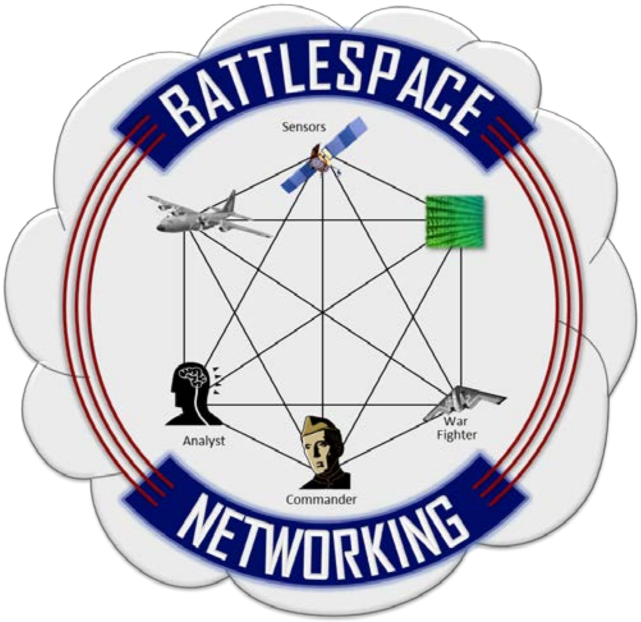
DEPUTY CHIEF OF STAFF, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR)

Battlespace Networking



An

ISR HORIZONS FUTURE VISION

May 2015

OPRs: Dr. Mark H. Linderman, AFRL/RIT (mark.linderman@us.af.mil)
Mr. Jeffrey Eggers, AF/A2D (jeffrey.eggers.1@us.af.mil)

Robert Otto

ROBERT P. OTTO, Lt Gen, USAF
Deputy Chief of Staff, Intelligence,
Surveillance and Reconnaissance

William J Bender

WILLIAM J. BENDER, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

Battles are won by applying the right type of force to the right targets at the right time with a rapidity the enemy cannot match. Such decisive actions are best performed as integrated operations across war - fighting partners and domains. These coordinated efforts depend on timely, accurate, and relevant intelligence which demands rapid, agile, and survivable collection, analysis, and dissemination. This vision of *Battlespace Networking* enables decisive action with a high-speed global network connecting sensors, command and control (C2) nodes, analysts, and war-fighters both tactically and globally. It spans air, land, sea, space, and cyberspace, as well as Services, agencies, and coalitions, to provide flexible and resilient networking in environments from permissive to highly contested.

This vision addresses both the networks and the information that rides upon them. The Air Force requires an operational network that is survivable and secure from our adversaries. It also must be adaptive to fluid operational environments and diverse mission applications. Yet this agility means its bandwidth will be in constant flux—so we will need to be smart and flexible with the types, timings, and priorities of the information we exchange. Regardless of the flux, we will still have much greater access to meaningful information and collaboration amongst distributed teams than we do today. This access will enable tremendous innovation in the tools we use and ways we work together to win the fight.

In the future, platforms and sensors (air, sea, land, space, and cyberspace), with very few exceptions, must participate in and extend the battlespace network. With the extensive use of the software-defined and comparatively high-bandwidth capabilities of Common Data Link (CDL) radios, ISR systems are already leading the way. While CDL and other technologies can provide tremendous capabilities right now, we must also enhance data link, network management, and information protection technologies. Today, our networks radiate detectable frequencies for hundreds of miles. To remain ahead of our adversaries, we need new technologies that move beyond the RF spectrum, offering low probability of intercept and low probability of detection in an Anti-Access/Area-Denial (A2AD) environment, blending seamlessly into the background. Having these current and future capabilities widely deployed across multi-Service platforms can deliver the boundless potential of fused full-spectrum awareness at the war-fighters' fingertips.

Coupled with new platform-hosted intelligence services, battlespace networks will provide the rapid and resilient information exchange critical for war-fighter-centric intelligence, reduce the fog and friction of war, and deliver the decision advantage needed to operate routinely inside the enemy's decision loop.

Linkage to Air Force ISR Strategy

Headquarters AF/A2's *Revolutionizing Analysis* whitepaper envisions a world where analysts are elevated from detached exploiters of data to collaborative creators of fused intelligence. *Sensing as a Service* supports this by outlining a concept of free information exchange based on intelligent sensing, platform-hosted web services, streaming analytics, and digital integration of sensors and analysts with war planners and fighters. *Battlespace Networking* advocates for the high-bandwidth resilient connectivity needed to execute these visions and ultimately to support the *Air Force ISR 2023* objectives of Full Spectrum Awareness and Delivering Decision Advantage.

This vision of Battlespace Networking supports the Air Force's Information Dominance Flight Plan and vision for Information Dominance which fully exploits the man-made domain of cyberspace to execute, enhance, and support all five Air Force core missions. It also supports several other future concepts including: *Enhanced Battlespace Awareness*, the *Air-Sea Battle Concept*, the *Joint Aerial Layer Network,* the CJCS *Joint Integrated Air and Missile Defense Vision 2020*, and the Office of the Secretary of Defense's *Data to Decisions* research portfolio. It also supports the *Targeting Strategy* for distributed operations and the *DCGS Vision* of networked war-fighter-centric ISR. Properly conceived and executed, *Battlespace Networking* is foundational to future ISR operations.

Tenets

The five tenets of *Battlespace Networking* build on three assumptions: 1) the network must support diverse missions and partners, 2) the network will often be challenged, and 3) the need for information will often exceed the capacity.

Of the five tenets, three tenets define the transformative nature of battlespace networking: empowering innovation; agile self-management for dynamic, contested battlespaces; and mission-aware information exchange. The last two tenets contend that all new operational systems, and the security woven through them, should contribute to a battlespace network that serves both their own missions and those of others.

Tenets of *Battlespace Networking*

- **Empowering Innovation**
- **Agile Self-Management for Dynamic, Contested Battlespaces**
- **Mission-Aware Information Exchange**
- **Mission-Enhancing Cybersecurity**
- **Net-Centric Unity of Effort**

Empowering Innovation

Innovation in this context is the ability of people to rapidly adapt deployed systems, processes, and tactics in novel ways in response to changing needs. It is one of our best weapons for combating the dynamic challenges of contested environments. Yet, the way we design technology can greatly affect our ability to innovate in combat.

Battlespace Networking can enable innovation for a wide variety of users of intelligence data (war-fighters, mission planners, analysts, decision makers…). It can facilitate robust data access through web-based services that will allow users to more easily and rapidly build tools and processes to accomplish the diverse efforts that lead to successful missions. Battlespace Networking, emphasizing a network based on internet protocol (IP) tailored for the realities of tactical networks, will:

- establish familiar architectures and flexible standards across the battlespace, and reduce the need for end users to build their own infrastructures
- support streaming analytics and machine-to-machine integration with combat planning and execution systems
- allow us to move from static, predefined, push-style dissemination of data to pull and subscription services that are flexible and user-defined with targeted pushes when appropriate

Though practical today, tactical networking is challenging for IP architectures, which are essential to empower innovation. As researchers develop new solutions, we must ensure that all interfaces remain non-proprietary, support a multi-vendor interlinked network, and remain interoperable with deployed legacy services and tools. The Air Force must work closely with our industry partners to implement these developments in their products to ensure they are affordable and scalable for the future.

Supported by more robust networking, a greater variety and availability of sensor information across multiple domains will support new types of data fusion and analysis products such as object-based production and anticipatory intelligence. Coupled with the inherent collaboration capabilities of a network, these innovations will support new tactics as data users are able to work together in real-time with a richer shared information environment. A genuine revolution in intelligence-driven operations will blossom when we evolve preplanned static data pipes to robust collaboration on a dynamic battlespace network.

Agile Self-Management for Dynamic, Contested Battlespaces

There is intense competition for the electromagnetic spectrum. “Blue” applications include communications, electromagnetic warfare, radar, etc. At the same time, the enemy uses part of the spectrum and actively tries to deny us other parts. Civil uses often continue during conflict too. To meet this vision, we must dynamically manage the spectrum with agile, redundant networks that operate in the environments they encounter, not the ones we had earlier predicted.

In this dynamic environment, communications systems and the end-users that access them must, as much as possible, be flexible in timing and bandwidth—employing on-board processing and memory, delay-tolerant networking, and opportunistic transmission of information tailored to available bandwidth and priorities. Network participants will frequently join and depart, so networks must be agile and self-healing. For example, if an asset is jammed or leaves the network, reconfiguring the network paths should not require human intervention. To engender trust, the networks must assure data integrity and inform war-fighters which authenticated users they can, and can't, communicate with at any time.

We have numerous kinds of data links today, such as the narrowband theater-scope Link 16, the global Common Interactive Broadcast, and the wideband CDL for ISR and there will continue to be a variety in the future. Therefore, we need gateways that will intelligently port web services to and from the non-IP data links to bridge them into a heterogeneous yet unified network. This "inter-networking" could also improve mission assurance and security. Connecting through commercial, coalition or potentially even adversary networks may increase the likelihood of delivery and decrease that of intercept. To meet this inter-networking requirement and to support the sensor-based web services and cross-domain discovery described in *Sensing as a Service,* the battlespace network must support internet routing protocols.

Mission-Aware Information Exchange

Modern operations rely upon rapid exchange of information around the battlespace. However, despite gains, demand for network resources can often outstrip capacity, which fluctuates unpredictably for many reasons. Furthermore, the priorities of messages can change from mission to mission and even from minute to minute. It is critical to manage the information flow to make sure the highest priority messages make it through in the shortest possible time.

It is just as critical that prioritization schemes flex and adapt with the dynamic missions and do not just rely on static templates. A static template, for example, may place all Command and Control (C2) data transmissions at a common priority, while a dynamic one could temporarily raise the priority of those messages supporting a critical strike mission. This is called "mission-aware information exchange."

Consider a Cursor-on-Target message traversing encrypted links from an Army counter-battery radar. A number of people need that information including the Air Force Tactical Air Control Party, the nearest MQ-9 Reaper crew, and the intelligence professionals who compile the order of battle—all on different data pipes with different urgency. A mission-aware router in one of the gateways inspects the message and queues it for distribution on the different networks at different priority levels.

For these mission-aware routers to dynamically prioritize messages, they must be able to inspect them—at least to a level that can identify their mission priority. Certain encryption schemes used today encode the whole data stream and hide the information needed to prioritize the messages. We need encryption schemes that allow the routers to decrypt the metadata separately from the message.

Ideally, this will evolve into self-managing "information objects" that replace our current messages. Rather than relying on external policies, these information objects will carry the metadata that controls how they will be prioritized, who can access them, and what parts of the information can pass through automated multi-level security gateways to reach other systems and networks, including legacy and coalition networks. Such a capability would operate like a self-enforced digital tear line with little or no infrastructure support needed.

Mission-Enhancing Cybersecurity

In such a complex and dynamic inter-network, there is often a tension between flexibility and security. There is a spectrum of security ranging from full lockdown to fully open where both extremes lead to mission failure. The operating point within this spectrum must balance mission needs and acceptable risk. Currently, this balance point is often static and hard-coded. Near-term efforts should focus on providing more flexible control of the balance point. Yet the fundamental nature of security in operations can and should change to a mission-enhancing paradigm. This mission-enhancing paradigm must focus on the network as a means to transport protected information vs. the current philosophy of a protected network. Our shift to protecting information before transport allows higher security postures with flexibility to seamlessly utilize a variety of networks.

Research is underway now that aims to provide dynamic intelligent security that protects the mission with data confidentiality, integrity, and availability while minimizing negative impacts to operations. As networks evolve from single-mission to multi-mission, current practices of hard-coding network addresses and physical loading of cryptography keys must evolve to techniques that scale and provide more precise access control. Cross-domain guards must match user authorities against data classifications rather than sensor sources. Making network security smarter will reduce the need for humans to manage it, accelerate security responsiveness to changing conditions, and ensure better access to information by those who really need it.

Net-Centric Unity of Effort

A network is only as good as the people it connects and the information it shares—and the larger and more interconnected the network, the more useful and resilient it is. Therefore, as many platforms as possible must become good net-citizens. The Air Force and mission partners must consider the overall enterprise and push networking requirements down to systems. As network nodes; aircraft, satellites, and terminals must forward data that supports other missions—just as we do now with Link 16. Sharing communications and processing power is a responsibility of net-citizenship and a benefit each should expect from others.

Recent U-2 upgrades are a shining example. Outfitted with very high bandwidth radios, the U-2 can now relay video and other sensor data from tactical assets to command posts, ships, and remote analysis centers. At the same time it can provide two way voice-over-IP and data services between forward and rear echelons or between multiple forward combatants. Other aircraft with lesser bandwidth can contribute too, and new upgrades should be fielded with spare capacity. This should not be seen as mission creep, but as a basic responsibility of a member of the battlespace network.

Modern technology empowers such cooperation. On-board processing and memory are rapidly increasing. Bandwidth is increasing through efficient use of existing spectrum and expansion into higher frequencies. Capabilities that required special hardware just a few years ago can now be done with software, which can be upgraded much more rapidly and at lower costs than hardware. Modular design helps too. The internal software of fighter and bomber aircraft typically takes over three years to update. Yet powerful new combat collaboration capabilities have been recently introduced without upgrading the aircraft software by including data link and processing on targeting pods and coupling them with high-bandwidth, man-portable radios on the ground. Similar efforts are underway to make some internal aircraft mission systems modular from the flight safety systems. These and other new capabilities must be designed with integration and interoperability at the forefront and broadly tested across services and legacy systems to ensure they enhance resiliency, agility and empowerment.

In addition to proliferating interoperable links and gateways, net participants must also commit to using the emerging net-management technologies described earlier. Whenever possible, primary information providers such as battlespace awareness and sensor platforms should commit to providing data in discoverable web services. It will be impractical to upgrade all data links, so gateways must have the intelligence to not only transcribe data but also to assign mission priority and cross-domain releasability.

In a contested environment, such mutual support is even more critical. Regional jamming and threats to satellite and other long-haul communications may force us to use alternate data paths. At the same time, survival itself may depend upon how quickly we can exchange threat data between platforms and across domains. Sensor platforms, fighters, bombers, tankers, satellites—everyone must become a good net-citizen, bearing the responsibilities and sharing the benefits which that entails.

Summary

The analyst is a war-fighter whose ammunition is intelligence and networks are the weapon they use to get it on target. Battlespace Networking provides the essential communication links underpinning the *Sensing as a Service* vision. *Sensing as a Service* provides the rapid collection management, streaming analytics, and information access needed to address the *Revolutionizing Analysis* goal of elevating analysts up from stovepipe data processers to mission-focused fusion analysts. These concepts, empowered by *Battlespace Networking* bring the considerable talents of the intelligence analyst to the fight.

Advanced battlespace networking needs an expanded physical network, adaptive IP-based net-management, and new information architectures. The physical network must have enough interconnected nodes and gateways to be robust and resilient. It must be responsive and adaptive to the threat and environment while increasing the bandwidth available to users. Such adaptability requires new net-management capabilities which in turn require new encryption schemes that allow mission-aware data flows and provide more automated access across domain boundaries. Mission-enhancing security is critical to ensure trust in such a diverse network that crosses classified, unclassified, and coalition domains. A great deal can be done with existing technology which can be deployed now and upgraded by software as the more advanced net-management technologies are developed.

An improved data architecture can support broader usage and empower innovation at all levels by making a wider variety of data available at better data rates, connecting more diverse types of users, and providing a common and well understood platform for tool development. To do this, the architecture must be IP-based, service-oriented, loosely-coupled, highly-interoperable, and open. We must also deploy a sensor-agnostic, object-oriented information exchange standard with security tags enabling cross-domain discovery. Moreover, we must unify our efforts to make all systems good net citizens. The network upgrades to the U-2 and the targeting pods are shining examples. Systems can and must contribute part of their bandwidth and processing power to the greater operational objectives.

Battlespace Networking is a critical underpinning to the ISR 2023 objectives of full spectrum awareness and delivering decision advantage. We simply cannot achieve these objectives without a flexible and resilient battlespace network spanning air, land, sea, and space. The Air Force ISR leadership is working together with the Air Force CIO A6 and partners across the AF, DoD and industry to implement these robust networks in support of the war-fighter. Firm leadership is needed, but we have the technology, infrastructure, and vision to make it a reality.