THREAT ASSESSMENT

Terrorism

Negotiating Bin Laden's Future

Secret negotiations over the arrest of Ussama Bin Laden have been conducted in recent weeks between a representative of the Talibans, Abdul Hakim Mudjahid, and the U.S. official who coordinates the fight against terrorism, Michael Sheehan. The White House hopes the talks will result in the "diplomatic" extradition of the Saudi-born fundamentalist leader. But *Intelligence Newsletter* understands that up to now no real solution has emerged even though some progress has been made here and there. Afghanistan's strong man, mullah Mohammed Omar, categorically rejects the idea of extraditing Bin Laden but appears willing to bend to some other demands of the American administration. For instance, the Talibans have begun disarming "Arab Afghan" units and moving their camps in the east of the country to the Kabul area. Elements based at the Dronthe camp near Jalalabad who belong to the Egyptian Jihad movement led by Ayman al Zawahiri, Bin Laden's staunchest ally, were moved out. But the measure was also taken as a precaution against a possible strike by U.S. Air Force special forces. On the other side of the border in Pakistan, gen. Pervez Musharraf, anxious to consolidate his grip on power, understands the American position but has been careful to avoid appearing too conciliatory towards Washington for fear of stirring up Pakistan's fundamentalist movement. But there are limits to that policy because information gleaned from a former deputy of bin Laden, an Algerian named Sidi Tayeb, who defected in Nairobi and has taken refuge in the U.S., has given Washington new elements to put pressure on Pakistan.

Proliferation

NATO's Closed-Door Talks

Differences between the **NATO** allies on proliferation issues burst into the open on Oct. 7-8 during a discreet meeting in Palma de Majorca of the **Defense Group on Proliferation** (DGP), an ad hoc panel set up by the Alliance to examine ways to halt the spread of weapons of mass destruction.

Founded in May, 1994, the DGP represents not only the NATO nations but also several East European countries, including Russia. Rarely publicized, its work concerns measures to take against nuclear or biological warfare strikes and to foster exchanges of information on terrorist groups that could unleash such assaults. It also takes stock of anti-missile defense systems and to identify the most effective measures to deal with an unexpected missile attack. Indeed, another of the group's concerns is to plan for emergency assistance for civilians affected by a missile strike.

Some countries at Palma like the United Kingdom and France called for NGO's to be included in active civil defense arrangements in the event of an attack on a member country. That proposal stirred a heated debate, however, because it would pre-suppose that sensitive information on defensive measures in an emergency be conveyed to the NGO's. According to participants in the meeting, the plan contains too many flaws to be communicated to outside organizations. And to correct them within a reasonable time frame a number of officials proposed setting up a panel within the DGP made up exclusively of biologists.

Strategy

Russians & Turks in Pipeline Showdown

A confidential memo from the Russian embassy in Ankara provides a clear measure of how much pressure officials in charge of Russian energy policy will try to put on Turkish prime minister **Bulent Ecevit** during his visit to Moscow between Nov. 4-6. The two countries have been bargaining for long months over two ambitious projects to supply Turkey with gas.

In the instance, two pipeline projects are competing for the privilege: the **Blue Stream** backed by the Russian company **Gazprom** and the **Trans-Caspian Gas Pipeline** (TCGP) that Turkmenistan is promoting with the help of **Shell** and **PSG**, an American consortium made up of **General Electric** and **Bechtel**. TCGP aims to pump gas to Turkey from Turkmenistan's huge reserves, passing by way of the Caspian Sea, Azerbaijan and Georgia. Russia's Blue Stream project would carry Russian gas over 762 km from Izobilnoye in Siberia to Samsun, a Turkish port on the Black Sea. The final leg would run under water.

The Turkish government, however, appears firmly intent on sticking to its current supply situation which allows it to keep its eggs in different baskets. The government has chosen natural gas to fuel its future economic growth. Turkey's own gas output covers just 2.8% of current consumption and the country's needs are to rise five-fold by the year 2010. As a result, the Turkish government signed a contract with Gazprom on Dec. 15, 1997 for the construction of Blue Stream; and on May 21 this year the state-owned gas utility **Botas** penned an accord with the Turkmenistan government to build TCGP.

However, the Russian government has no intention of sharing the cake with others. During Ecevit's visit Russian prime minister **Vladimir Putin** is expected to pepper the Turkish leader complaints in the hope of getting him to relent vis a vis TCGP, in the name of good relations between Russia and Turkey.

One beef will be the existence of clandestine Turkish networks which date from the previous war in Chechnya and which pump reinforcements and supplies to fundamentalists battling Russian troops. Information

INFORMATION WARFARE

50

USA TODAY
November 8, 1999, Monday, FINAL EDITION
SECTION: NEWS; Pg. 22A

LENGTH: 606 words

HEADLINE: U.S. government tries to staunch cyber 'brain drain'

BYLINE: Will Rodger; M.J. Zuckerman

DATELINE: WASHINGTON

BODY:
WASHINGTON -- The federal government is declaring a **cyberwar** on Corporate America, its primary competition in a battle for skilled computer security specialists.

In a pronounced case of "brain drain," the government is finding that after a few years of service, it loses its best trained, most skillful computer security specialists. Those specialists go to the private sector, which offers big salaries and the potential for huge windfalls.

The Cyber Corps, a $ 16.9 million White House proposal, is meant to staunch that flow by providing college scholarships and other cash incentives in return for a military-style commitment of perhaps five years serving the government in purely defensive computer security measures.

"The greatest concern I have right now is the lack of trained people," says Richard Clarke, national coordinator for security at the National Security Council. "Getting more people into this field and enabling the federal government to compete on a more even playing field with the private sector for the best and brightest is a very important step."

Though few details have been worked out, the creator of the proposal, Mark Montgomery of the National Security Council staff, says he hopes it would work like military service, where 25% of those attending service academies complete a military career before going into the private sector, he says.

Yet, it's generally agreed that the government faces an uphill fight.

The Federal Cyber Service Initiative, or Cyber Corps, "is a step in the right direction," says Gary Beach, publisher of *CIO* magazine, which serves corporate chief information officers and technology specialists. "But I was in a McDonald's outside of Boston recently, and they were offering a $ 3,000 signing bonus for new managers. At McDonald's! You're going to see more and more upfront signing bonuses" and harsh competition for talent, especially in the technology field, he predicts.

"We're victims of our own success and prosperity," says Beach,

adding that he is familiar with a graduating class from the University of Maryland, where C-plus students are getting starting salaries of $ 50,000 in the information technology field. Government service pays from $ 10,000 to $ 20,000 less for the same jobs.

The $ 16.9 million sought from Congress is the first step for the program. In its first year, it would provide scholarships for 300 college juniors. The next year, it would be supporting 600 juniors and seniors.

Though $ 5.75 million of the first year's funding is earmarked for training current government employees, enhanced training and incentives would likely become more costly in future budgets.

Montgomery says that the government is considering seven universities as candidates for student scholarships and others are seeking to be included. He declined to identify those schools until Congress approves the proposal.

Lance Hoffman, professor of computer science at The George Washington University here, says the scholarship program could be particularly popular because it would eliminate tuition payments.

Other scholarships, he says, might do nothing to reduce the actual fees students pay because they are often offset by reductions in financial aid.

Marcus Ranum, a security consultant and president of Network Flight Recorder in Woodbine, Md., says the program is promising but might need to be expanded.

"There should be at least one person for every connection to the Internet," he says. "The military alone probably has at least a thousand connections."

Clip 52

U.S. Embassy in Moscow allows some staff to leave to avoid Y2K problems

November 8, 1999
Web posted at: 9:44 AM EST (1444 GMT)

MOSCOW (AP) -- The United States will pull out some embassy employees in Russia and three other ex-Soviet states in case anything goes wrong because of the year 2000 computer glitch, an embassy official in Moscow said Monday.

"We have what's called an authorized voluntary departure policy," said the official, who declined to be named. "People are not being evacuated, but they can choose to leave if they wish."

The decision by the State Department came after officials agreed that Russia, Belarus, Ukraine and Moldova will be among countries worst affected by the changeover glitch, which could foul up computers that cannot distinguish between the years 2000 and 1900.

The U.S. Embassy official said the State Department had asked embassies around the world to study what Y2K problems could occur and recommend possible options.

He said a committee of embassy officials agreed that some problems were likely to occur in Russia. He said the embassy did not believe Y2K-related problems would be serious, but that some nonessential personnel would be allowed to leave.

The United States had said previously that, though accidental missile launches or nuclear-reactor breakdowns in connection with the bug are unlikely in Russia, there may be power outages and communications failures.

The Moscow embassy will remain open during the New Year, the official said. He said he didn't know how many embassy employees would take advantage of the State Department's offer, which will pay for plane tickets out of Russia, hotel rooms and a daily allowance.

AsiaNow
En Español
Em Português
Svenska
Norge
Danmark

FASTER ACCESS:
europe
japan

TIME INC. SITES:
Go To ...

CNN NETWORKS:
CNN
CNN International
CNN Headline News
more networks
transcripts

SITE INFO:
help
contents
search
ad info
jobs

WEB SERVICES:

No one knows exactly how bad Y2K-related problems could be in Russia. The country's electricity monopoly -- expected to be one source of problems -- said last week it will shift its huge grid to manual control on December 31 to ensure it avoids outages.

But United Energy Systems cannot guarantee that breakdowns will not occur, deputy chairman Alexander Remezov said.

"We can't give a 100 percent guarantee that not one of these many systems will fail," Remezov said last week. He said generating plants will have a week of coal or fuel oil reserves on hand at the New Year in case something goes wrong.

Russia has done far less than other countries to prepare for the year 2000 bug, partly because it has been more focused on trying to counter severe economic problems.

But the country has proportionately fewer computers than more developed countries, and government officials have said repeatedly that no major breakdowns will occur.

RELATED STORIES:

For more US news, myCNN.com will bring you news from the areas and subjects you select.

RELATED SITES:

See related sites about US

Note: Pages will open in a new browser window
External sites are not endorsed by CNN Interactive.

LATEST HEADLINES:

WORLD:

Russian troops forge ahead in Chechnya
Mideast talks begin despite bombing
Vietnam flood toll tops 500, weather aids relief efforts
Ruling party names Labastida winner in Mexican primary

US:

Second robot to work on recovery of EgyptAir 'black boxes'
Study: Day care slightly weakens child-mother bond

54

Washington Post
November 8, 1999
Pg. 1

Military Grappling With Rules For Cyber Warfare

Questions Prevented Use on Yugoslavia

By Bradley Graham, Washington Post Staff Writer Monday, November 8, 1999; Page A01

During last spring's conflict with Yugoslavia, the Pentagon considered hacking into Serbian computer networks to disrupt military operations and basic civilian services. But it refrained from doing so, according to senior defense officials, because of continuing uncertainties and limitations surrounding the emerging field of cyber warfare.

"We went through the drill of figuring out how we would do some of these cyber things if we were to do them," said a senior military officer. "But we never went ahead with any."

As computers revolutionize many aspects of life, military officials have stepped up development of cyber weapons and spoken ominously of their potential to change the nature of war. Instead of risking planes to bomb power grids, telephone exchanges or rail lines, for example, Pentagon planners envision soldiers at computer terminals silently invading foreign networks to shut down electrical facilities, interrupt phone service, crash trains and disrupt financial systems. But such attacks, officials say, pose nettlesome legal, ethical and practical problems.

Midway through the war with Yugoslavia, the Defense Department's top legal office issued guidelines warning that misuse of cyber attacks could subject U.S. authorities to war crimes charges. It advised commanders to apply the same "law of war" principles to computer attack that they do to the use of bombs and missiles. These call for hitting targets that are of military necessity only, minimizing collateral damage and avoiding indiscriminate attacks.

Defense officials said concern about legalities was only one of the reasons U.S. authorities resisted the temptation to, say, raid the bank accounts of Yugoslav President Slobodan Milosevic. Other reasons included the untested or embryonic state of the U.S. cyber arsenal and the rudimentary or decentralized nature of some Yugoslav systems, which officials said did not lend themselves to computer assault.

U.S. forces did target some computers that controlled the Yugoslav air defense system, the officials said. But the attacks were launched from electronic jamming aircraft rather than over computer networks from ground-based U.S. keyboards.

No plan for a cyber attack on Yugoslav computer networks ever reached the stage of a formal legal assessment, according to several defense officials familiar with the planning. And the 50 pages of guidelines, prepared by the Pentagon general counsel's office, were not drafted with the Yugoslav operation specifically in mind.

But officials said the document, which has received little publicity, reflected the collective thinking of Defense Department lawyers about cyber warfare and marked the U.S. government's first formal attempt to set legal boundaries for the military's involvement in computer attack operations.

It told commanders to remain wary of targeting institutions that are essentially civilian, such as banking systems, stock exchanges and universities, even though cyber weapons now may provide the ability to do so bloodlessly.

In wartime, the document advised, computer attacks and other forms of what the military calls "information operations" should be conducted only by members of the armed forces, not civilian agents. It also stated that before launching any cyber assaults, commanders must carefully gauge potential damage beyond the intended target, much as the Pentagon now estimates the number of likely casualties from bomb attacks.

While computer attacks may appear on the surface as a cleaner means of destroying targets--with less prospect for physical destruction or loss of life than dropping bombs--Pentagon officials say such views are deceiving. By penetrating computer systems that control the communications, transportation, energy and other basic services in a foreign country, cyber weapons can have serious cascading effects, disrupting not only military operations but civilian life, officials say.

Other U.S. government agencies have sided with the Pentagon view that existing law and international accords are sufficient to govern information warfare. But Russia is challenging this view.

Over the past year, Moscow has tried to gather support for a United Nations resolution calling for new international guidelines and the banning of particularly dangerous information weapons. In comments to the U.N. secretary general published last month, Russia warned that information operations "might lead to an escalation of the arms race." It said "contemporary international law has virtually no means of regulating the development and application of such a weapon."

But the Russian initiative has drawn little backing. U.S. officials regard it as an attempt to forestall development of an area of weaponry in which Russia lags behind the United States.

In a formal response rejecting the Russian proposal, the Clinton administration said any attempt now to draft overarching principles on information warfare would be premature.

"First, you have extraordinary differences in the sophistication of various countries about this type of technology," said a State Department official involved in the issue. "Also, the technology changes so rapidly, which complicates efforts to try to define these things."

Instead of turning cyber assaults into another arms control issue, the administration prefers to treat them internationally as essentially a law enforcement concern. U.S. officials have supported several efforts through the United Nations and other groups to facilitate international cooperation in tracking computer criminals and terrorists.

For all the heightened attention to cyber warfare, defense specialists contend that there are large gaps between what the technology promises and what practitioners can deliver. "We certainly have some capabilities, but they aren't what I would call mature ones yet," a high-ranking U.S. military officer said.

The full extent of the U.S. cyber arsenal is among the most tightly held national security secrets. But reports point to a broad range of weapons under development, including use of computer viruses or "logic bombs" to disrupt enemy networks, the feeding of false information to sow confusion and the morphing of video images onto foreign television stations to deceive. Last month, the Pentagon announced it was consolidating plans for offensive as well as defensive cyber operations under the four-star general who heads the U.S. Space Command in Colorado Springs.

But complicating large-scale computer attacks is the need for an extraordinary amount of detailed intelligence about a target's hardware and software systems. Commanders must know not just where to strike but be able to anticipate all the repercussions of an attack, officials said.

"A recurring theme in our discussions with military operators is, well, if we can drop a bomb on it, why can't we take it out by a computer network attack," said a senior Pentagon lawyer specializing in intelligence. "Well, you may be able to. However, you've got to go through a few hoops and make sure that when you're choosing an alternative method, you're still complying with the law of armed conflict and making sure collateral damage is limited."

In their guidelines document, titled "An Assessment of International Legal Issues in Information Operations," the Pentagon's lawyers warned of such unintended effects of computer attacks as opening the floodgates of a dam, causing an oil refinery in a populated area to explode in flames or triggering the release of radioactivity. They also mentioned the possibility of computer attacks spilling over into neutral or friendly nations and noted the legal limits on deceptive actions.

"It may seem attractive for a combatant vessel or aircraft to avoid being attacked by broadcasting the agreed identification signals for a medical vessel or aircraft, but such actions would be a war crime," said the document, which was first reported last week by defense analyst William M. Arkin in a column on The Washington Post's online service. "Similarly, it might be possible to use computer morphing techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed. If false, this also would be a war crime."

The document also addressed questions about whether the United States would be any more justified in using cyber weapons if a foreign adversary first hacked into U.S. computer networks. The answer: It depends on the extent of damage. One complicating factor, the defense lawyers wrote, is the difficulty of being certain about the real source and intent of some cyber attacks, whose origin can easily be disguised.

In the case of Yugoslavia, U.S. military authorities were slow to put together a plan for conducting information operations. But one was

eventually assembled and approved by the middle of the 78-day war, the high-ranking officer said.

The plan involved many traditional information warfare elements--psychological operations, deception actions, electronic jamming of radar and radio signals--targeting not just Yugoslav military and police forces but Milosevic and his associates, the officer said. One tactic was to bombard the Yugoslav leadership with faxes and other forms of harassment.

Chicago Tribune
November 11, 1999 Thursday, CHICAGO SPORTS FINAL EDITION
SECTION: NEWS; Pg. 3; ZONE: N

LENGTH: 1439 words

HEADLINE: CLINTON SAYS U.S. TO BE SPARED BIG Y2K WOES;
REPORT TO PRESIDENT PREDICTS FAILURES IN SOME DEVELOPING NATIONS; U.S. AND RUSSIAN MILITARY COOPERATING TO REDUCE RISK OF NUCLEAR LAUNCH.

BYLINE: By Vincent J. Schodolski, Tribune Staff Writer. Tribune news services contributed to this report.

BODY:
President Clinton reassured Americans on Wednesday that there will be "no major national breakdowns" because of computer failures at the end of the year, but raised concerns that things would not go so smoothly in the rest of the world.

Clinton, receiving the latest federal government report on the so-called Y2K problem, said he is confident that the federal government is fully prepared for the year 2000 conversion.

"The American people can have full faith that everything from air traffic control systems to Social Security payment systems will work like they should," he said.

Nevertheless, the U.S. and Russia next month will take the unusual step of stationing high-ranking military officers in each other's countries to guard against the possibility of false warnings of a nuclear strike that might be generated by computers when their internal clocks change from 1999 to 2000.

"The greatest risk for significant Y2K-related failures continues to be in developing nations and countries that got a late start on the problem and already have fragile infrastructure systems," the report said. It cited Russia, Ukraine, China and Indonesia as "more likely to experience significant failures."

The report addressed a particular concern of some scientists: accidental launch of nuclear weapons.

"Y2K problems will not cause nuclear weapons to launch themselves," the White House promised. "Nuclear weapons launch requires human intervention."

The U.S. and Russia are working to ensure that no one in the nuclear chain of command makes decisions based on faulty data. Starting in late December, U.S. and Russian military officers will huddle at computer screens in a control room in Colorado to ensure that a Y2K malfunction in their early-warning systems does not fool either side into believing a nuclear strike has been launched.

Talks between President Clinton and Russian President Boris Yeltsin led to agreement to establish the joint control room at Peterson Air Force Base in Colorado Springs.

The base will be fed modified data gathered by the U.S. global early warning network, information meant to show the Russians that the U.S. has not launched a nuclear attack, even if their own system indicates one is under way.

While U.S. weapons systems have been extensively tested for Y2K problems and are widely believed to be safe, experts say the deteriorated systems in Russia and other parts of the former Soviet Union are vulnerable to failure.

In particular, there is concern that Y2K-related problems might leave the Russian military incapable of knowing with certainty the meaning of data from its satellites, sensors and radar.

"By itself it can't cause a spontaneous missile launch, but Y2K can increase the risk of a mistaken launch," said Bruce Blair, a senior fellow at the Brookings Institution who has studied the possibility of a global computer glitch

affecting nuclear weapons.

"A network could go blank, or issue a false alert and this could lead to bad judgment on someone's part."

Because of such concerns, a group of prominent scientists has called for some 4,400 nuclear weapons in the U.S. and Russia to be taken off "hair trigger," an alert status that means the warheads can be launched within 15 minutes.

In a full-page advertisement in The New York Times, the group urged taking the weapons off alert status and called the failure of U.S. and Russian leaders to deal forcefully with the issue "the deadliest gamble in history."

While some U.S. officials and many scientists suggest that such fears are exaggerated, they do not rule out the potential for Y2K-related problems with nuclear weapons.

"I think that it is very likely that there will possibly be very severe errors in the Russian early-warning system and the computer networks that process that information," said Michael Kraig, a consultant on nuclear weapons policy and operations at the British American Security Information Council, a Washington-based think tank.

When one of the components in the early-warning system detects what might be a hostile missile launch, horns or signals sound in control centers such as NORAD, the North American Aerospace Defense Command, in Colorado.

The commanders at those control centers then have three minutes to decide if the data are reliable.

If, after checking other sensors and satellites built into the redundant system, the commanders decide that a launch has taken place, a teleconference call is set up linking top officials in the Pentagon, NORAD and the headquarters of the U.S. Strategic Forces in Nebraska.

Between 10 and 12 minutes remain while the data are verified and radars checked before U.S. intercontinental ballistic missiles are launched.

"Within 30 minutes that command center is going to be a crater if there is an ICBM attack, so things have to be done fast," said Kraig.

During negotiations on staffing the joint center, U.S. defense officials were reluctant to provide the raw data gathered by U.S. intelligence sources.

"The information coming out of NORAD will be filtered," said Lt. Commander Anthony Cooper, a Pentagon spokesman. "It will be unclassified information."

That has led some observers to conclude that the Colorado exercise will be little more than a flawed confidence-building measure, because the Russians will know the U.S. military is seeing the classified information they are being denied, and thus the Russians cannot be sure what is actually happening.

The data will flow in one direction only, because the Russians balked at providing the U.S. with the information gathered by their own early-warning system.

Experts have suggested that the Russian military was unwilling to provide the data because it feared providing the U.S. with an intelligence windfall, revealing exactly how seriously the former Soviet system had deteriorated.

"Russia has a lot of holes in its systems and there is no way they are going to share that information with the country they have their weapons pointed at and show how vulnerable they are," said Kraig.

The U.S. early-warning system will be sufficient to detect any Russian launch, said Kraig. "Their data would basically be of no use to us anyway," he added.

Kraig said that in researching an article for a journal called "Forum for Applied Research and Public Policy," he discovered how debilitated the Russian ability to monitor U.S. weapons systems had become.

Because of the loss of aging satellites and the failure to update and repair ground radar systems, Kraig said, the Russians are incapable of monitoring missile launches from the continental United States for three hours every day.

Western technological superiority, coupled with the reluctance of the Russian military to provide its early-warning data, complicated efforts to cooperate during the runup to Y2K. The efforts also were complicated when the Russians broke off negotiations in protest over NATO's bombing campaign in Kosovo.

But the bigger problem, the experts said, was the basic conflict between the idea of lowering the missile-alert status and the long-held U.S. and Russian doctrine on deterring nuclear war. That doctrine required that each side be able to survive a potential first strike, so that neither side could expect to knock out the other's ability to launch its missiles in retaliation.

The doctrine was known as mutually assured destruction, or MAD.

Taking missiles off hair-trigger status would slow the response time to a first strike and raise the possibility that a retaliatory strike could not be launched in time--thus destabilizing the "balance of terror."

Pentagon spokesman Cooper said that U.S. and Russian officials considered the idea of "de-alerting" their strategic missiles, but ultimately rejected it for several reasons, including difficulties with verification.

Without the possibility of taking nuclear weapons off hair-trigger status, the imperfect system of sharing U.S. early-warning data with the Russians will be all that is available to deal with possible Y2K problems.

With only 52 days remaining before the new year, Clinton noted some local governments, schools, hospitals and small businesses are lagging on repairs.

He cautioned against further delay.

Wednesday's report noted that the best-prepared sectors are the federal government, power and water utilities, airlines and rail companies and telephone services.

However, only half of America's 911 call centers confirmed last month that they were ready, and more than one-third of the country's elementary and secondary schools told the Education Department they aren't yet prepared.

60

Aviation Week & Space Technology
November 8, 1999
SECTION: DEFENSE; Vol. 151, No. 19; Pg. 81

LENGTH: 1542 words

HEADLINE: Telecom Links Provide Cyber-Attack Route

BYLINE: DAVID A. FULGHUM

DATELINE: WASHINGTON

BODY:
To keep the door open for U.S. penetrations of Yugoslavia's military computers, virtually none of the country's system of cellphone, telephone, computer or Internet nodes were bombed during this summer's air campaign, except for links to the field forces in Kosovo.

As a result, U.S. military hackers were able to invade the computers that integrated the Yugoslav air defense system, a tactic that was first attempted against Iraq during the 1990-91 Persian Gulf war, senior military officials have publicly acknowledged.

Now the questions are how and how successfully was this offensive computer war conducted. And, what preparations are being made for the next war when foes will be aware that computer hacking is as likely to be a U.S. or NATO weapon as GPS-guided bombs or cruise missiles.

Both Air Force Gen. John Jumper, a committed technologist and commander of U.S. Air Forces, Europe, and Army Gen. Hugh Shelton, chairman of the Joint Chiefs of Staff, confirmed that a successful **information warfare** (IW) attack was carried out to confuse and disable the Yugoslav air defense system. "We know we had an effect, but the [IW] system isn't sophisticated enough yet to tell us exactly how effective," a senior Air Force official said.

HOWEVER, THE FIRST official "lessons-learned" document from the Pentagon indicates that the offensive computer effort was not applied quickly enough and may not have been a total success due to planning snarls. It appears that the computer attack wasn't launched before the U.S. lost two fighters to Yugoslav air defenses, one of them the seemingly invulnerable F-117 stealth light bomber. A second F-117 was damaged before the Yugoslav air defenses were finally rendered impotent.

The Pentagon outlined the problem in its report on the air war. Analysts contend that "conduct of an integrated information operations campaign was delayed by the lack of both advance planning and strategic guidance defining key objectives." Only later did U.S. computer hackers penetrate air defense computers with enough success to insert false messages and targets to protect attacking NATO aircraft. The major problem, however, was that it took too long for U.S. operators to find an offensive computer attack target and then get permission to strike. "The decision cycle and approval time was too slow," a senior Air Force official said.

Pentagon officials said they fully recognized that successfully conducting operations to disrupt or confuse an enemy's ability to collect and disseminate information is increasingly important. As a consequence, the services are going to devote a great deal of attention to developing information warfare plans and testing them in exercises.

However, the first steps into computer warfare are seen as harbingers of opportunity by defense contractors, pointing to one of the few areas where substantial fresh investments will be made and new defense programs launched. The Pentagon's report called for added emphasis on developing such technology and called for "innovative and affordable ways to exploit our technological skills in electronic combat to bring greater pressure to bear on a future enemy's air defense system."

TECHNOLOGY GIANTS like TRW, Raytheon and Boeing are already involved and moving to strengthen their efforts in what is now being dubbed the recently merged C4ISR field. That abbreviation stands for command and

control, communications, computers, intelligence, surveillance and reconnaissance. It involves the merging, fusion and overlapping of new technologies that continue to exploit the far corners of the electromagnetic spectrum.

"We think the whole area of C4ISR -- information warfare and operations -- is going to be an increasingly important part of our future," said the CEO of a major U.S. corporation involved in the new discipline. "But we'll have to see how that plays out in budgets and programs."

One attraction of the new C4ISR discipline is that it is so new and innovative that at least temporarily it may be able to shrug off some of the more onerous Pentagon acquisition rules.

"A lot of this technology can't be bought off the shelf," the industry official said. "There's no shelf for high energy lasers, missile defense or offensive computer warfare. It's changing as it's being thought about in the Pentagon. But, with Space Command taking over defensive and offensive information warfare, it should give you some idea where the Pentagon's planning is going on the subject."

While the initial intrusions made into Iraqi computer and communications systems in 1990-91 were made by tapping land lines, operations against Yugoslavia in 1998-99 appear to have involved space and airborne technology.

"I don't think there is any potential adversary that has a totally self-contained military command, control and communications system," the industry official said. "Nothing is that tightly compartmented. Everybody is using civilian commercial mechanisms through some portion of their data transport." The problem was compared to a leaky dike. "They don't have enough fingers to put in all the holes," he said. "It's an opportunity for us if we want to be intrusive."

THE INFORMAL SURVEY conducted by a former Army intelligence officer and bomb damage assessment specialist working for Human Rights Watch, William Arkin, appears to confirm that the U.S. computer assault was done through space-based satellite systems or from aircraft.

In August, Arkin was allowed by Yugoslav officials to conduct a 20-day survey of the damage done by NATO air forces during which he discovered that only three of about 30 telephone system nodes were bombed and none of the three network control stations that supported the cellphone system. The latter remained untouched even though Yugoslav sympathizers were reportedly calling in the times that NATO aircraft were taking off from bases in Italy during the Kosovo air campaign.

"By comparison, in Iraq [during 1991], the telecommunications system was bombed flat, including the urban telephone exchanges which were located in post offices," Arkin said. "In Yugoslavia, the telecommunications fabric remained intact, suggesting that it was useful for other purposes [such as intelligence gathering and computer attack]. The telephone system nodes bombed were a key one in Pristina, the capital of Kosovo, and two others in Serbia -- Kragujevac and Uzice."

All through the war, Yugoslav civilian computer operators kept up a high level of Internet activity, and international telephone calls went through without interruption, even to the U.S., Arkin discovered. He contends that the decision to attack Yugoslavia's computer system was reflected in the decision to keep as many communications links as possible untouched and operating so that the defeuders couldn't identify and block the links the U.S. used to intercept, alter aud reinsert Yugoslav electronic data.

"Clearly the whole game is to collect as much information as you can about what the enemy is doing," the industry official said. "You want to get more information than they have, deny them the ability to collect, and in an offensive sense, to corrupt or disrupt their internal data."

As to the development of new IW technology, "there is a bit of a fog right now, but we know where we have to go," the industry official said. "We are proceeding with certain parts of it. We're right now on the cusp of formulating a strategy. The fact that you could hack into a mission critical system is a pretty scary thing, so at the very least you need a defense."

Some time ago, major U.S. companies developed the ability to provide secure verification in computer

communications.

"If you are on the other end of this electronic interface, are you who you say you are?" the industry official said. "We've done this as part of normal C3I authentification for the various [government] agencies concerned with this sort of thing. And since electrons don't know if they are on the offense or defense," the technology turned to penetrating computer defenses, as a new weapon for the Pentagon.

Arkin believes the Pentagon-owned and operated MilStar and DSCS satellite constellations are the most likely routes for a computer intercept and penetration system since there are legal problems involved in using commercial satellites for military purposes. Moreover, there are other approaches being developed using manned and unmanned aircraft.

THE USAF IS MODIFYING its EC-130 fleet with offensive electronic capabilities, including the ability to intercept directional microwave beams and side lobes and alter them, that allow them to get into enemy communications systems. Similar IW packages are envisioned for the service's fleet of long-endurance UAVs.

The Army is not far behind. Maj. Gen. David Gust, the program executive officer for intelligence and electronic warfare, said the service's collection of signals intelligence gathering aircraft -- including the RC-7 (airborne reconnaissance low), RC-12 Guardrail, future Airborne Common Sensor and Tactical UAV -- are being considered for the information warfare/offensive computer attack role.
URL: http://www.aviationweek.com

MILITARY ISSUES

64

Washington Post
November 10, 1999
Pg. 39

Playing At Dirty War

By David Ignatius

Just when you think there's nothing more you could possibly learn about the Vietnam War, along comes a book that offers a startling new glimpse at that monumental misadventure.

The new book is called "The Secret War Against Hanoi," and it describes for the first time some of the devious covert operations the United States ran against North Vietnam. I've been hearing bits and pieces of this tale from ex-spooks over the years, but seeing it gathered together by a careful historian, Richard H. Shultz Jr., is a revelation.

What you realize anew, reading this catalogue of spies and saboteurs and secret operations, is that Vietnam was a laboratory for the men who had fought and triumphed in World War II. They wanted to use the same clever tools of technology and deception that had confounded the Nazis. They had won the big war in 1945 partly through code-breaking and double-cross operations, and they couldn't imagine losing this little one in Asia. But they failed, and the reasons why are a telling restatement of the larger failure of Vietnam.

The secret warriors certainly fought as hard as our regular Army troops, and they came up with some monstrously clever ideas. But many of them were blunted by bureaucrats back in Washington, who had authorized the operations but weren't prepared to follow through on them. More important, our covert actions were confounded by a peasant enemy in Hanoi who was, in a sense, too primitive to appreciate the scope of our manipulations.

The secret war was launched in 1964, under the jurisdiction of the bland-sounding Military Assistance Command Vietnam Studies and Observation Group, known as MACVSOG. The heart of the program was psychological warfare, or "psywar," which was intended to confuse and demoralize the enemy.

Americans are good at thinking up nasty surprises, especially in wartime, and they came up with some doozies. They crafted fake Chinese ammunition that would blow up in the faces of North Vietnamese soldiers--making them mistrust their weapons. They put a contaminant in rice caches along the Ho Chi Minh trail that rendered the rice so disgusting even the maggots wouldn't touch it.

Some of the tricks were replays of techniques used in World War II. Our secret warriors sent fake letters with inflammatory information to unwitting recipients in North Vietnam, so Hanoi's secret police would think the recipients were traitors or spies. They created clandestine radio stations to broadcast propaganda. When this tactic seemed to be failing, because so few North Vietnamese had radios, they decided to ship in radios, too!

The jewel of the program--the black sapphire, if you will--was an effort to create a phony opposition movement in North Vietnam called the "Sacred Sword of the Patriots League." The name was meant to evoke the legend of the Vietnamese hero Le Loi, who had used a magical sword to expel the

Chinese from Vietnam in the 15th century.

The imaginary opposition group began clandestine radio broadcasts in 1965, supposedly from its base in mountainous Ha Tinh province, which had been Le Loi's home base. Leaflets were dropped over the North Vietnamese countryside proclaiming its exploits.

To make Hanoi believe that a real resistance movement existed, the deception operation needed foot soldiers. They were gathered from among North Vietnamese POWs and poor fishermen who were kidnapped from the North Vietnamese coast by gunboats flying the Sacred Sword flag. From 1964 to '68, more than 1,000 of them were taken for "training" to a place called Paradise Island off the South Vietnamese coast, which had been fabricated to look like a liberated zone in the North.

Some of these Sacred Sword recruits were then parachuted into the North. Our dirty tricksters assumed most of them would be captured and tortured for information, but they didn't care. What they divulged about their training would only reinforce the myth that there was a real opposition group.

And our operatives were devilishly smart. They would parachute one Sacred Sword agent out the door first, and leave his comrades sitting on the bench--instead dropping a dozen dummy parachutes laden with blocks of ice. When the North Vietnamese found the empty parachutes on the ground, they would assume a far greater force had been sent in.

The poor Vietnamese agents would be given phony messages for other Sacred Sword units that didn't exist. Special spy gear and messages for this larger force would be sewn into their clothing.

It was a cynical exercise in a kind of covert tricks the British like to call "moving the furniture." And it seems to have played on the paranoia of the North Vietnamese, who came to believe that three times as many agents were operating in the North as was really the case.

But there was an inescapable problem. An imaginary movement to topple Hanoi's government could not be credible if it wasn't backed up in reality. And through all the machinations of MACVSOG, the politicians back in Washington refused to sanction any serious effort to overthrow the North Vietnamese regime. They thought that would be too dangerous.

In that sense, the United States was simply playing at dirty war in Vietnam. Operators in the field were encouraged to invent the sort of schemes that had been used so successfully in the ultimate war for life and death, World War II. But Vietnam proved to be an all-out struggle for only one side, and that was the side that ultimately prevailed.

66

Wall Street Journal
November 12, 1999
Pg. 1

The Price of Power – last in a series on military spending

U.S. Faces Defense Choices: Terminator, Peacekeeping Globocop Or Combination

By Thomas E. Ricks, Staff Reporter of The Wall Street Journal

What kind of war will the U.S. fight in the future?

Some defense experts argue that the threat will most likely come in the form of an epic confrontation with a powerful, state-of-the-art military. Say, for instance, Iran in 2025 smites its neighbors with chemical weapons and seizes Saudi Arabia's oil fields.

Others predict there won't be any more big wars -- just a plethora of enemy "ankle-biters" menacing U.S. troops with nettlesome firefights, as the Americans feed starving refugees on one block while separating warring factions on the next.

But there is growing agreement on the bottom line: Despite spending about $275 billion annually, the U.S. military isn't preparing for the battles of tomorrow. It can't attract enough recruits to meet its needs, yet it uses labor inefficiently, as if people were a free, conscripted good. Promising innovations such as unmanned aircraft are stifled by a continued focus on big-ticket armaments designed to confront the Soviet Union, including a huge nuclear arsenal of submarines, missiles and bombers.

Defense research-and-development spending is declining, and fewer high-tech companies find it financially rewarding to help the military create weapons for the information age. Meanwhile, the Pentagon oversees a vast overcapacity of bases and other installations that consume billions of dollars, thanks to bureaucratic turf wars and congressional parochialism.

"Every year we probably are wasting money," says retired Gen. Edward Meyer, a former Army chief of staff, because today's spending "isn't going to the force we necessarily will need in the future."

Yet even among those who have concluded that the armed forces are due for a major overhaul, a fierce debate is raging over exactly how to do it. The basic question is simple: If we were starting from scratch, unburdened by the baggage of past wars and threats, what sort of military would we build for the 21st century?

The answer depends on what role America wants to play in the world. Should it continue to shoulder responsibility for problems around the globe, or retreat to a strict defense of its own borders? Flowing from there are many secondary issues: Should the services be reorganized, perhaps with a separate Space Force? How quickly should the familiar weapons of the Cold War be abandoned in favor of new, information-age gear? Should the defense budget be smaller, or bigger?

In Pentagon offices, war-college classrooms and think-tank outposts, three major options have emerged. Each foresees certain kinds of conflicts, offers distinct advantages and carries unavoidable risks. Whatever course is taken, the growing consensus is that a different approach is needed-and that the terms of the current congressional debate, focused largely on incremental changes in the size of the defense budget, have become largely irrelevant.

The Terminator

With his thick eyeglasses, owlish appearance and analytical skills, Michael Vickers strikes many as the prototypical academic. But his looks belie his previous career, as an Army Special Forces soldier and operative for the Central Intelligence Agency.

Now employed at the Center for Strategic and Budgetary Assessments in Washington, a small but influential defense think-tank that advocates gradually but radically transforming the Pentagon, Mr. Vickers is considered one of the leading thinkers about the U.S. military of the future. What worries him most is the possibility of another huge war. To meet that threat, he argues for creating a formidable military to deal with big potential adversaries by deterring them and, if not, by showing no mercy in taking them on.

"I like a knife fight as much as the next guy," says Mr. Vickers, who during his military career learned to parachute behind enemy lines with a small nuclear bomb in his backpack, performed counterterrorist operations in Central America and helped equip and train the Afghan resistance for the CIA. "But the world is going in the direction of space, long-range precision strikes and maybe information operations" -- that is, attacks on adversaries' computers.

Many top military thinkers agree that numerous powerful adversaries await the U.S. in the not-so-distant future. To assume that no new adversary will emerge is to bet against history, says Maj. Gen. Claude Bolton Jr., who runs the Air Force's fighter and bomber acquisition programs. The U.S. was involved in wars during most of the decades of the 20th century, with two in the 1990s. "Somewhere between 2010 and 2020, this country will be spending a hell of a lot of money fighting another major war," he says.

Most who worry about a big challenge look to the East. The greatest military surprises in U.S. history, they note, have come from Asia: Pearl Harbor, China's intervention in Korea and the Tet Offensive. The most obvious threat is China, but some are wary of Japan, too. Even India, now just a fledgling nuclear power, could emerge as a major strategic concern, with many experts now quietly saying that within two decades it will loom larger in U.S. calculations than Russia. Throw in the East's next wave of nuclear powers, such as North Korea, Iran and Syria, and there are plenty of potential enemies capable of picking a nasty fight with the U.S.

"The price of global domination is about to go up, sharply," predicts Paul Bracken, a political scientist at Yale whose new book, "Fire in the East," argues that 400 years of Western military domination of Asia are coming to an end.

From Mr. Vickers's perspective, all this argues for a cutting-edge force of intimidating power. He contends that today's weapons -- heavy tanks, manned bombers, aircraft carriers and the like -- are "sunset systems," destined to go the way of the horse cavalry and the battleship. "By 2020, the era of tank primacy and mass armies will be over," predicts Mr. Vickers, who has been running a series of

68

futuristic war games for the Pentagon. "I think we are in a period of revolutionary change in warfare."

Therefore, he thinks the U.S. should spend the next 20 years striving for the sorts of technological gains achieved between the world wars, when the nation's small but ingenious military first experimented with aircraft carriers, amphibious landings and tank warfare.

The core of the Terminator force likely would be a small but fast-moving and highly lethal Army that would cut through enemy forces such as tanks through horse cavalry. He and others argue that sheer mass, an advantage in industrial-era warfare, will become a vulnerability because it simply presents the enemy with a larger target. Faced with advances in battlefield sensors and precision-guided weaponry, this new Army's front-line units would have to be able to scoot around in armored vehicles or even armored uniforms, never presenting a stationary target for long.

Rather than toting all their own firepower, with the tons of logistical supplies that entails, they would be able to call in missiles and rockets from the air, sea and perhaps even from space-based "battlestars" hovering in lunar orbit. For transport, they might use armored tilt-rotor aircraft that take off like helicopters but then fly like propeller planes. Robots could lead their most dangerous patrols. Overall, ground forces might look more like today's small, elite Special Forces units than current infantry and tank divisions that require more than 10,000 people apiece.

Mr. Vickers estimates that the Army of the future would require about one-third fewer troops than the 470,000 it has today. Overall, his military would total about one million troops, compared to 1.4 million now.

The Terminator force's Navy also would look very different. Some experts advocate "mobile offshore bases," huge slow-moving ships with mile-long runways that would more resemble oil rigs than aircraft carriers. But Mr. Vickers says global satellite coverage would make surface ships too vulnerable. Instead, he foresees a force of submarines and semisubmersible vessels. These would include missile-toting "arsenal ships" that would carry warheads capable of dispensing dozens of "brilliant" flying munitions that individually zero in on tbe sound of enemy tank engines.

Mr. Vickers also would give the Air Force a complete makeover, cutting its fundamental tie to piloted planes. The new Air Force would feature a mix of manned and unmanned aircraft, almost all of which would rely heavily on radar-evading "stealth" technologies. Dozens of small, unmanned bombers armed with tiny but potent 50-pound precision-guided, superexplosive bombs would hang under the wings of buge airborne aircraft carriers. And Mr. Vickers probably would recognize the growing military importance of outer space by creating a new "Space Force" that could launch attacks against spots on earth or protect satellites and other key positions in orbit.

Yet there are two major risks to Mr. Vickers's force.

First, such a leap simply might not work. A tough, precision-guided military might prove to be the 21st-century equivalent of the Maginot Line, the powerful border fortresses built by France in the 1930s. Having a strong military doesn't ensure victory. It may instead simply drive adversaries to find new, as yet unknown "asymmetrical responses" -- indirectly through terrorism, or directly by finding and exploiting cracks in the American arsenal, just as the blitzkrieg enabled the Germans to bypass the Maginot Line and shatter the French army in World War II.

Also, in the 21st century, militaries will have to operate in a world blanketed by satellites, and there is

no guarantee that the U.S. will be the one to figure out the best way to turn that globally transparent environment to its advantage.

Perhaps even more worrisome is the huge expense of creating, equipping, training and maintaining a Terminator force. It would take about a decade of intensive research to develop the new weaponry, and another decade of even heavier spending to procure it all, an effort akin to the 1980s Reagan buildup. The budget would also have to accommodate big increases for training.

Mr. Vickers argues for trimming the current military to pay for the Terminator force. But today's military leaders insist they already are overwhelmed and actually need more troops. They say that creating the Terminator force would require many more troops to conduct realistic experiments. So the defense budget likely would have to be boosted by as much as 20%, or about $60 billion a year -- far beyond the public's appetite.

Moreover, though Prof. Bracken and those in his camp may worry about military threats from Asia, his colleague at Yale, historian Paul Kennedy, warns in "The Rise and Fall of the Great Powers" that history has shown that allocating too much national wealth to the military can itself weaken a nation's power.

Globocop

Retired Marine Gen. Charles Krulak thinks Mr. Vickers's line of reasoning misses the point. "The days of armed conflict between nation-states are ending," he told Congress this year before stepping down as commandant of the Marine Corps. Instead, he argues that the military must prepare itself to police democracy's empire, fighting small skirmishes or solving humanitarian crises wherever they pop up.

His vision is a natural extension of his experience as the Marine-general son of a Marine general. The Marines always like to focus more on people and on training than on their weapons. Like many Marine officers of his generation, Gen. Krulak was molded by combat in Vietnam. What the military went through in 1969 and 1970, he once said in an interview, shaped its determination to create a highly trained, well-led, well-motivated force prepared for its missions. "If you can get through that, you carry in your heart and soul: 'Never again. Never again,' " he says. It also taught him that a determined low-tech foe can counter the conventional military might of U.S. forces.

To be ready for the future, this view holds, the U.S. should prepare its troops to deal with chaos itself. In part, that means giving troops new weaponry, such as better gear to deal with operating in a more urbanized world. But mostly it means finding good people and training them far better than they are now. It is a view widely popular in the military, which tends to focus on the next decade, during which no one is predicting the rise of a major adversary.

Gen. Krulak, who now works for MBNA Corp., a Wilmington, Del., banking and consumer-lending firm, envisions more of a "small war" military in the future -- something akin to his beloved Marine Corps. The general foresees "the three-block war," as in Mogadishu, Somalia, in 1992 and 1993, where U.S. forces on one block fed starving refugees, on the next separated warring factions, and on the third engaged in a firefight.

To move seamlessly from one of those tasks to the next, the military would be light and generally low-tech, with more emphasis on simple boots-on-the ground infantry than on snazzy new weapons

70

and remote-control battlefields. Rather than spending tens of billions of dollars on research or big new weapons systems, it would put its money into recruiting, training and paying the professional force it would need for these brushfire operations. The Navy would support the missions mainly with cruise missiles and ground-attack aircraft. The Air Force would play the role the Navy did in the days of late-19th-century "gunboat diplomacy," striking from afar with a handful of fighters and bombers to enforce the will of Washington.

The Army would move away from relying on 70-ton main battle tanks or long-range artillery pieces. Instead, it would focus on long-term, open-ended peacekeeping missions in places such as Bosnia and Kosovo. Strategic nuclear forces might be slashed to the bare minimum-probably just missiles aboard submarines, negating the need for existing land-based missiles and the nuclear bomber fleet.

If such a police force is all that is needed, the U.S. military could be cut drastically and supported by a defense budget about one-third smaller, some defense experts say.

Yet this military strategy carries two downsides.

The first is that it is easier to get into these "small war" missions than to get out of them. The most striking characteristic of America's post-Cold War military operations is that they seem interminable. U.S. forces now have been fighting Saddam Hussein for twice as long as they fought Hitler. The Army may end up spending a full decade in Bosnia -- 10 times the initial estimate offered by President Clinton on national television. Eventually, predicts Boston University's Andrew Bacevich, a retired Army colonel and an expert on international relations, "Americans will awake to an unruly world in which the United States has assumed vast burdens not easily shed."

Even more worrisome, this sort of work erodes a military's ability to wage high-intensity war. If a big war did come along unexpectedly, the American armed forces probably would be dangerously unprepared. Recently, the U.S. Army declared that two of its 10 divisions are unready for combat because they are engaged in peacekeeping missions in Kosovo and Bosnia.

This was the shock that hit England in 1914 and still resonates there today. The British imperial force had been adept at fighting Queen Victoria's small wars in remote places such as Afghanistan and the Sudan, where just last year the U.S. showed its current might with cruise missiles. But when the British army suddenly had to wage a new sort of war on the European continent, it was devastated. Unimaginative and militarily uneducated officers proved unable to adapt to the vastly different circumstances of large-scale industrialized warfare, and they led a generation of British youth to slaughter.

The less the U.S. looks able to fight a big war, the more likely it is that an adversary will try to take it on. So it is possible that pursuing a purely constabulary course today would condemn the U.S. to a big war a decade or two in the future.

The Insurance Force

Army Maj. Gen. James Dubik thinks the answer lies in a mix of Mr. Vickers's high-tech force and Gen. Krulak's low-tech boots on the ground. Gen. Dubik's vision attempts to hedge the security bet with a force that can reliably and efficiently execute police missions, but that also gets ready to confront powerful enemies in the 21st century.

Gen. Dubik has spent about half his military career as an infantryman and paratrooper, and the other half studying and teaching at military schools such as West Point and Fort Leavenworth School of Advanced Military Studies, and civilian universities including Harvard, Johns Hopkins and the Massachusetts Institute of Technology.

On his most recent overseas assignment, as a commander of the 1st Cavalry Division on the peacekeeping mission in Bosnia, he began writing an essay that considered what the U.S. military should look like after today's threats, such as North Korea and Iraq, have passed from the scene. As the Balkans winter settled in earlier this year, he spent his evenings at his Army-issue computer, tapping out his vision of the future of the U.S. military.

He prescribed a military with four main parts. First, it would have a big "prevention and war-fighting" component that would train for conventional high-intensity warfare -- and be used only for that. Second, it would have an "engagement force" for peacekeeping and other current overseas operations and for reinforcing the first force when needed for combat.

Third would be a small "experimental force" to keep the U.S. one step ahead in figuring out how to fight in the future. Finally, there would be a support force that would create the other three -- recruiting, training and managing everyone else. The existing services would remain in place, but their job now would be to supply people to each of the new functional forces.

"I wanted to start the debate," Gen. Dubik says of his essay.

He started one all right, and got himself promoted right into the middle of it. This week, Gen. Dubik took command of a new Army position as "commanding general for transformation" -- essentially, the first Army officer assigned to the 21st century. His mission at Fort Lewis, Wash., is to design the new "medium-weight" Army that is supposed to be as mobile as light infantry while packing the punch of a heavy tank unit.

The Pentagon bureaucracy is skeptical of Gen. Dubik's compromise force because it risks making the military a jack of all trades and master of none. By trying to do everything, the military could wind up doing nothing particularly well. Experimentation especially might suffer, because the Pentagon's tendency is to rob tomorrow to pay for today. So the concern here is that the U.S. could wind up with a force that is broken up for different missions yet isn't particularly adept at any of them. This isn't a small concern in an endeavor where the price of incompetence can be death. Also, establishing the Dubik force would require a massive reorganization of the U.S. military, the biggest since 1947, when the bloody lessons of World War II and the first breezes of the Cold War forced change. Little such motivation exists today: Defense matters rank low in public-opinion polls, and no presidential candidate has made defense reform a key issue. Confronting entrenched interests would require large amounts of capital, both political and financial. And it likely would be difficult to garner popular support for what amounts to an unglamorous hedging of bets.

It's hardly clear which military will emerge from today's U.S. armed forces -- if any significant change occurs at all. Indeed, the U.S. may be able to muddle along for decades with a big but increasingly ineffective military. Or the nation might retreat into isolationism and decide that the core of its military should be a wall of missile defenses. But the biggest worry among proponents of transformation is that it isn't easy for a successful military to remake itself. It was the defeated Germans, constrained by the Treaty of Versailles, who combined the tank, the machine gun and the

radio to overwhelm the French and the British militaries in 1940. Army Maj. Donald Vandergriff and other military reformers argue that the U.S. military won't really change until it is forced to do so by some sort of disaster akin to Jimmy Carter's hostage-rescue debacle in the Iranian desert in April 1980, which presaged the Reagan buildup.

The first step toward genuine transformation, military reformers argue, will be to grasp just how profound the change must be, covering everything from how the U.S. armed services recruit new people to how those troops are trained, organized and equipped.

"The Cold War was a two-generation national emergency, and it has seeped into the marrow of our bones," says Chris Seiple, until recently a Marine Corps strategist. "We have all known nothing but the Cold War."

Editor's Note: The sixth part of this series also appears in today's *Current News Early Bird.* The first five parts appeared in the *Early Bird* on September 22-23, October 12, 15, and 22.

74

Jane's Defence Weekly
November 10, 1999

Interview

Vice Admiral Thomas Wilson

Director of the US Defense Intelligence Agency

Having focused its energy and resources on developing new technologies over the past decade, the US intelligence community must now return to the "fundamentals" of intelligence gathering to successfully address today's "trickier" threats, according to Vice Adm Thomas Wilson, director of the US Defense Intelligence Agency.

"If we emphasised dissemination and technology in the last 10 years, the pendulum probably needs to swing the other way for a while," the Department of Defense's top intelligence officer says.

"We need to emphasise the quality, depth and breadth of our analysis so that we have the right balance between information and information interpretation. I don't know that we need to change our organisation or that the organisation is not right for the new world order, but I do think that to some extent we need a return to the fundamentals or a return to basics."

Perhaps the most important fundamental is people. "People are the most important asset we have in the intelligence community," according to Adm Wilson. "It is fundamentally a people business. We get great benefit from diversity in our community. We should strive for an even more diverse community, in terms of cultural backgrounds and ethnicity.

"Our business is about understanding the capability and intent of other countries and it's a pretty diverse world out there. It's a challenge for us to compete with industry and academia to recruit, train, retain and educate the workforce to give us the depth and breadth of analytical capability that we need."

Another basic function that may justify greater emphasis is human intelligence (HUMINT) gathering. "Everybody recognises and supports the need for very good and perhaps more and better human intelligence," Adm Wilson says. "It is the way to get confirmation, to get some idea about a country's intentions, as opposed to their capability.

"It takes human intelligence to sometimes understand where [new threats] may be coming from and what the nature of those threats are. It is the right kind of people with language and observation skills that we can train and retain. I particularly support a strong US HUMINT capability."

Improving the intelligence community's series of databases, some of which have atrophied in recent years including those with outdated information blamed for the US' accidental bombing of the Chinese embassy in Belgrade, Yugoslavia earlier this year must also be a priority.

"Intelligence officers are aware of database limitations," Adm Wilson says. "They're not perfect. Some are more up to date than others and you never know which one you are going to need in real time. We're used to working with that limitation. For the most part, we are able to work with it in the

targeting business. The Chinese embassy bombing was an aberration, but it was an aberration that we couldn't catch in part because of database weaknesses.

"Thcre's a tendency over time to draw away people who arc filling databases, which is a basic responsibility, to do more briefings or more current intelligence or more special assessments. We need to have a refocus on this issue of databases. We are essentially pledging ourselves to do that: prioritised, federated work on database improvements from the quality perspective from the way it's constructed, the way it's updated, the way its accessed so that in the future we can say that databases are not a weakness but a strength.

"We have the same attitude about interoperability," Adm Wilson continued, "and making our intelligence capability more easily interoperable with the warfighting systems that the military components are using. It's one thing that has changed since the Cold War. Intelligence used to be more secretive and more 'behind the green door'. Now we have easier and faster ways, technically, to directly input to the warfighters' command and control systems. There is a changed mindset that we must plug and play at that level. We have made great progress in that in the last several years but we have a way to go. Databases and interoperability with the common operational picture are essentially top priorities of intelligence."

Adm Wilson believes the back-to-basics approach must be combined with new intelligence gathering techniques to adequately address the assymetric threats that now pose the greatest danger to US national security at home and abroad. "How do you deal with the assymetric threats of terrorism, the proliferation of weapons of mass destruction, drugs, information warfare? If you stop and think about it, the assymetric threat is the threat to this country's homeland. We know people are working them from both a terrorist and military perspective.

"We recognise that we need to do some shaping of our community and our capabilities," Adm Wilson concludcd. Assymetric threats "may take a different warning apparatus and different kinds of databases, analytical tactics, techniques and procedures. We have made adjustments but we need to continue to refine and develop our systems so that we can be efficient and effective in addressing those threats even as we continue to address the foreign military threat. That's why it's not getting any easier.

"As the force structure has come down and as the threat has become more diversified or trickier, intelligence is even more important. We're engaged in a wartime pace all the time, trying to understand what is happening in this new world of ours."

- Bryan Bender, JDW Washington Bureau Chief

76

New York Times
November 7, 1999
Pg. 1

With Milosevic Unyielding On Kosovo, NATO Moved Toward Invasion

By Steven Erlanger

BELGRADE, Yugoslavia -- In early June, Prime Minister Tony Blair of Britain, the most outspoken advocate of a ground invasion of Kosovo, had ordered the preparation of 30,000 letters calling up Britain's army reserves. Typed and addressed, they were about to go into the mail, making possible the commitment of up to 50,000 British troops -- half the standing army -- to go into Kosovo.

In Washington, President Clinton, with enormous reluctance, was about to give his own approval to preparations for a ground invasion of Kosovo, including up to 120,000 American troops -- despite his vow, in a televised speech on the first day of the war, March 24, that "I do not intend to put our troops in Kosovo to fight a war."

Based on interviews with senior officials from seven governments -- the United States, Britain, Germany, Italy, France, Finland and Yugoslavia -- the United States came much closer to a ground war in Europe than is commonly understood.

On June 2, the day before President Slobodan Milosevic of Yugoslavia agreed to accept NATO's terms for an end to the conflict, the national security adviser, Sandy Berger, convened a lengthy meeting of the Clinton administration's top national security officials. The meeting included a detailed discussion of how NATO could win the war.

At almost the same time, former Prime Minister Viktor Chernomyrdin of Russia and President Martti Ahtisaari of Finland were in Belgrade, laying out NATO's terms to Milosevic, but few in Washington expected Milosevic to agree to them.

Chernomyrdin, unhappy with the terms, had nearly refused to go to Belgrade, but he listened as Ahtisaari told Milosevic that NATO would hit the city harder from the air, destroying its bridges and power plants, and was bound to invade Kosovo if necessary. Two weeks before, Clinton had said that "all options are on the table," and Chernomyrdin made it clear to Milosevic that Russia, which had supplied Belgrade radar information on incoming NATO aircraft, would be unable to help any further, even in the event of a ground invasion.

In Washington, White House officials were still looking hard for ground options short of the proposal put forth by Gen. Wesley Clark, the NATO commander, which called for an invasion by up to 175,000 allied troops. They discussed the creation of a limited "exit corridor" for displaced Albanians to get out of Kosovo, and of "safe areas" for them inside Kosovo, where they could be given food and shelter.

But the Joint Chiefs of Staff, who did not favor an invasion, made it clear that they preferred Clark's proposals to anything that committed too few American troops to too limited a goal.

And the officials knew, they say, that Clinton had just a few days to authorize preparations for an invasion if it was to be sold to NATO, a reluctant Pentagon and a skeptical Congress and carried out before the winter, giving the refugees a chance to return home. The idea of the war's dragging through to the spring -- with Milosevic damaged but hanging on to Kosovo, 850,000 refugees still in camps and the NATO alliance fraying or splitting -- "was too awful to think about," one senior official said.

The British thought they needed up to four months -- 120 days -- to prepare for an invasion, which is why the call-up letters were nearly in the mail. The Americans thought they needed less than 90 days -- but their schedule was rudely extended when they suddenly discovered that, without significant new roadwork, the large American M1 Abrams tanks could not negotiate the single route from Albania into Kosovo.

Clark, whose troops were already rebuilding the road from Tirana to Kukes, in Albania, in preparation for a possible invasion, had wanted a decision by June 1, but thought June 10 was an absolute deadline to start an invasion in September. Clinton's ambassador to NATO, Alexander Vershbow, a former National Security Council official, believed for the first time that he could sell a ground war to the alliance, despite German, Italian and Greek unhappiness, but would need five or six days to do it.

The meeting of the officials broke up with an understanding that of the three American goals for the war -- NATO's victory, holding the alliance together and keeping Russia on board -- victory had become the only outcome that mattered, even if the alliance split and the Russians broke off cooperation with the West.

There was as yet no paper for Clinton to sign, but the only plan on the table was Clark's idea of an invasion by 175,000 troops through Albania, with some helicopter assaults from Italy and possibly a feint from the north, from Hungary, to tie Yugoslav forces down.

"Clinton was going to have to decide in a couple of days," one senior official said, referring to a formal approval by the president of intensive preparations for a September ground war. "There was no way around that."

The White House announced that Clinton would meet with the Joint Chiefs on June 3.

Earlier on June 2, Berger had met a group of outside experts and analysts who had been critical of the administration and urged the authorization of a ground war. The group included a former ambassador to the United Nations, Jeane Kirkpatrick; two former ambassadors to NATO, Robert Hunter and William Taft; a former NATO commander, George Joulwan; a former State Department official, Helmut Sonnenfeldt; a RAND Corp. official, Stephen Larrabee; and two former National Security Council officials, Ivo Daalder and Jeremy Rosner, who had helped Clinton sell NATO expansion to the Senate.

Berger told them that he was still convinced the air war was working -- an opinion not universally shared -- but told them that "we will win" no matter what was required to get "the Serbs out, NATO in and the Albanians back" to Kosovo.

There were "four irreducible facts," Berger said, according to notes taken by participants. "One, we will win. Period. Full stop. There is no alternative. Second, winning means what we said it means. Third, the air campaign is having a serious impact. Four, the president has said he has not ruled out any option. So go back to one. We will win."

In a subsequent discussion, Berger elaborated: "We have not yet concluded that the air campaign is not working. But we are preparing for the possibility that it isn't." And he said that victory would be won "in or outside NATO," adding: "A consensus in NATO is valuable. But it is not a sine qua non. We want to move with NATO, but it can't prevent us from moving."

He said, "There are a number of options and a number of time lines on how to use force, and we are looking at all of them." But in fact, officials say, there was only one option by then that the Joint Chiefs would support: Clark's option, even though the Pentagon and Defense Secretary William Cohen never liked the idea of an invasion at all.

An authorization by Clinton to send tens of thousands more American and NATO troops to prepare for a Kosovo invasion would have a psychological impact on Milosevic. Ideally, the officials hoped, such a decision would bring Milosevic to capitulate without the need to send those forces into battle.

Clinton had already had severe criticism from NATO officials and even a former NATO general, Klaus Naumann, for what they called the strategic folly of ruling out a ground invasion from the beginning of the war.

At the start of the bombing campaign, American and NATO expectations were that Milosevic would give in after just a few days of essentially symbolic bombing. American estimates that he would not hold out for more than 12 days of an escalating air campaign were wildly inaccurate.

Three weeks into the war, the officials said, as Milosevic drove ethnic Albanians out of Kosovo by the tens of thousands, there was real panic in Western capitals and new strains between Berger and Secretary of State Madeleine Albright, who thought Milosevic would cave in early.

Blair was becoming convinced that a ground option was vital and made his own trip to NATO headquarters in mid-April -- just before NATO's queasy 50th anniversary summit meeting and again just afterward -- to discuss such an option.

While Clinton asked Blair in a telephone call to stop pressing publicly for a ground invasion before the summit meeting, the two men met with top officials during the meeting for a serious discussion of an invasion and approved joint planning for one, though it is not clear, some officials said, whether the chairman of the Joint Chiefs, Gen. Henry Shelton, was informed.

Clark was given quiet authorization by the NATO secretary-general, Javier Solana, after conversations with Berger, to begin to discuss ground options. And Clinton was said to have decided that a ground war, if it had to happen, would not be "a half effort," one official said.

By mid-May, Clark had come up with his plan, and it was treated skeptically by the Pentagon, which was still unwilling to authorize the use of Army Apache helicopters over Kosovo. Still, with Blair pressing Clinton and the apparent failure of the air war to drive Milosevic out of

78

Kosovo, Solana was authorized to have Clark work out a modified, detailed invasion plan. Clinton again had to ask Blair, in strong terms, to stop his government's public campaign for a ground option.

But in a photo opportunity on May 18, Clinton pointedly said that "all options are on the table," and within days, Clark was in Washington going over his plan with the Joint Chiefs. Clinton approved positioning up to 45,000 NATO troops (including 7,500 Americans) in Macedonia, to serve as part of a NATO occupation force for Kosovo if Belgrade capitulated, but as the core of a potential invasion force if not.

Pressed again by the British, Clinton sent Cohen to a secret meeting with his counterparts from Britain, Germany, France and Italy. At the meeting in Bonn, Germany, on May 27, the ministers decided that their governments would have to decide whether to assemble a ground force for an invasion, and do so pretty quickly.

So the officials, including Clark, reacted with enormous distrust and skepticism to clear signals coming from Belgrade as early as May that Milosevic was interested in discussing a deal. Despite all of NATO's public claims that Milosevic's army was being badly hurt, NATO generals understood that the army was well dug in and was not going to be bombed out of Kosovo. Increasingly, therefore, NATO strikes were aimed at putting political pressure on Milosevic and his regime by bombing civilian targets like bridges, roads, heating plants and electrical power stations.

"We knew he would have to capitulate sometime," one senior Western official said. "The only question was when. And no one expected him to cave in so soon."

Milosevic's acceptance of NATO's terms hit Washington with a shock early on June 3, and Clark and others evinced great skepticism, convinced that Belgrade was just trying to buy time and short-circuit any invasion.

But senior Yugoslav officials have said that Russian support for NATO's terms, the prospect of more intensive airstrikes against Belgrade's bridges and electrical and water systems, and, perhaps most important, the understanding that a ground invasion was imminent, were enough for Milosevic, who had won some important diplomatic shifts in NATO's stand.

Important for him, the United Nations would sanction the peace and control Kosovo, not NATO; Russian troops would be among the peacekeepers, and Kosovo was acknowledged to be a sovereign part of Yugoslavia. "It was the best moment for Milosevic to agree and save himself," one official said.

"In the end, the president concluded that he could not risk losing the war, and he was therefore prepared to send ground forces into Kosovo to assure a NATO victory," Daalder said. "But why did he and his advisers arrive at this conclusion so late into the war? Why did they not consider what might happen if Milosevic did not immediately cave when the bombing started? Indeed, why go to war if you're not prepared to go all the way?"

Daalder, now a senior fellow at the Brookings Institution, is working on a book about the Kosovo crisis with Michael O'Hanlon.

Some have contended that Kosovo has shown the possibility of winning a war with air power alone. But Daalder and numerous officials suggest that key to the psychology of Milosevic's decision was the prospect, real at last, of a ground war that he could not win and that would have decimated his army and police, two of the pillars on which his regime clearly rests. And one of the great security problems of the Balkans, as Milosevic holds on to power, these same officials say, remains his army and police, which he was able to withdraw nearly intact from Kosovo, precisely because NATO failed to destroy them from the air.

U.S. News & World Report
November 15, 1999
Pg. 45

Balkan Brinkmanship

A war plan for Montenegro amid fears of upheaval in the restive Yugoslav republic

By Richard J. Newman

Will Montenegro host the next Balkan war? Gen. Wesley Clark is taking no chances. U.S. News has learned that in early October, NATO's top general asked his bosses at the Pentagon for approval to start drawing up plans for possible NATO military action in Yugoslavia's junior republic. Clark's concern: that Yugoslav President Slobodan Milosevic, alarmed at the growing prospect of independence for Montenegro, would order a crackdown by the 12,000 Yugoslav troops there and perhaps send in thousands of reinforcements.

Intelligence officials say no such move appears imminent. But Montenegrin President Milo Djukanovic has already taken steps toward independence. Just before meeting with U.S. officials in Washington last week, for instance, he approved the German deutsche mark as an alternative currency to the Yugoslav dinar. U.S. policy makers tried to rein in his ambitions last week, cautioning Djukanovic not to count on automatic U.S. support if he tries to wrench Montenegro free of Yugoslavia. But many feel that a break with Belgrade is inevitable.

Air and sea. If war does erupt, U.S. military leaders hope to be better prepared than they were for the recent Kosovo operation, in which NATO still lacked plans for a ground campaign weeks into the war. So Defense Secretary William Cohen and Gen. Henry Shelton, chairman of the Joint Chiefs of Staff, agreed to let Clark draw up war plans for Montenegro. Those plans call for an amphibious task force, including more than 2,000 U.S. marines, to storm the port of Bar. Their mission would be to neutralize the Yugoslav Navy–particularly two diesel submarines and a handful of small ships equipped with cruise missiles–and secure the port as a beachhead for inland operations. Another key objective would be the airfield in Podgorica, the capital. A brigade of air assault troops would take that, landing by helicopter. Warplanes would keep the skies clear and target any missile or artillery batteries offering resistance. U.S. officials say other NATO countries are developing similar plans.

But the risks could be substantial, and some planners find the prospect of U.S. involvement in a Montenegrin ground war unrealistic. Rugged mountains and poor roads would make troop movements a "horrible nightmare," says one NATO official. That would make it difficult to resupply troops in Podgorica. And moving in enough heavy armor to secure outlying areas could take weeks and leave slow-moving columns exposed in valleys. A bigger problem may be the lack of political support for a military operation. "We are flying without political top cover," warned one military official in a memo on the subject. Some in Washington even worry that Clark, known for advocating aggressive action against Milosevic, might actually provoke a war by planning for one. "People are concerned about signal sending," says one Pentagon official. "There's a fine line between contingency planning and putting those plans into motion."

SCIENCE, SPACE & TECHNOLOGY

80

New York Times
November 9, 1999

Giant Hopes For Tiny Satellites

By Warren E. Leary

WASHINGTON -- The concept of less being more will take on new meaning in space next month when the Air Force launches a fleet of tiny experimental satellites made of miniature components -- diminutive machines that could one day work together in groups to replace or supplement larger spacecraft.

Driven by economics and the desire to approach working in space in a different way, researchers are exploring methods to make and use midget spacecraft -- some weighing less than a pound and hardly larger than a pack of playing cards -- that could be used alone to perform simple tasks or flown in formations to execute more complex ones.

Interest in tiny satellites that can distribute the duties and risks of working in space has grown with advances in microtechnology that are reducing the size of machines and components. For example, rapid improvements in microelectromechanical systems, or MEMS, are allowing researchers to produce switches, valves, levers, gears and other machine components that are too small to be seen by the human eye. Space engineers say they are harnessing such elements to make bantam satellites with techniques similar to those used to produce computer chips.

"The goal is to one day build a satellite on a chip," said Dr. Siegfried W. Janson, a senior scientist with The Aerospace Corp., a private research organization in El Segundo, Calif. "We're talking about fully integrated satellites that could be mass produced cheaply by the hundreds and sent into space in groups to perform a variety of tasks."

Satellites are generally classified by weight, with standard ones weighing a ton or more, small satellites coming in between 200 pounds and a ton, and microsats considered those that fall between 20 pounds and 200 pounds. The new wave of smaller satellites that engineers see for the future are so-called nanosatellites ranging from 20 pounds down to 2 pounds, and picosatellites that weigh in at less than 2 pounds.

Janson said he envisioned producing satellites weighing as little as half a pound that are assembled from layered silicon wafers containing sensors, computing power, communications systems, mechanical devices and even micro rocket thrusters. Swarms of such satellites, launched together on single, inexpensive rockets, could replace more expensive single satellites for some tasks, he said, or spread out to take on entirely new roles in space.

In addition to low cost, networks composed of dozens, if not hundreds, of inexpensive tiny satellites could offer a new standard of reliability, proponents say. If one or several of the machines in a formation fails, others in the group could redistribute themselves and continue performing the assigned task, they say, something not possible with a single-satellite mission.

Peter V. Panetta of NASA's Goddard Space Flight Center in Greenbelt, Md., agrees, saying there is growing interest in increasingly smaller satellites and other spacecraft. "This isn't just a fad," he said.

"A lot of people see this as the future and are working toward the technical breakthroughs to make these things possible."

Panetta, manager of NASA's Nanosat Technology Development Program, said the agency hoped to have a constellation of 100 nanosatellites, weighing as little as 2 pounds each, launched by one rocket on a single mission in 2008. This approach would be ideal for science missions requiring measurements to be taken simultaneously from many locations, he said, such as monitoring the amount of solar radiation absorbed by, and then reflected from, the Earth.

As a step toward the goal of flying formations of nanosats, NASA announced in August that it would sponsor the Nanosat Constellation Trailblazer mission. This flight of three, 40-pound microsats, scheduled for 2003, will test MEMS technology, formation flying and methods of operating several spacecraft as a system to pave the way for future nanosat clusters, Panetta said.

Formations of nanosats could be the only way to study certain phenomenon, he said, such as the dynamics of the magnetosphere, the area around the Earth that traps high-energy particles from the sun in the planetary magnetic field. This moving, tear-shaped region extends more than 150,000 miles from the Earth in the direction away from the sun, he said, and only a network of satellites could constantly monitor its changes.

Dr. Mark E. Campbell of the University of Washington in Seattle recently completed a NASA-sponsored study of possible deep space missions for clusters of pico or nano-sized spacecraft. Among the possibilities, he said, are teams of semi-autonomous craft that could swarm around asteroids or comets to make measurements and then assemble themselves into a communications array to send the results back to Earth. Another possibility is to send a mother ship to a planet that would release orbiting picosats that would slowly drift down through its atmosphere and send data back to Earth via the mother craft.

"My guess is that it will take 15 to 20 years to put together a system like this, but this is where the technology is heading," Campbell said.

Engineers also envision jobs for single midget satellites, like launching one along with each expensive, large spacecraft. If a problem arose with the main spacecraft, the tiny satellite buddy could detach and examine the larger ship to help ground controllers diagnose and fix the difficulty.

To test the concept of midget satellites in space, several picosats are scheduled to be launched into Earth orbit early next month on the inaugural launching of a new Air Force booster rocket. The rocket, formally called the Orbital/Suborbital Program Space Launch Vehicle but nicknamed Minotaur, uses the first two stages of decommissioned Minuteman II intercontinental ballistic missiles and upper stages from Orbital Sciences Corporation's commercial Pegasus rocket. The Air Force hopes to use surplus ICBM's as a cheap way to launch small government payloads.

Among Air Force and university payloads offered a free ride on the first flight is the Orbiting Picosat Automated Launcher, or OPAL, built by students from Stanford University. The OPAL mother ship is to fire off a half dozen pico-sized daughter satellites, including a pair built by the Aerospace Corp. and the Pentagon's Defense Advanced Research Projects Agency.

The two battery-powered satellites in this pair, each weighing about a half-pound and slightly larger than a pack of playing cards, are to be connected by a 100-foot tether to keep them from drifting too

82

far apart to communicate with one another. The satellites will spend several days communicating with one another and with a third picosat at a ground station to see how they operate as a system, and testing an array of experimental MEMS radio switches.

The tether between the craft contains a gold wire to help Earth-based radar track the tiny objects, which raises the issue of old picosats becoming space debris that could damage other craft through space collisions.

Panetta of NASA said designers were aware of the potential problem with the tiny, hard-to-follow spacecraft and see it as an issue to address in mission design. One approach, he said, is to put nano-thrusters on Earth-orbiting satellites that could be fired at the end of a mission to slow the craft enough to fall out of orbit and burn up in the atmosphere. "You don't want the solution to one problem to create another," he said.

The Washington Post
View Related Topics
November 12, 1999, Friday, Final Edition
SECTION: A SECTION; Pg. A07

LENGTH: 488 words

HEADLINE: New **Spy** Satellites at Risk Because Funding Is Uncertain, Pentagon Told

BYLINE: Vernon Loeb; Walter Pincus, Washington Post Staff Writers

BODY:
Congress has put the Pentagon on notice that a new generation of **spy** satellites--the most expensive intelligence program in the nation's history--will be scaled back next year unless money can be found for computers and communications equipment needed to process the vast stream of data from space.

The new satellites, estimated to cost at least $ 4.5 billion over the next 10 years, are designed to produce high-resolution photographs and targeting information with fewer gaps in coverage than the current generation has.

But Rep. Jerry Lewis (R-Calif.) and other proponents of the new satellites warned this week that they could become "the biggest white elephant in U.S. intelligence history" unless Congress and the White House also agree to pay for a processing and dissemination system, which would cost an estimated $ 1 billion to $ 2.8 billion.

"There is, effectively, no money budgeted now to task the satellites, process the digital data they collect, exploit the information," Lewis said. "In English: It does not do any good to take pictures that no one will ever see."

His remarks came in debate minutes before the House passed the fiscal 2000 intelligence authorization conference report on Tuesday. The Senate is expected to give its approval next week to the same bill, which directs the National Reconnaissance Office--the super-secret intelligence agency that builds and operates spy satellites--to scale back its new fleet unless money is appropriated for the processing system in 2001.

A senior intelligence official responded that the president's proposed budget for fiscal 2001 would include money for the processing system. But the official said she was "sympathetic" to congressional concerns abont where the funds would come from. "We don't have a billion dollars lying around the intelligence community," she said.

The capabilities of the new optical and radar satellites remain highly classified. But John Pike, an intelligence expert at the private Federation of American Scientists, said he believed the optical satellites would circle the globe at an altitude of about 1,000 miles, twice that of current satellites, enabling them to stay over targets for half an hour instead of just five minutes.

One Capitol Hill source who tracks intelligence issues said the new satellites would be able to provide a military commander in a tent in Saudi Arabia with computerized pictures of a spot 20 miles away in Iraq one hour after they were taken--if the processing system is funded.

In addition to the language on satellites, House and Senate conferees also added a provision to the bill making it a crime to identify publicly, by name, any retired covert CIA or Defense Department employees within five years after they have left government service. The secrecy of the names of covert operatives currently working for the CIA or Pentagon already is protected by law.

84

Richmond Times-Dispatch
November 4, 1999

Blackbirds 'Bigger Than People Think'

By Peter Bacqué, Times-Dispatch Staff Writer

The SR-71 was a sweet plane to fly, especially down low, but it could be a handful when it was running high and fast.

Blackbirds are "a lot bigger than people think," ex-SR driver Jay Murphy said. But at the same time, they were "a lot more agile than people think. It's really a lot of fun to fly, once you get down subsonic and down into the traffic pattern."

On the other hand, said Rich Graham, another "habu," their own nickname for SR-71 fliers, "supersonic, it was a different airplane."

Pilots could fly the aircraft by hand -- as opposed to letting the autopilot do the flying -- while churning along at three times the speed of sound and 15 miles up, he said, "but not with much precision in the pitch axis."

That "dead zone" in the ability to control the nose's up-and-down motion at Mach 3 complicated life in the stratospheric fast lane.

Even a 1-degree deviation from the plane's desired attitude would see the plane climbing or descending at 3,000 feet a minute, Graham explained, and distorting its finely tuned reconnaissance sensor's view.

Raise the nose too high, and the Blackbird would "depart controlled flight," Graham said. "The next step was to bail out, and it would break up."

The opposite motion was just as bad. "If you get the nose down too far, you can't pull it up," Murphy said.

Should something really go awry and the SR-71 lose power from both engines, it "has all the glide dynamics of a rock," he added.

"The book says you need 375 knots [of airspeed, or about 430 mph] for a restart," he said. But, "you could put that [control] stick all the way forward and you'll never see 375 knots."

Power-off, the aircraft would start to "maple leaf," descending and oscillating, shaking so violently, Murphy said, that it would rip checklists off their hook-and-eye fasteners.

On the other hand, "when the airplane was running right, it was a pure joy," said one of its former pilots, Tom Allison. "You have the engines running on minimum afterburner, you're in a slight climb, and it's smooth as glass.

"This thing is built to cruise," he said. "It's like cruising down the beltway in your Cadillac."

Since the SRs flew at extreme altitudes, the rates of change in what their crews were seeing below were small, producing little sensation of speed.

The only indicator of how fast the Blackbird was moving was its distance measuring equipment, notching off 33 miles every minute, the pilots said.

"Let's say you're flying 20 miles off the Soviet border and traveling at 33 miles a minute," Allison said. "You're going to have to make decisions very quickly. Otherwise, you could make headlines in a hurry."

At such velocities, timely planning for each flight maneuver was critical. For instance, pilots began to set up their landing descent from 80,000 feet and Mach 3 about 350 miles from their destination.

And occasionally, the SR-71's speed turned time on its ear, the pilots said.

"We used to take off from Okinawa at 6 o'clock early in the morning," Allison said, "and, after a four-hour flight, land at Beale [Air Force Base in California] at 7:30 the night before.

"So if it was a really good night, you could live it over again."

The bird built for speed

On July 28, 1976, an SR-71 set two world records for its class: The absolute speed record of 2,193.167 mph and the absolute altitude record of 85,068.997 feet.

The plane holds numerous point-to-point records, including one set by the SR-71 that was being delivered to the Smithsonian's National Air and Space Museum: Los Angeles to Dulles International Airport in 68 minutes.

More than 90 percent of the airplane was built from super-high-strength, lightweight titanium metal to sustain the heat encountered at speeds of more than 2,000 mph, the speed of a rifle bullet.

At Mach 3, the temperature of the plane's nose was up to 800 degrees Fahrenheit, the windshield more than 600 degrees and the engine exhaust section 1,200 degrees. Skin friction heating drove the temperature inside the plane to 300 degrees.

At top speed, more than 80 percent of the engines' thrust comes from the movable-spike engine inlet, only 20 percent from the engines themselves.

The chine, the SR-71's aerodynamic forebody, created much of the plane's lift while at the same time stabilizing the aircraft.

Aircraft originated in secrecy in 1950s

The basic design of the SR-71 originated in secrecy in the late 1950s with the aircraft designation of A-11.

President Johnson publicly revealed its existence on Feb. 29, 1964, when he announced that an A-11 had flown at sustained speeds of more than 2,000 mph during tests at Edwards Air Force Base, Calif.

Development of the SR-71s, as strategic reconnaissance aircraft, from the A-11 design began in February 1963, and the SR-71 first flew on Dec. 22, 1964.

Only 32 were built, of which 12 were destroyed in accidents or so severely damaged that they were scrapped. No SR-71 was ever lost to hostile fire, Despite being shot at more than 1,000 times.

The U.S. Air Force has retired its fleet of SR-71s because of a decreasing defense budget, the planes' high costs of operation, and advances in satellite reconnaissance.

However, new hypersonic aircraft, code-named Aurora, are rumored to be under development -- or even flying -- to succeed the Blackbird.