficult for classical computing. However, like AI, quantum poses real risks in an adversary's ability to use a cryptanalytically relevant quantum computer. The IC CIO will need to develop a plan to baseline and risk assess existing systems and migrate to quantum-resistant public-key cryptographic system. Given the adversary strategy to "exploit now and decrypt later" this effort must be put on the fast track.

For 70 years, information technology has gone hand in hand with the US national security enterprise. A large part of that success was the close partnership with the private sector, with the government providing core R&D funding and allowing the private sector to scale up new technologies through venture capital investment. Organizations like In-Q-Tel and the Defense Innovation Unit help with these commercial partnerships, but more needs to be done. The barriers, such as the long process for obtaining security clearances, an onerous contract and acquisition process that disincentives private business from doing government work, and a more robust process to secure software for classified networks need to be addressed to ensure the IC can ride the next technology wave. ■