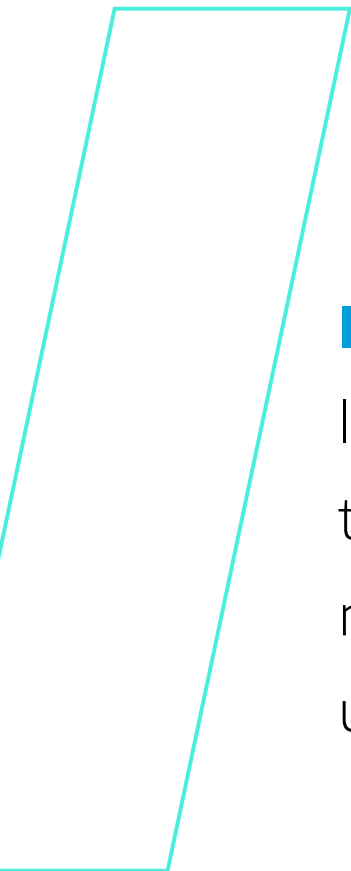


IT Modernization in the IC **Part I**

Expert Dialogue

How advanced technologies support IC mission effectiveness





In the Intelligence Community, a fast-changing global security landscape is creating unprecedented operational pressures. The IC is tasked with tracking near-peer threats worldwide, while also addressing rising cybersecurity concerns. All this is driving a need for technology upgrades in general and for network modernization in particular.

Jill Singer, vice president of national security and defense for AT&T Public Sector, describes in part I of the IT Modernization in the IC series, how technological enhancements can help the IC to meet mission more effectively, while also ensuring a higher level of cyber protection.

What are some of the IC's most pressing challenges?

They have a global mission to collect, process, analyze and disseminate information to the top government leaders. And the list of threats that the IC tracks is ever-growing, whether it's China, Russia, Iran, the pandemic, climate change, drugs, organized crime, terrorism, and more. To respond to all of the threats and the requirements, the IC needs to have advanced IT resources to process and digest such data.

Given the vast volume of data, the IC is adopting technologies that can modernize and transform collection analytic capabilities. By doing so, it can maintain its advanced strategic awareness of emerging threats and address the tactical issues of the day.

How do the IC's needs differ from those of other federal agencies?

There are some similarities with other federal agencies that also have a global mission. Many have experienced an exponential increase in the need for worldwide bandwidth. But the IC also has some unique circumstances related to both security and timeliness.

By definition, IC agencies are required to operate in closed, secure environments—both physical and virtual. At the same time, their mission applications demand lower latency and faster response times: For the IC, seconds actually do matter. In fact, it's a challenge to implement commercial hardware, software and technologies. IT modernization requires an extra effort, because of their unique operating environments.

“IC agencies are required to operate in closed, secure environments—both physical and virtual.”

How does IT modernization help the IC meet mission?

Information technology allows the IC to keep its people focused on activities that are uniquely reserved for human intellect and brain power. With artificial intelligence, for example, they can analyze mountains of data with less manual processing. That creates improved effectiveness for both mission collectors and administrative support personnel.

They're also focused on evolving and adapting their cybersecurity postures within the Zero Trust framework as outlined in the recent presidential Executive Order. The IC agencies are working to mitigate constant cyber threats, while also maintaining the high availability of their mission-critical IT infrastructures.

The implementation of advanced telecommunications technologies—software-defined networking, 5G mobility and Internet of Things—can help to improve the way these agencies operate, while providing flexible, elastic network capacity and highly secure access at the edge.

How can commercial capabilities support the IC in achieving its modernization goals?

Companies such as AT&T are continuously investing in infrastructure to optimize day-to-day operations. IC agencies can leverage these innovations to accelerate their own digital transformation. For example, we have implemented software-defined technologies, orchestration in our core network, the use of open-source technologies, and 5G. We are driving convergence of mobile and wireline infrastructures into a comprehensive network ecosystem. All of which can support the diverse needs of the IC.

Cloud infrastructures are critical to our business, and we're engaging some of the large hyperscalers to handle key parts of our infrastructure. These resources are also integrated into the solutions that we deliver to our customers. We have one of the world's most powerful global backbone networks serving hundreds of millions of subscribers. And we've also proven that running a network in the cloud drives speed, security, cost improvements and innovation. These strategic decisions allow us to focus on what we do best—operating those networks in support of mission-critical activities for our customers.

Why is software-defined networking the future solution for the IC?

It's all about agility.

With software-defined networking, IC agencies can quickly update their architectures and services through a software change, rather than having to purchase and deploy new hardware, which on a global scale is time consuming and expensive. They can provision new network services, scale bandwidth up or down, maintain and update a variety of network functions—all from a centralized location. Software defined networks allow them to avoid vendor lock-in, which means they have more freedom to try new solutions and new capabilities as quickly as they emerge. This is the kind of flexibility that the IC needs to keep pace in an ever-changing threat environment.



Jill Singer



What is the role of commercial innovation in supporting cybersecurity efforts within the IC?

Whether it's a 5G wireless network or a traditional wireline network, we focus on making sure that layers of security are integrated throughout the architecture of the network. That enables us to predict, respond and correct any malicious activities that might occur on the network. 5G combined with Edge Computing allows data considered sensitive or proprietary to be kept locally within an agency's internal network, which can keep private data within their control. And edge security controls can provide broader, more centralized visibility across the entire attack surface, compared with legacy security controls.

How receptive are the IC agencies in adopting newer technologies?

As a whole, the IC agencies are extremely open to new technologies. The people within the IC community are smart, capable, adaptive and forward-looking. They want the best tools and technologies to help them meet mission.

Across the IC, we see robust use of commercial cyber-defense capabilities. We are also seeing a shift from government-owned, government-operated networks, toward more managed-services networks. That demonstrates their openness to bringing in partners: The IC agency still retains ownership, but they are working with commercial providers on the engineering, implementation and operation of those networks.

“We are seeing a shift from government-owned, government-operated networks, toward more managed-services networks.”

How can the IC begin to pivot toward these modernized solutions?

In the near term, 5G is going to be a real game-changer, as IC agencies begin to explore its application toward specific mission goals.

Technology modernization calls for a bit of the classic “think big, start small” approach. IC agencies can evaluate emerging technologies and conduct test pilots. Implementing 5G in an unclassified environment gives the IC a chance to understand how these technologies can enhance operations, so they can assess the utility of those technologies to meet their needs.



In Part II, we'll continue to explore the implementation path for IC agencies looking to improve their technology posture.



att.com/publicsector