EDITORIAL WHITEPAPER

C4ISR&NETWORKS
www.C4ISRNET.com

Rethinking ISR

Underwritten by:
Brocade

NEW TECHNOLOGIES FOR ISR

Rethinking ISR

How innovations like SDN change the ISR mission

BY JOHN EDWARDS

The military is rethinking its intelligence, surveillance and reconnaissance (ISR) mission to address an increasingly dangerous world as well as budgetary pressures.

The services are addressing emerging threats with fresh approaches and technologies. Innovations, such as software-defined networking solutions, offer benefits including reduced size, weight and power and an ability to adapt to increasingly dynamic environments. Redefining ISR with these added capabilities promises to exert a positive ripple effect across the enterprise, improving agility, enhancing performance and reducing risk from the data center to the war fighter.

ADDRESSING THREATS

The world is becoming an increasingly unstable, unpredictable and dangerous place. New threats appear regularly and the military must be prepared to respond immediately, efficiently and capably. Whether it's preparing for a possible cyber attack, responding to a disease outbreak, or targeting an expanding fanatical enemy who works in the shadows, today's military faces multiple, rapidly evolving threats that were unimaginable a generation ago.

Legacy ISR and support infrastructures, designed for a different type of world, are now failing to help commanders and war fighters meet essential mission goals. However, exciting new solutions are entering deployment to replace or augment aging ISR technologies and related systems.

"The [Department of Defense] has put the big defense contractors on notice that they need to be as innovative as a startup is when it comes to fielding new ISR systems," said Col Cedric Leighton (ret.), a former deputy director of training for the National Security Agency and chairman of Cedric Leighton International Strategies, a consulting firm located near Washington, D.C.

INTEGRATED SENSOR ARCHITECTURE

The Army has multiple legacy sensor systems in theater that communicate only with specific systems. This limitation makes sharing actionable information beyond set parameters a burdensome and costly point-to-point integration task. The arrangement also poses a growing deployment challenge as emerging sensor technologies become available.

"We want sensor systems to collaborate," said Joe Durek, deputy director of the Modeling and Simulation Division of the Communications-Electronics Research, Development and Engineering Center (CERDEC) Night Vision and Electronic Sensors Directorate (NVESD) in Fort Belvoir, Virginia. "We shouldn't need countless server racks to do this, and a soldier shouldn't need a Ph.D. to configure all these. He just needs to be able to bring up a sensor, control it and understand its data."

The Integrated Sensor Architecture (ISA) foundational architecture, developed at CERDEC NVESD, establishes standards to bring together sensors within an area of operation so they can communicate with each other without physical, point-to-point integration.

"The idea is that a sensor can come online to a network, register and communicate its capabilities to the network and, in turn, other assets and sensors on the network can subscribe to the types of information they want or don't want — basically like a filter," Durek said. "Now, you have this fundamental architecture enabling sensors to not only recognize the systems they want to interact with but to also broker the information exchanges."

ISA utilizes a capability called dynamic discovery to find other ISA-compliant systems on the tactical network and relay information to operators. "For example, a soldier may not know that another unit's aircraft is flying over or that a convoy is passing through, but ISA's dynamic discovery will automatically identify the system, couple with it, and provide the sensor's information directly to the soldier," Durek said. The technology is designed to improve a mobile soldier's situational awareness by providing the ability to query different sensors as the individual moves through an area and accesses information that was previously unavailable, such as event messages or spot reports.

"We developed ISA under the Deployable Force Protection program, which seeks to provide the critical capabilities needed for a forward operating base to defend itself — one of those being interoperability," said Christine Moulton, the ISA project lead at CERDEC NVESD. She noted ISA stands apart from other interoperability architectures because it is designed to work in the tactical

NEW TECHNOLOGIES FOR ISR

environment.

"We assumed [the soldier] would have bad communications, small bandwidth and intermediate communications, so we designed it to handle those situations and recover," Moulton said. "We even have a working prototype that we've tested in the field." Over the past four years, all DFP projects have been ISA-enabled, ISA-compliant and communicating over the ISA network.

CERDEC has a formal technology transition agreement (TTA) with the Program Executive Office Intelligence, Electronic Warfare and Sensors (PEO IEW&S) under its Sensor Computing Environment program (Sensor CE). Sensor CE is a component of the PEO IEW&S mission, which has a portfolio that covers a broad range of capabilities across the reconnaissance, surveillance and target acquisition spectrum.

"We've worked closely with PEO IEW&S doing multiple integrations of ISA with their BETSS-C systems and standard ground system," Moulton said. "The TTA allows us to not only transition all the work that we've done to Sensor CE, but it also allows us as an R&D organization to continue working closely with them, informing Sensor CE in the future of how best to go about adding new features into ISA capabilities that they want to add." She noted the agreement is the first step in a continuing process to develop technology options that will make Sensor CE a reality. "And that, ultimately, will provide the soldier a full picture of the battlefield so he or she can make even better decisions."

> 'We want sensor systems to collaborate. We shouldn't need countless server racks to do this, and a soldier shouldn't need a Ph.D. to configure all these.'
>
> **Joe Durek, CERDEC NVESD**

NEXT-GENERATION ISR NETWORKING

Many different technologies are used for ISR, including wireless sensors, imaging devices and handheld radios. All of these systems require fast and reliable network support to feed data warehouses and big data analytics platforms as well as to deliver vital information from servers to analysts, commanders, war fighters and other individuals who require fast access to actionable insight and intelligence wherever they are located.

Legacy networks struggle to keep pace with an increasingly mobile, adaptable and information-driven military. Today's military leaders, working in close cooperation with commercial partners, are planning and developing a new generation of fast, reliable and flexible network technologies.

One of the most promising developments in ISR communication is software-defined networks (SDNs), a new approach that unbundles the traditional device-bound, vertically integrated network stack to provide greater network automation, architectural flexibility and programmability for policy-driven control and self-service innovation. SDN technology allows military users to achieve the network agility required by increasingly dynamic environments. SDNs can also disaggregate traditional, vertically integrated networking stacks to improve manageability, increase network service velocity and customize network operations for specialized environments all the way up to the tactical edge.

"Software-defined networking is a way to orchestrate the delivery of services and applications from the data center to the client," said Vince Garr, senior systems engineer in the federal unit of network solutions provider Brocade, located in Herndon, Virginia. "You can do it in minutes, hours and days rather than days, weeks and months."

SDN technology works by separating a network's control and forwarding planes, making each easier to optimize. In an SDN, a controller supplies an abstract, centralized view of the overall network, allowing network administrators to quickly and easily make and enact decisions on how underlying systems, such as routers and switches, on the forwarding plane will manage network traffic.

With a centralized, programmable network that can automatically and dynamically handle changing requirements, an SDN can deliver increased agility and flexibility. Adopters can quickly and efficiently deploy new applications, services and infrastructure components to meet quickly changing goals and objectives. SDNs also foster innovation, allowing the creation of new kinds of applications and services specifically designed to address specific mission parameters and goals.

Although they were initially designed for data center environments, SDNs have taken the networking industry by storm due to their cost savings, the ability for customization and operational flexibility they provide, including virtualization, orchestration and automation, said Josip Pilipovic, a computer engineer in the communication networks and networking division of CERDEC's Space & Terrestrial Communications Directorate (S&TCD) in Fort Belvoir, Virginia.

"SDN architecture implies the separation of control and data planes, but these tactical edge characteristics do not allow for

NEW TECHNOLOGIES FOR ISR

strict separation of data and control planes," Pilipovic said. "CERDEC S&TCD is looking at a hybrid architecture that would allow for the autonomous operation of wireless switches while retaining the benefits of a SDN architecture." The Army's SDN-based ISR network will implement SDN controllers to perform policy updates and enforcement functions and network virtualization, Pilipovic said. The SDN controllers will also be used to determine what to do with unknown/unexpected packets and other functions.

The wireless switches will perform neighbor discovery and autonomous link layer routing functions within their area of responsibility. "It will be important to provide network connectivity and packet delivery without controller intervention," Pilipovic said "One of our goals at S&TCD is to create an Army SDN architecture that provides the following: minimal or no configuration required, ease of maintenance and reduced number of protocols, scalability for large networks, optimum multicast and unicast forwarding, faster convergence times and robust loop mitigation and/or preventions."

Sitting at the tactical edge, an ISR network is substantially different from networks operating within a conventional data center environment. An ISR network must often cope with unreliable and low data-rate wireless links as well as mobile nodes with no fixed network infrastructure. Meanwhile, units subject to reassignment often create reconfiguration needs. Additionally, it's necessary to implement broad surface cyber protection because firewalls aren't limited to gateway nodes. Multi-level Secure Networks also need to be considered.

> 'In theater [with SDN] you can respond very quickly to networking problems. So, if a virtual router fails, it essentially takes three minutes to try to figure it out.'
>
> **Vince Garr, Brocade**

Garr noted SDN's speed and flexibility is often crucial to a team on the tactical edge. "To a war fighter in theater, to have the power to make that decision, or to have someone else see something fail and have that power to make that decision remotely on their behalf, is pretty powerful," he said. "It also shows that the appliance doesn't have to be treated in a very special manner by a certified technician who only knows how to work on that box, so it eliminates an awful lot of the cumbersome prospects of networking today."

SDNs are also easier to maintain and repair than conventional networks. "In theater [with SDN] you can respond very quickly to networking problems," Garr said. "So, if a virtual router fails, it essentially takes three minutes to try to figure it out and, if you can't, you can take a known, good copy of it and start it up in its place and bring the service back online."

Since SDN promises to be a key component in the Internet of Things, the military will find it necessary to address the technology from various aspects, according to Leighton. "They can both use SDN and evaluate the effects of SDN on military operations," he said, noting that SDN will also likely characterize adversary networks in the near future. "They will have to be understood before they can be exploited for intelligence purposes."

Garr noted an SDN can be easily deployed in stages without disrupting legacy network services. "The idea is that instead of forklifting your network to get a whole new solution from a vendor, you could buy from your current network provider and, when you want to implement SDN, you can do it on a port-by-port basis or on a service by service basis, depending on the application," he said.

MEETING NEEDS AND REQUIREMENTS

ISR technologies are supposed to be based on requirements levied by the combatant commands, the forces in the field that have the most potential for direct contact with the enemy. Yet, according to Leighton, this isn't always the case. "In practice, you don't always know what you need or want, so the requirements process is not as responsive as it could be," he said. "Also, sometimes the headquarters level of a combatant command is out of touch with what its forces in the field really need."

During the conflicts in Iraq and Afghanistan, former Secretary of Defense Robert Gates rejuvenated the Joint Urgent Operational Needs (or JUONS) process. According to Leighton, this initiative had the effect of fast-tracking technological initiatives and bypassing the more cumbersome traditional requirements process that went through the Joint Requirements Oversight Council. "The joke about the JROC process was that it 'never met a requirement it didn't like,'" Leighton said.

Gates also gave the ISR Task Force (ISR TF) added muscle. "So, between the JUONS process and the ISR TF, a lot of new technological advancements in the intelligence collection, surveillance and reconnaissance areas were developed, implemented and fielded," Leighton said.

New ISR technologies are evaluated and assessed by both vendors and the DoD. "Some are tested at labs, some are tested

NEW TECHNOLOGIES FOR ISR

operationally," Leighton said. "Ideally, they are tested in both environments."

What's needed is an acquisition strategy that embraces open networking to ensure that the network supporting the mission doesn't become so outdated that the network outlives the standards body that originally supported it.

"It seems that the technology has marched on and vendors only support the standards when there is profit," said Garr. "By open, Brocade defines this as open standards, open systems, or even open source. By taking this approach, the DoD will ensure that the feature requirements they want to routinely insert in their networks will be readily available. Then the DoD will keep pace with the industry, and keep the attention and interest of the innovators who embrace open interoperability, in an ongoing fashion. It helps insulate the DoD ISR network from requiring ongoing forklifts. This is highly important when you're really talking about a affecting weapon system."

SOLUTIONS: INSIDE AND OUTSIDE

Leighton said the DoD relies on a mix of outside consultants and in-house research efforts to develop optimal ISR networking solutions. "No matter how hard the DoD tries, it finds it cannot completely eliminate the outside consultant," he said. "They just have to make sure the ones they pick bring the most bang for the buck."

Leighton noted many ISR networking vendors are frustrated by highly demanding DoD processes and requirements. "Some of these processes are necessary to ensure security standards are met, for example, but the Pentagon is looking to streamline as many of these [processes and requirements] as possible," Leighton said.

Recent initiatives, such as opening the ISR program to startups, is a good move and one that's likely to help DoD secure the most innovative solutions for ISR. "You don't want innovators, even big ones like Google, to quit the DoD market because it's too hard to penetrate or it's too hard to meet outdated standards," he said. ■