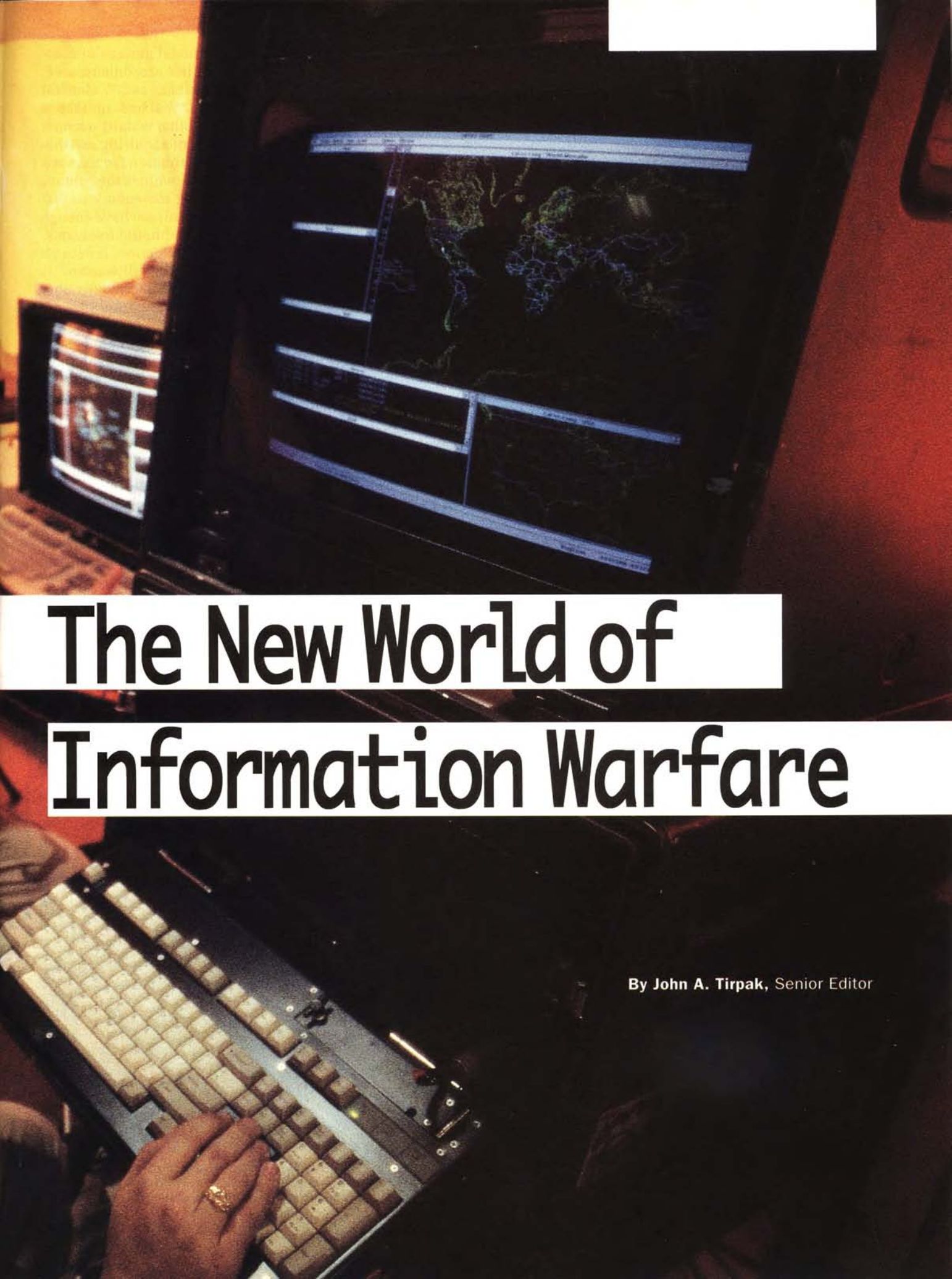
Staff photo by Guy Aceto

The Air Force has decided it must be "mainstreamed"—involving all aspects of the mission—rather than letting it be captured by experts and specialized organizations.



The New World of Information Warfare

By John A. Tirpak, Senior Editor

Staff photo by Guy Aceto

Above and previous pages: Technicians from the 609th Intelligence Squadron, Shaw AFB, S. C., participate in the annual Green Flag exercise, which integrates some elements of information warfare into its scenarios.

IN THE opening round of the Persian Gulf War in 1991, Air Force pilots in F-117s squeezed triggers and released 2,000-pound iron bombs on Iraqi telephone exchanges, power stations, command-and-control nodes, and other vital information and communication links.

In the future—possibly soon—such an attack might be conducted far from the target, with a computer terminal replacing the airplane, "logic bombs" replacing the ordnance, and the "enter" key replacing the trigger.

These real-world and hypothetical strikes both are examples of information warfare (IW), which is rapidly assuming a central place in modern military thinking and planning. It involves much that is new as well as much that is familiar.

With tight limits on the assets available for any given mission, the armed services are depending as never before on information systems to make sure forces are employed when and where they will have the most telling effect. With this dependence, however, comes a vulnerability that an opponent could exploit. IW works both ways.

To the Air Force, IW is "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions," said Maj. Gen. Robert E. Linhard, director of Plans in the office of the Air Force deputy chief of staff for Plans and Operations, quoting from "Cornerstones of Information Warfare," published by USAF last fall.

Two years ago, Gen. Merrill A. McPeak, then the Air Force Chief of Staff, charged General Linhard and others with formulating a doctrine for IW. When they presented their findings, General McPeak told General Linhard, "You don't have it right, yet."

"Though we absolutely correctly reflected the thinking of the time, our concept was too evolutionary from the traditional notions of command and control, reconnaissance, electronic combat, etc.," General Linhard said. "We had to take a broader view" that would account for the synergy of acquiring and disseminating information from a variety of sources as well as the ruinous effect of forcing the enemy to distrust his own data or not have enough of it to make good battle decisions.

With further reflection, it became apparent that, just as "air warfare" is not a mission unto itself but rather an element of everything the Air Force does, so, too, is "information warfare" fundamental to all aspects of the mission. And, just as there is no "air warfare" or "space warfare" department in the Air Force—because every function contributes to it—there will be no "information warfare" command, General Linhard said. "We decided . . . whatever this buzzword means, it must be mainstreamed rather than captured by some expert group."

As a whole, IW—or more specifically information dominance—has now been designated the fifth pillar of the Air Force's core competencies, along with control of the air, control of space, global mobility, and the ability to project power precisely.

"We consciously chose not to have an information warfare 'czar,' " General Linhard said, because doing so would contradict the notion that IW must be integral to all mission areas. "We believe we're thinking about it

USAF photo by SSgt. Louis Briscese

Information warfare works both ways. Not only will USAF try to disrupt the enemy's flow of information, it also will seek to ensure that such data as Global Positioning System transmissions (above) arrive uninterrupted to its own troops.

correctly, now," the General added. "We're all 'information warriors.' "

Rather than let IW become too esoteric, the General said, the Air Force will develop doctrine for it as it applies to theater operations, "to look for a 'counterinformation' mission . . . rather than an IW doctrine." Such an approach "works for us pretty well." There are "other people working on strategic information warfare," he added.

General Linhard also hastened to note that USAF is not attempting to co-opt the IW mission, pointing out that both the Navy and Army are pursuing IW in their own ways. The combination of all the approaches strengthens the resilience of US systems and "enhances joint operations," he said.

There will be no line item in USAF's budget for "information warfare," but assets that tighten the link between sensor and shooter, such as the E-8 Joint STARS, receive ample funding and are inextricably intertwined with IW.

Two Categories

"Cornerstones" broke IW down into intellectually and operationally manageable chunks while stressing the synergy among them. There are two broad categories—"attack and defend information" and "exploit information."

- Attacking and defending information consists of psychological operations, military deception, security measures, physical destruction, information attack, and electronic warfare. These aspects could include destroying command-and-control links with ordnance, undermining enemy troop confidence in their leadership through TV broadcasts, sending computer "viruses" into an enemy logic system to cause it to fail at a critical moment, and jamming enemy radars.
- "Exploiting information" simply means gathering all that is knowable and turning it into military decisions faster than the adversary can, or "acting within your opponent's decision loop," General Linhard explained. "Information operations" fall into this category and include such missions as command and control, combat identification, intelligence, generation of weather data, and surveillance, he noted.

"There isn't a line item for 'information warfare' in our budget," General Linhard pointed out, "and there hasn't been a big uptick in what we're spending on it, because so much of it is the same thing we've been doing all along," such as collecting intelligence and waging psychological warfare. The main boosts in funding have gone to systems that tighten the link between the sensor and shooter, such as the E-8 Joint Surveillance and Target Attack Radar System aircraft, he said.

The Air Force is, however, keenly aware that the systems and capabilities of the information age are evolving at blinding speed, with computer power doubling every eighteen months or less, and ever-more-powerful hardware becoming available to potential "bad actors" for a low entry cost.

At a recent IW symposium in Washington, D. C., sponsored by the Armed Forces Communications and Electronics Association, Vice Adm. John M. McConnell, USN (Ret.), former head of the National Security Agency, said that he has conducted experiments to see how vulnerable some of the nation's supposedly "secure" computer systems are, and he has found that some could be cracked "with $10,000 worth of equipment, a half-dozen college students, some pizzas, and beer."

Among the potential targets of terrorist groups or enemy states might be the nation's power grid, the public telephone switching system, the stock markets, the Federal Reserve, the Internal Revenue Service, "strategic" companies, the research-and-development structure, or the air traffic control system.

Of these information- and computer-dependent networks, the air traffic control system is least vulnerable, Admiral McConnell said, "because that system is so old and arcane."

Asked if the national banking system could truly be "crashed," Admiral McConnell said that, with enough hardware and expertise, "I think it's doable."

Given the vulnerability of such "strategic" targets, it is likely that less prominent databases and e-mail systems, such as logistics-trafficking systems or personnel files, could also be compromised. Because the likelihood of such attacks is rising, the Air Force has moved to keep ahead of the threat.

Anticipating the Possibilities

The Air Force Information Warfare Center has been set up at Kelly AFB, Tex., charged with anticipating IW offensive and defensive possibilities, creating such IW exercises as Blue Flag, and integrating IW into other exercises. It is also developing the concept of the "air ops center," which would collate the wealth of information coming into a theater command post from a multitude of sensors and networks and translate it into a coherent picture of the battlespace for the commander in chief, General Linhard said.

Last fall, the 609th Information Warfare Squadron was established at Shaw AFB, S. C. It was chartered

Photo by Randy Jolly

Because modern fighters rely so heavily on computers, they may be vulnerable to attempts to cripple their electronics with electromagnetic pulses or high-power microwaves. USAF's information warriors are seeking ways to protect them.

to be a deployable counter-IW capability that will move with 9th Air Force units, protecting the information systems set up at expeditionary sites while advising the theater commander of the threats and opportunities facing him in an IW context.

"We're here for protection of 9th Air Force assets against computer intrusions . . . and to affect the enemy," said 609th IWS Commander Lt. Col. Walter E. "Dusty" Rhoads.

The 609th should be operational late this summer, and Colonel Rhoads expects that within two years the unit will have 100 persons—about forty officers and sixty enlisted, with perhaps two civilian specialists—who are skilled at "watching the fence" of a computer system, detecting or stopping intrusions, finding out who the intruders are, and preventing them from causing damage. It is a capability that already can "protect three or four bases," with fewer than a dozen people, and "if it provides a benefit, . . . we may set up additional units" like the 609th at other numbered air forces, he said.

Among the armed services, "we're the first dedicated unit" for this type of mission, Colonel Rhoads noted.

Though the prospect of unwanted intrusions might seem reason enough to create stringent barriers against use of Air Force networks, "we don't want to put up a brick wall," Colonel Rhoads said. To do so would hand potential enemies a "win" by slowing down the system and reducing the efficiency of USAF personnel who must move data quickly.

"The biggest threat . . . is the openness of the US system," he continued. "The whole Air Force needs to be educated about IW," and the service is "getting the word out to tighten things up."

For now, the unit "has no doctrine in place; . . . [but] several drafts are in the works," the Colonel said. The mission is so new, "we're making it up as we go along . . . and creating the blueprint for those who will follow."

The unit is developing a visual presentation to show a commander a penetration of the base network in progress—"kind of like an air defense picture," Colonel Rhoads explained. The systems envisaged will help determine which information tools the intruder is using and what damage he might be able to inflict.

Finding personnel to staff this new operation is challenging, the Colonel said, because USAF has no Air Force Specialty Codes for information warriors. For now, he is recruiting from the communications, computer service, and intelligence fields.

When called on to deploy, the 609th would take with it "computers, software and monitoring tools, fire walls, and routers," said Deputy Commander Maj. Andrew K. Weaver. "Almost all of it is commercially available," he added. "The military is using almost everything off the shelf," because the hardware and software are changing so rapidly that a military-developed system would probably always be outdated, compared with an opponent's system.

In addition to performing a kind of "electronic Security Police" function, the 609th will probe friendly systems for flaws or vulnerabilities that an enemy could exploit and help to "set up barricades . . . that they would have to go around," Major Weaver said.

Colonel Rhoads declined to discuss the 609th's capabilities for offensive IW operations but acknowledged that anything an opponent might try to do to disrupt or disable a US system could be met with a comparable response.

Nothing Is Invulnerable

Offensive and defensive IW operations are becoming increasingly important for contractors as well, because the effectiveness of the systems they provide to the Air Force inevitably hinges on the integrity of the data the systems process.

"Everything we do is aimed at insuring our product lines in tactical air," said Charles A. Anderson, vice president for Information Warfare Programs at Lockheed Martin Tactical Aircraft Systems in Fort Worth, Tex.

Mr. Anderson said his organization, recently set up to mirror the mission areas outlined in "Cornerstones," is developing the means to make certain that USAF F-16s and F-22s won't be vulnerable to IW attacks, either in the hangar or in flight.

"Suppose you were able to get into the database of a ground or airborne system and change it," Mr. Anderson said. The result could be a plane's sensors "recognizing" a friendly aircraft as an enemy or switching the target coordinates for a standoff missile. Such IW attacks could happen in the middle of a dogfight, sending missiles after phantom targets or disabling their ability to fuze. An aircraft's electronic fly-by-wire system might be crippled by electromagnetic pulses or high-power microwaves.

"We would be remiss in believing our systems are invulnerable" to such threats, Mr. Anderson said. "Nobody knows how much of this is feasible," but the company does not want to wait until it happens to start working on countermeasures.

Lockheed Martin is also working on all other aspects of IW, from sensors and processors to jammers and knowledge systems that will push collated, reliable information into the cockpit in real time.

It is important to his organization that it look at IW "not just with regard to the vulnerability of a single system but the . . . vulnerability of a total integrated system," Mr. Anderson said.

One of General Linhard's biggest concerns is that the acquisition system is running too slowly to keep up with the threats engendered by IW.

"Part of the struggle that all the services are going through," he said, "is that cycle time for a generation of computers is months, while the cycle time for our acquisition system is much longer. We must find a way to integrate the state of the art in a timely fashion."

Admiral McConnell went a step further and said, "The half-life of technology used to be months. Now it's weeks, if not days."

Enemies will constantly be watching the US for signs that it is "behind the power curve" in some area—a place where an enemy can "find a niche . . . and attack you asymmetrically," General Linhard said.

"We need to have a flexible and intelligent capability to recognize what the state of the art is," he added.

All of the information available to the US—by tapping into an adversary's communications, imagery from satellites and unmanned aerial vehicles, and electronic reconnaissance—and the ability to convert that data into a form useful for decision-making gives the US the "coercive power of information," General Linhard said.

The US is entering an age when it can enjoy "virtual presence" around the world, able to react to any action within hours by means of a stellar network of sensors and information systems coupled with aircraft and standoff weapons only hours away from any point on the globe.

Lockheed photo by Eric Schulzinger

Information now flows directly from satellites into the cockpit, which is one component of the information dominance that the US hopes to maintain over its potential enemies.

Any potential adversary will "know that we know" whatever may be going on in a given area, he said.

Mr. Anderson said he shares the concerns that the Army's Gen. J. H. Binford Peay III, commander in chief of US Central Command, expressed in recent testimony before Congress, that the US might be putting too much emphasis on IW.

"You have to be careful about moving too fast toward total dependence on IW at the expense of the pointy end of the spear," Mr. Anderson said.

Staying Ahead

Admiral McConnell observed that the US is "two, three, or four years ahead of the rest of the world" in thinking about IW and debating its ramifications, particularly as they increasingly encroach on "personal liberty, law enforcement, and national security." But the US must stay ahead, he said, because "we have orders of magnitude more to lose than the rest of the world" to IW attack.

For now, counterinformation operations are not going to replace the F-117, or any other combat aircraft, as in the hypothetical "cyber-strike" against an enemy's command-and-control nodes and power grid. Colonel Rhoads believes such a scenario might be "ten to fifteen years away" at the earliest, though he cautioned that technology might bring such a capability sooner. ■

Unmanned aerial vehicles help give the US virtual presence, feeding data to decision-makers who can react to any action, anywhere, within hours, giving the US "coercive power of information," according to Maj. Gen. Robert Linhard.