

Cracks in the Net

Foes of the West look for chinks in its technological armor

DAVID A. FULGHUM and DOUGLAS BARRIE/LE BOURGET

Western leaders are aware that network-centric operations provide their military forces with massive advantages over those who don't have the capability, but their foes also know that to have any chance at success in war they must disrupt, tap into, or destroy confidence in those networks.

This year's conflict in Iraq revealed at least one tool that would likely be used in such attacks, GPS jamming. Many intelligence-gathering, targeting and precision-weapons capabilities at the heart of network-centric warfare are dependent on faint signals from the space-based navigation system.

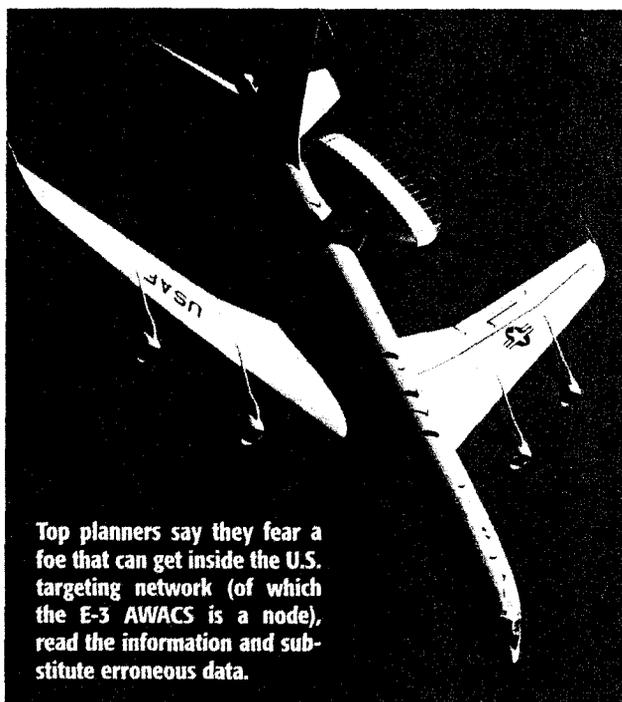
The war also refined another concern: small, pointed invasions of networks that could cast doubt on network data, even if a computer network attack were unsuccessful. Senior defense planners are no longer greatly worried about a massive invasion or shutdown of their computer networks. They worry that a network-savvy foe could plant doubts about whether a key sensor is providing accurate information.

THE EFFECT, concern that information may be corrupt or false, need only be momentary, just long enough to create doubt about a network's validity or security. Users like U.S. tactical commanders, or the intelligence community, might then be forced to ignore what could be crucial information—such as intelligence from an AWACS, Joint-STARS or Rivet Joint aircraft—during the crucial phase of an operation.

Aerospace industry and defense officials from several nations, interviewed at the Paris air show, say that the potential for attack of these military networks, and key technologies that support them, is great enough to launch new businesses dedicated to countering these emerging threats. For example, sensors (such as Rafael's Litening pod) are being developed to find and target GPS- and communications-jamming devices. Weapons (such as the U.S.-built HARM) are being improved so they can follow jamming signals and

destroy the source of electronic interference.

"Information attacks on a military network of sensors and platforms require a sophisticated effort," said a Raytheon official. "But GPS jamming



Top planners say they fear a foe that can get inside the U.S. targeting network (of which the E-3 AWACS is a node), read the information and substitute erroneous data.

USAF M50T DAME AHSCHWENGE

is a [less demanding] possibility. [Foes] know we use GPS all over the network. That's an obvious point of attack."

In addition, whole lines of all-weather weapons are being developed that aren't dependent on GPS.

"A lot of people are researching geolocation and geo-registration techniques that take images from radar or electro-optical/infrared sensors and correlate data from the scene with an onboard database," the Raytheon official said. "That's a hot area of research right now [with] Harris, BAE Systems, Boeing, Lockheed Martin and us. That gives you a way to derive geodetic targeting coordinates as an alternative to GPS." Officials from France and Israel say they also are working on these technologies as insurance against the possibility that

the U.S. could cut off or degrade their GPS access for political reasons during a national emergency.

"While a number of non-GPS techniques show a lot of promise, we don't yet know the accuracy that they can produce, their limitations or processing needs," the Raytheon official said. Also, "it will probably take a few years to figure out how to scale them down enough to put those capabilities into weapons. I think you'll see them first on aircraft, for targeting purposes, and then on weapons, as image-based terminal guidance."

U.S. officials also suggested that GPS jamming vulnerabilities may be a door that is quickly closing as a tool for asymmetric warriors—who look for chinks in network-

centric operations. "When we get 20 dB. [decibels] more signal power [from advanced GPS satellites] and we widely deploy anti-jam antennas and digitize the anti-jam technology, GPS will become about 40-50 dB. more robust to jamming than it is today," the Raytheon official said. "If you have a signal today that can be defeated by a 10-watt jammer, then it would take a 1-megawatt jammer to defeat the next-generation signal. GPS will become significantly

more reliable over the next 10 years."

Moreover, the demand for systems to protect computer networks will continue to boom for decades, predict senior planners.

"If you are a parent today, raising a youngster, one of the areas you ought to push them toward is network security," said Adm. Vern Clark, U.S. chief of naval operations, in an interview about network-centric threats, just prior to the Paris air show. "This is going to be a job market that is crying for people for the next 200 years."

More specifically, "You've got to develop anti-jam capabilities," for communications and GPS signals as well as anti-penetration defenses for computer networks, Clark said. "I think you also have to develop local hubs and redun-

dancies." These maintain parallel capabilities in case a foe is successful in damaging or penetrating one node of a network.

The fear of attack on network operations remains widespread in the U.S. military, government and aerospace industry.

"The idea that networks are going to be a target is very much on people's minds," said an L-3 official. "That's why we are not far from establishing a standard set of requirements—I should say methodology—that each network will employ to keep vulnerabilities at least tolerable."

"The easiest and most direct attack is by interrupting the communications paths," the official said. "That's why companies involved in network-centric operations have to ensure their 'most sacred nodes' aren't served by only a few communications paths. 'That's not a good design for use in battle,' he said. It is also a reason that planners give for now concentrating on what is called network topography-extensive mapping communications routes, before a system is put into service. 'We're doing lots of vulnerability studies. We have to make sure that wireless data links are anti-jam.'"

Jamming aimed at network-centric communications is expected to be the earliest manifestation of an anti-network operation.

"**THE MOST OBVIOUS** point of attack is wireless links," the L-3 official said. "If the network has a high degree of jamming immunity, it will take more powerful jammers to affect it."

Randy Bigum, Lockheed Martin vice president for strike weapons, also identified the data link environment as an area where an enemy could try to develop countermeasures. Even though it would be a difficult problem for a foe, developing the ability to interrupt or circumvent a wireless link that controls a man-in-the-loop weapon would potentially be a highly attractive countermeasure, he said.

However, increasing jamming power also threatens the jamming device by making its position easy to target with anti-radiation or jam-following weapons like HARM, that have been modified to track the necessary frequencies. "The more power they use to jam, the bigger target they provide," he said.

A murky part of the HARM missile improvement program is its "dial-a-frequency" capability, which would allow it to target both GPS and communications-jamming frequencies. Israel's Rafael missile company has related

plans that would fit its Litening navigation and targeting pod with the capability to locate and target jamming sites with enough accuracy to attack them with precision-guided weapons.

A FOE'S IMMEDIATE response to the vulnerability of jammers is to distribute them over a wide area. The jamming signal is then rapidly alternated between sites to ensure they can't be targeted. The Russians, in fact, operated "blinking" jamming systems during the Cold War. But new network-centric targeting systems, operating in real time and using data from a number of intelligence-gathering aircraft, such as the RC-135 Rivet Joint, can provide almost instantaneous targeting.

Another option for protecting wireless links would be to encode, spread communications over several frequencies and provide redundant systems. Avoiding communications jamming will differ from warding off GPS jamming, the L-3 official said. The frequencies involved are different and power needs will vary. "It will take much more to jam a Ku-band data link than the GPS signal."

More dangerous than jamming is the threat that someone could surreptitiously enter the network and exploit the information stored there or feed it erroneous data. Concerns that someone could take control of the codes and keys

and enter a real-time operational network has some U.S. officials fixated.

"The worst circumstance would be if an enemy is inside the network reading us—so they know our target information and feed us false data," the L-3 official said. "It only takes one genius. If he can hack in, he can cause you to doubt your own information." Even a few incidents could compromise a large system. "It's harder to do than jamming, but it offers the biggest payoff," he said.

"I think Vern [Clark] is on to something that we need to be very concerned about," a Northrop Grumman official said. "It doesn't take complete control [for an attack to produce results]. They don't have to capture the node. All they have to do is intrude and cause us to discount [a sensor's value] for a significant amount of time."

Those who have to confront such problems believe there is no solution, only the need to outpace the enemy's efforts.

"This challenge will never go away, so we are going to have to constantly invent to stay ahead of it," Clark said. "An enemy has to have access. He has to figure out how to penetrate. It's not easy. We are constantly developing more sophisticated techniques to deny access. They're going to keep working, and that's never going to stop from now on." 

Embracing the Foe

Moving in close hobbles
U.S. net-centric operations

DAVID A. FULGHUM/LE BOURGET

Network-centric warfare as practiced by the U.S. crushed the Iraqi army within weeks, but is now struggling to adapt those techniques to a conflict with a guerrilla force that is hard to find as it moves in small groups among a large population and urban sprawl.

"The bad news is that in a war against terrorists the network doesn't fit anymore," said Maj. Gen. (ret.) Isaac Ben-Israel, until recently the director of the defense research and development directorate in Israel's Defense Ministry. "The good news is that most of the pieces will fit if you alter the way they are used."

The Israel Defense Force (IDF) had to undergo the same transformation

since conflict with Palestinian militants began in 2000. The IDF is now engaged in an "extensive war against Hamas [and other organizations]," said Ben-Israel, who was at the Paris air show as a consultant to several defense industries. That requires the ability to watch key locations for days at a time and track individuals instead of larger military units until they are free of crowds and can be struck with less chance of unintended collateral damage.

Some capabilities become more important. For example, "The demand for UAVs is increasing every day to detect infiltration and to help in finding and eliminating certain people," Ben-Israel said. "It's a different war, and we had to change. You can still use the network to