INFORMATION AGE AIRPOWER

By Marc V. Schanz

At a recent AFA/Mitchell Symposium, Air Force leaders explored how airpower will evolve.

Any future conflict between the US and a near-peer adversary will increasingly turn on the ability to collect, disseminate, and exploit information faster than the opponent, senior USAF leaders and others declared at a recent forum in California cosponsored by the Air Force Association's Mitchell Institute for Aerospace Studies.

Air Combat Command boss Gen. Herbert J. "Hawk" Carlisle said in a speech that during Operation Allied Force over Serbia in 1999, Serbian air defense artillery shot down an F-117 stealth fighter aircraft with a 1960s-model SA-3 missile. Using innovative tactics, basic communications, and even human spotters watching strikes take off from Aviano AB, Italy, the Serbs were able to take down one of USAF's top-of-the-line assets at the time, in the opening days of the campaign.

The loss is a teachable moment as to how information drives advantage, Carlisle said. "Whether it's old school or new school," success will hinge on how airmen can leverage what they know about their enemy, Carlisle said in his remarks to the Dec. 4 Mitchell-RAND Corp. forum on aerospace power. Hosted at RAND's headquarters in Santa Monica, Calif., Air Force leaders, airmen, business executives, aerospace industry officials, and others came together to discuss how the US will adapt its aerospace power and its air, space, and cyber forces and reform its acquisition processes to better prosecute the challenges of the "information age."

Gen. Hawk Carlisle speaks at an Air Force Association-Mitchell Institute for Aerospace Studies event in Los Angeles.

Staff photo by Abby Gillett

WHAT I NEED, WHEN I NEED IT

The Air Force faces a future where its dominance will be challenged in all the domains it operates in—air, space, and cyberspace. Power projection will hinge on finding the right information grid in a given crisis or scenario and working to get inside adversary decision-making cycles. Situational awareness, Carlisle said, is the ability to "know what I need, when I need it, and nothing more."

This need is why initiatives such as enabling the powerful sensor and computing capabilities on the F-22 and the F-35 fleets are so critical to success in the years to come, he added. As demonstrated in Operation Inherent Resolve missions, information and target sharing among F-22s, the combined air operations center, and the rest of the combat fleet is crucial to the completion of a robust and responsive find, fix, target, track, engage, and assess (F2T2EA) chain.

USAF has built two fifth generation aircraft capable of taking in enormous amounts of information, but at present the F-22 and F-35 cannot disseminate that data beyond those fleets via data link, Carlisle said. That connectivity is how USAF is going to complete an effective kill chain and enable survival and success of combat forces in future wars.

It is also why USAF is transforming its high-end training to better leverage these new tools.

For decades at Nellis AFB, Nev., aircraft would show up, with good guys on one side and bad guys on the other, they would fly, and then lessons would be sorted out in debrief, said Maj. Gen.

Jay B. Silveria, commander of the USAF Warfare Center, during a panel on modern air operations. But one Red Flag last year saw some 3,000 participants, with about a third of the participants not flying at all, he stated. These airmen operated ISR elements of the air operations center, helping run a "virtual war" while live flying occurred simultaneously. Distributed Common Ground System airmen helped utilize U-2 imagery for the exercise, and cyber operators were protecting against aggressors attempting to infiltrate network systems. This integrated training is helping airmen across the force see how different capabilities plug in and leverage each other, he said.

But this will involve more than just linking modern fighters to the rest of the fleet. Carlisle said it also means building a responsive and flexible "combat cloud" network, linking up forces from a joint terminal attack controller on the battlefield to the analysts working in a Distributed Common Ground System somewhere around the world.

Today, after more than a decade improving close air support practices in Afghanistan and Iraq, strike coordinates are now sent digitally to pilots, but the process is still human driven and deliberate.

Machine learning—which drives technology such as commercial smartphone apps guiding cars to more efficient routes in the civilian world—could be harnessed for use in combat, he said. As a result, the once-deliberate 72-hour air tasking order is evolving toward being a "constant product," one taking prioritized information and threat analysis and signals intelligence and disseminating it to the combat air forces in a given operation, Carlisle said. Instead of pilots working various systems to operate their aircraft, as the pilots of fourth generation fighters were taught, they can now perform mission management with the powerful tools and sensors at their disposal.

"We can make them the decision-makers, based on what we are giving them," Carlisle said. This will keep combat power survivable, as network nodes can be dispersed beyond centralized locations such as a combined air operations center.

The future force will increasingly be defined by the evolution of what Carlisle dubbed "in-garrison combat operations," or missions performed by airmen supporting tasks ranging from remotely piloted aircraft operations to satellite movements to cyber defense and offensive operations. "We need to talk about it—and how we do that moving forward," Carlisle said.

Information exploitation will improve use of limited and in-demand assets like RPAs, he said. Rather than chopping a single aircraft to a combatant command to fill a requirement at a given time, USAF and DOD should employ predictive intelligence capabilities better to "cross cue" assets to surge to meet demands when they emerge.

As ATOs evolve and get more responsive, the ability to predict needs and "share" capabilities will increase, with the help of USAF's distributed ISR network and global command and control infrastructure.

UNDER THREAT

USAF's dominance on the battlefield is increasingly tied to its vast space and cyber capabilities, but that dominance is under threat as never before, Air Force Space Command boss Gen. John E. Hyten said in his address to the forum. "We used to fight based on mass. Now we have information as the discriminator on the battlefield," he said. "We have come down huge numbers in size, but we can leverage information." USAF must better prepare to defend those domains and fight in them. This is why AFSPC is moving forward with an overhaul of its shift system for space operations, to stand up a "space mission force."

The experience and proficiency of airmen operating space assets must be enhanced uniformly, Hyten noted. To do this, USAF must rebalance the experience levels of airmen tasked with operations. Currently, AFSPC's satellite operations crews perform at a high level, but they are usually very young and lack significant experience in their respective system. This is because the old AFSPC system was a split system, featuring a "crew force" of airmen who perform operations for a certain period of time, then progress to "day staff," who are not generally operating assets but working staff and headquarters functions. The result of this system, he noted, is that AFSPC's most experienced and capable operators are not working on crew shifts running valuable space capabilities, a potential danger if something bad were to happen on orbit.

This is why AFSPC is moving to "blow up the day staff," Hyten said, and stand up the space mission force.

AFSPC will now have two sets of crews operating its on-orbit capabilities, rather than a separate "day staff" from the airmen who perform operations. These two crew sets will carry out operations four months at a time, and as one shift maintains USAF's space capabilities, the other will undergo rigorous high-end training and skills development, such as participating in Red Flag and other high-intensity training events. This new training and operations regimen will help sharpen new capabilities needed to defeat the hardest threats that could emerge in orbit.

But the cyber domain is also rife with potential threats and vulnerabilities, and the Air Force needs to better prepare for those avenues of attack as well. A culture shift needs to take place to move cyber airmen into more of an operational footing, rather than support a mindset that prioritizes tasks such as network support, Hyten observed.

"The cyber squad of the future will work with the ops group," he said, not the mission support group, and the cyber airmen will fight with computers—their weapons system—just like airmen fight in other mission areas.

This need is driven by the increased vulnerabilities through the cyber domain that could affect US operations in the future. "If someone hacks into my email, I'll be annoyed," Hyten said, but he's more worried about the vulnerability of systems such as the GPS network or the computerized logistics system that support the F-35 fleet.

Though policy guidelines are slowly catching up to capabilities in cyberspace, and cooperation among other arms of government, the Intelligence Community, and international partners is at an all-time high, there is work left to do, he said.

"Fly, fight, and win in air, space, and cyber," Hyten noted. "It's that simple."✪

Marc V. Schanz is the director of publications for the Mitchell Institute for Aerospace Studies.