Document created: 10 October 01

Building a BattleSpace Wide Web

Lt Col Robert A. Colella

Introduction

While executing B-2 missions during Operation Allied Force there were several "fleeting" opportunities to attack mobile Surface to Air Missile sites that were playing, and occasionally winning, a frustrating cat and mouse game with allied aircraft. B-2 missions were planned with options to strike these mobile targets based on their last known locations. During the 14-hour flight from Whiteman to Kosovo, the battlespace picture changed constantly. If the mobile target revealed itself while the B-2 was enroute, and the Air Operation Center was able to confirm the location, the B-2 was then tasked in-flight to "execute" the pre-planned "flexible" option.

The opportunity to fix the target's location, process the information and decide to act diminished as the B-2 closed on the target's "last known location." If the target's location was not resolved in time, the opportunity was lost. The B-2 performed this type of "flex-targeting" on several missions and was successful in destroying several SA-3 sites and mobile long-range early warning radars by using updated positions passed in-flight.[1] The serial process used in this example to disseminate information must mature in the future so that users can "pull" information rather than having to wait for it to be pushed. As Operation Allied Force progressed and mission planning experience at Whiteman AFB grew, B-2 bomber crewsgained "real time" appreciation for the paths information takes as it moves from sensor to shooter.

Quickly it became apparent that all warfighting systems must be able to plug into a common battlespace picture, or Battlespace Wide Web (BWW). Every combat system must be able to push and pull from this web the information it gathers or needs. As the information battle moves to center stage in the 21st Century, the challenge for a fighting force rests in linking information during combat operations from all combat platforms, synthesizing it, and providing it to a BWW for all the users.

The Problem

There are three major obstacles to building better battlespace awareness through a BWW. The first is a lack of standardization between sea, air, land and space platforms to enable them to talk to each other. The second obstacle is finding a way to optimize the use of the sensors on all platforms in the battlespace. The final obstacle is the system of institutional stovepipes between strategic collection channels and end users of information at operational and tactical levels. All three of these problems have solutions in the commercial sector. To ease the transition to a BWW for combat platforms, the Department of Defense (DOD) must take advantage of technological innovations to optimize combat platforms across a common battlespace interface in the same way that the Internet connects PC platforms today.[2]

Standardization

Compatibility between individual platforms is the first barrier to better battlespace awareness. During combat operations, specialized sensors on individual platforms collect imagery and signal data to perform individual missions. The potential to share all the information collected across all platforms is unrealized as links to pass information between individual platforms or "nodes" are inadequate, incompatible, or do not exist. General John P. Jumper, then the commander of US Air Forces in Europe during Operation Allied Force and now the Commander of Air Combat Command, summed up the need for better integration in order to strike time-critical targets when he testified to Congress after Operation Allied Force:

> "We must fully develop the technology and tactics to rapidly strike targets. To do this, we need equipment that will provide real-time imagery and target location directly to our fighter and bomber crews. This will allow us to reduce the barriers between the "sensor" and the "shooter" in the targeting cycle—what we call "attacking the seams." To make airpower as effective as possible against mobile targets, we must have complete integration between all available air and space sensors at our nation's disposal."[3]

Closing the gaps between sensors and shooters requires compatibility among all the platforms that are capable of gathering and sharing information horizontally across platforms and not just vertically through individual stovepiped systems. At the ground level, part of the answer lies in standardization initiatives like DOD-directed Defense Information Infrastructure (DII) Common Operating Environment (COE) standards. In 1993, DOD realized that many functions of command and control systems were so fundamental that almost every command, control computer, communication and information (C4I) system shared them.[4] In the past, individual contractors developed these common functions "from scratch" for every system DOD acquired. The differences in the software for these common functions across the different platforms led to incompatibility between the systems. The DII COE initiative had two goals. First, it was supposed to provide a common set of tools for software designers to save the government time and money in development, and second, and more importantly, it was to ensure compatibility between all future C4I systems. The goal of DII COE is to "field systems with increasing interoperability, reusability, portability, and operational capability, while reducing development time, technical obsolescence, training requirements, and life-cycle cost."[5] DII COE will ensure individual system compatibility as it is implemented across DOD. Once that is accomplished, the ability to optimize all the individual sensors will evolve, and sharing will lead to synergy among platforms.

Optimization: Reaping What is Sown

In combat, there is "untapped potential" within every individual combat and C4I system. Increasing the level of utilization on individual platforms and the level of integration between platforms could provide a unique synergy. An F-117's infrared targeting system's sole purpose is to support the F-117 mission to drop two laser-guided bombs on two targets. When the F-117 is flying to the target, that sensor is idle, or in current jargon "underutilized." Additionally, individual aircraft with threat warning systems serve only to warn those aircraft. Tapping underutilized and independent sensors has wide application across the battlespace for targeting, bomb damage assessment, and intelligence collection.

Utilization

The actual amount of time that onboard sensors and processors are utilized on strike platforms amounts to only a fraction of what a sensor, if properly managed, could provide a common battlespace picture. In the transit to and from a target in hostile territory, a platform may overfly many other targets. If an onboard sensor is idle during this time, it could be used to provide imagery to other platforms. Missions could be planned to perform these functions, or an ad hoc system of real-time requests could also be used. Targeting sensors are usually of high fidelity and quality and could provide targeting data for other platforms. In addition, they could be used to provide bomb damage imagery from other attacks. The ability to manage requests of this type, assign tasks to assets and the architecture to push and pull this type of data exists today. For example, Napster is an on-line Internet program where stored information is transferred between users who use software to initiate requests and receive replies to locate data (in this case, music files) for the users.

Another example of a system that taps unused potential is the Search for Extraterrestrial Intelligence (SETI) program.[6] This program uses personal and other computers that are voluntarily hooked up on-line to The University of California at Berkley to analyze the massive amounts of radio wave data collected in its search of the cosmos for extraterrestrial intelligence. The program runs as a screen saver on idle computers that are connected to the Internet. When a participating computer's central processing unit (CPU) is idle, the SETI program uses the CPU to process the collected radio wave data. In a sample 24-hour period, SETI used 2665 idle CPUs to accomplish 22.85 trillion computations/second. On average, each connected CPU was idle and used by SETI for close to 20 hours of the 24-hour period.[7] Assuming that these computers were left on by design 24 hours a day, SETI takes advantage of processor time that is already paid for and sitting idle 83 percent of the time. Also of note is that over 100 different operating systems run this program through the Internet.[8] The software is able to interconnect the different hardware configurations to take advantage of CPU time that otherwise would go unused. In combat the underutilized potential of onboard sensors could be similarly exploited.

Integration

Beyond using idle sensors, individual aircraft with passive threat warning systems can be linked to provide a broader picture across the battlespace. Each "aircraft centered" picture can be linked to build a "common battlespace" picture for every aircraft. This would allow aircraft to "see" threats over the horizon from their own position based on offboard data from other aircraft. Ideas like this are limited only by the ability to push and pull data from platforms. Unfortunately, the current ability to do this is minimal with very few aircraft equipped with LINK 16 or other data link devices. Future acquisitions must demand that every platform be able to "plug and play" into a common battlespace picture.

Stovepipes: Physical/Philosophical

Part of the latency in the present sensor to shooter path lies in the stovepiped "plumbing" of strategic collection systems. From an architectural standpoint, too many of the "sensor to shooter" information paths travel along an enclosed path from start to finish. Access to data is

not possible until it is analyzed and processed as a finished product. The ability exists within many strategic systems to move data on large data highways from "platform to headquarters to headquarters to platform," but the information infrastructure to move data efficiently between individual nodes at the operational and tactical level does not exist.

Beyond architecture there are philosophical obstacles that create parochial stovepipes as well. Within intelligence organizations that "own" a sensor there is a tendency to control all aspects of collected data from cradle to grave. This introduces fog and friction and latency as information travels from sensor to shooter. Both the C2 and intelligence communities need to evolve from the strategic level to the operational level to achieve the synergy available at the pointy end of the spear in information dominance. The problem exists in C2 nodes that do not want to relinquish responsibility for a C2 decision over or near the battlespace. It extends to intelligence analysts, used to working at a "strategic pace" that do not want to release information for "operational" or "tactical" applications for fear of being in error. The result is that data is often analyzed beyond its shelf life in a time critical environment. This institutional as well as doctrinal issue requires overcoming more than just bandwidth. Concern over the potential for aircrews or other users to misuse data or information leads to information latency and degraded situational awareness for all participants. As time withers the value of any piece of information, the end result is a reduced probability of kill, increased sorties to achieve campaign objectives, and what should be an unacceptable increase in the exposure of aircrews in a hostile combat environment.[9]

Solution: World Wide Web Infrastructure

Interoperability, reclaiming wasted potential, and eliminating stovepipes will set the stage to provide a common user interface for every warfighter. In the 1990s the "ARPAnet" population of hosts and connected nodes exploded beyond universities and military users and became today's Internet.[10] Transparent to Internet users is the "network of networks" linked together through the common user interface that made this explosion possible. That interface, TCP/IP or Transmission Control Protocol/Internet Protocol, was developed for the military to allow users to connect systems in a redundant and robust fashion across DOD regardless of manufacturer. Today's Internet is even more capable, as software applications allow users to "virtually" tailor and filter information to the few pieces they want to build their personalized picture.

The systems in the Air Force "Web", be they strike aircraft, ISR platforms, U-2, Rivet Joint, JSTARS, AWACS, Air Operations Centers or other C4I nodes, currently do not work together in this manner to provide each user a tailored and accurate "Battlespace Wide Web" picture. There is not a TCP/IP protocol to connect all these systems together. Age and the physical limits of many hardware systems make it difficult to re-engineer many older systems; however, future acquisitions must establish a common interface at the appropriate level of architecture for each user to plug into the battlespace web of the future.[11]

The Air Operations Center (AOC)

The Air Operations Center (AOC) is currently the best way to link and manage data and communications. Acting as a hub in the spoke of a wheel, an AOC can push and pull data to and from its connected systems. During Operation Allied Force, General Jumper commented that the

AOC represented the best our current technology had to offer in terms of real time management of battlespace information:

> "…the CAOC 'is a weapon in its own right'. In Operation Allied Force 'The CAOC connected pilots and controllers airborne over the battlespace to the nerve center of the operation.' Handling the strike execution, the CAOC 'served as the pulse point of aerospace integration: linking up many platforms in a short span of time. Multiple intelligence sources down-linked into the CAOC for analysis. Operators integrated target information and relayed it to strike aircraft. Pilots could radio back to the CAOC to report new targets and get approval to strike.' "[12]

Though powerful, the CAOC's greatest strength is also its greatest weakness; as it is the central hub through which all data passes. All information in this schema flows from system to CAOC to system. To dominate the future battlespace, information must travel in a redundant and transparent fashion from system to system and not through a central "nerve center" or other single point of failure. TCP/IP provides automatic recovery from the loss of a node and was a key design feature for the military to ensure a robust system with ARPAnet. The problem with a CAOC is that, while it is easy to identify and provide security for this important hub in the architecture, by its very nature it is also the most lucrative target for an enemy. So, would a BWW be any less vulnerable than a CAOC? Yes.

Security

Obviously a system that is so interconnected might present opportunity for adversary attack, and if the "Battlespace Wide Web" becomes an Achilles' heel for US airpower it will not have served its purpose for the warfighter. The redundancy throughout the system, however, will ensure it is robust. And the primary security concern for the warfighter will be potentialoutside attacks that could corrupt or gain unauthorized access. Yet, these concerns all have solutions in technology that provide for encryption and security on the Internet today. Similar technologies can be applied to ensure both the security and the integrity of the data within the BWW of the future.[13]

Conclusion

The US possesses a great ability to gather information in combat. There are very good collection assets, and there is good plumbing to move data to intended points of destination. What does not exist, and what is desperately needed, is the ability to synthesize all the available battlespace information at every system participating in the combat scenario in order to push and pull data on demand to all the combat systems "connected" to the battlespace. Integrating in this fashion will improve the survivability and efficiency of combat strike aircraft, allow for improved real time targeting for the JFACC, and provide better situational awareness at the tip of the spear. The desired objective and method to employ airpower becomes clear as a complete picture is drawn for each player. As General Jumper said in comments to the Air Force Association Eaker Institute in October 1999:

> "Indeed, the day may be dawning when the Air Force is able to seamlessly combine information from U-2s, UAVs, and other ground- and space-based sensors. "We will be where we need to be in the ISR world when we have transparent linkages ... among our platforms," said Jumper. "When the

> amalgamation of these and the product of these sensors are presented in a way that ... is in targetable, quality data, that is when ISR will have come of age."[14]

As time and space compress, we must take advantage of our own technological abilities to gather information and use it to our tactical and operational advantage to execute combat operations. The USAF should speed this process along by demanding a common interface standard and compatibility between all systems for all future acquisitions. If a system does not "plug and play" by design, then it should not be funded. A common push-pull interface between combat platforms is the first step to glean this wealth of information currently left field. The advantage in the next 25 years of aerospace research and development will go to those who figure out how to put all the existing pieces of the puzzle together. Once that happens the synergy that results will close the gaps in the seams between sensors and shooters in the battlespace of the future.

Notes

1. "Jumper on Airpower," *Air Force Magazine* 83, no. 7 (July 2000): 43.

2. Martin Libicki, "The Mesh and the Net," McNair Paper, 29 March 1994.

3. House, *Congressional Subcommittee on Military Readiness,* 26 October 1999.

4. Carnegie Mellon University URL, on-line, Internet, 4 April 2001, available from: http://www.sei.cmu.edu/str/descriptions/diicoe_body.html Last Modified: 22 September 2000.

5. Ibid.

6. SETI, or the Search for Extraterrestrial Intelligence, is a scientific effort aiming to determine if there is intelligent life out in the universe. There are many methods that SETI scientific teams use to search for extraterrestrial intelligence. Many of these search billions of radio frequencies that flood the universe, looking for another civilization that might be transmitting a radio signal. Other SETI teams search by looking for signals in pulses of light emanating from the stars.

7. SETI website statistics presented below, accessed 3 April 2001. On-line, Internet, available from: http://setiathome.ssl.berkeley.edu.

	Total	**Last 24 Hours**
Users	2906558	2665
Results received	308241507	506210
Total CPU time	615412.832 years	1150.253 years
Floating Point Operations	7.863267e+20	1.974219e+18 (22.85 TeraFLOPs/sec)
Average CPU time per work unit	17 hr 29 min 22.5 sec	19 hr 54 min 18.7 sec

8. UC Berkeley SETI Program, on-line, Internet, 3 April 2001, available from: http://setiathome.ssl.berkeley.edu/.

9. Ben R. Rich and Leo Janos, (Boston, Mass,: Little, Brown and Company, 1994), 123.

10. Carl G. O'Berry, "Information Systems and Applications," in *Technology and the Air Force*,ed. Jacob Neufeld et al. (Washington D.C.: Air Force History and Museums Program, 1997), 316-7.

11. "*Introduction to TCP/IP*," on line, Internet, 2 April, 2001, available from: http://www.yale.edu/pclt/COMM/TCPIP.HTM.

12. Rebecca Grant, "The Kosovo Campaign: Aerospace Power Made it Work", Air Force Association Special Report, (September 1999): 18-19.

13. House, *Congressional Subcommittee on Military Readiness,* 26 October 1999.

14. "Eaker Institute Panel," *Air Force Magazine* 82, no. 10, (October 1999): 32.

Disclaimer
