



# THE CYBER MENACE

## Letter to Editor

Gen. Kevin Chilton, USSTRATCOM

The world has yet to see all-out cyber-war, but it's getting closer.



By Rebecca Grant

It was a milestone in the short but nasty history of cyber-war. In November, Washington suffered from a severe, painful, and widespread attack on the Pentagon's most sensitive computers. The most worrisome aspect was evidence that the attack had official Russian state origins.

Defense officials said the strike damaged networks in US Central Command, overseer of US wars in Iraq and Afghanistan, and affected vital computers

in combat zones. Moreover, the attack penetrated at least one highly protected and classified DOD network, according to published reports.

"This one was significant; this one got our attention," a defense official told the *Los Angeles Times*.

The world has yet to see an all-out, no-kidding cyber-war, but the skirmishes are growing larger, and more numerous, a fact that does not go unnoticed in US security circles.

Russia, which has picked around the edges of DOD cyber systems for years, may finally have done it. Several intelligence sources say there is evidence of Russian government involvement, making this the first time a major cyber power has successfully invaded classified US military networks.

The specific threat in this incident was "agent.btz," a computer worm. Computer experts have reported that agent.btz can allow attackers remotely

to take control of computers and rifle their files. The infection spreads via removable disk such as a flash drive. Knowing this, DOD banned the use of external computer drives—a drastic move.

USAF's Chief of Staff, Gen. Norton A. Schwartz, received a specialized briefing about the attack. Officers at the Air Force Network Operations Center outlined efforts to halt the spread of the agent.btz worm and protect military computers.

Events in 2008 have made it only too clear that cyber threats have become everyday dangers. Leaders of USAF and other government bodies have moved from merely ruminating about threats in cyberspace to treating them as real and present dangers, especially regarding potential effects on US military forces.

Call 2008 the year that cyberspace—its vulnerability, its defense, and its exploitation—passed the point of no return as a major issue for national security officials. International events and the confluence of several major government moves drove the subject of cyberspace higher up the list of priorities.

Overseas, the August 2008 conflict between Russia and the small neighboring state of Georgia included a wave

of Russian cyber assaults directed against the government of Georgia; civilian computer experts had to step in to restore services.

### Attack of the “Botnets”

With cyberspace, the challenges are large and onerous. They range from mastering the forensic tasks of attack attribution all the way to much broader questions about proportionality of response and legitimacy of certain targets.

Even before the agent.btz attack last November, there had been a string of foreign-origin attacks on networks at the State, Commerce, and Homeland Security departments, as well as on the Pentagon.

As last year's Russian attack on DOD systems illustrated, cyber peers are already here. Most agree on the need for strong, offensive cyber options. The steady drumbeat of attacks on US systems underlines the point.

The potential threats are difficult to characterize. Said Michael G. Vickers, assistant secretary of defense for special operations, low-intensity conflict, and interdependent capability: “Nation states and nonstate actors continued to seek ways and means to counter the advantages we obtain from our use of information and to turn those same ad-

vantages against us in both conventional and unconventional ways.”

Air Force Gen. Kevin P. Chilton, commander of US Strategic Command, speaking with Pentagon reporters in Washington, D.C., expressed growing concern from a military standpoint. “I firmly believe we'll be attacked in that domain,” said Chilton. “Our challenge will be to continue to operate in that domain.”

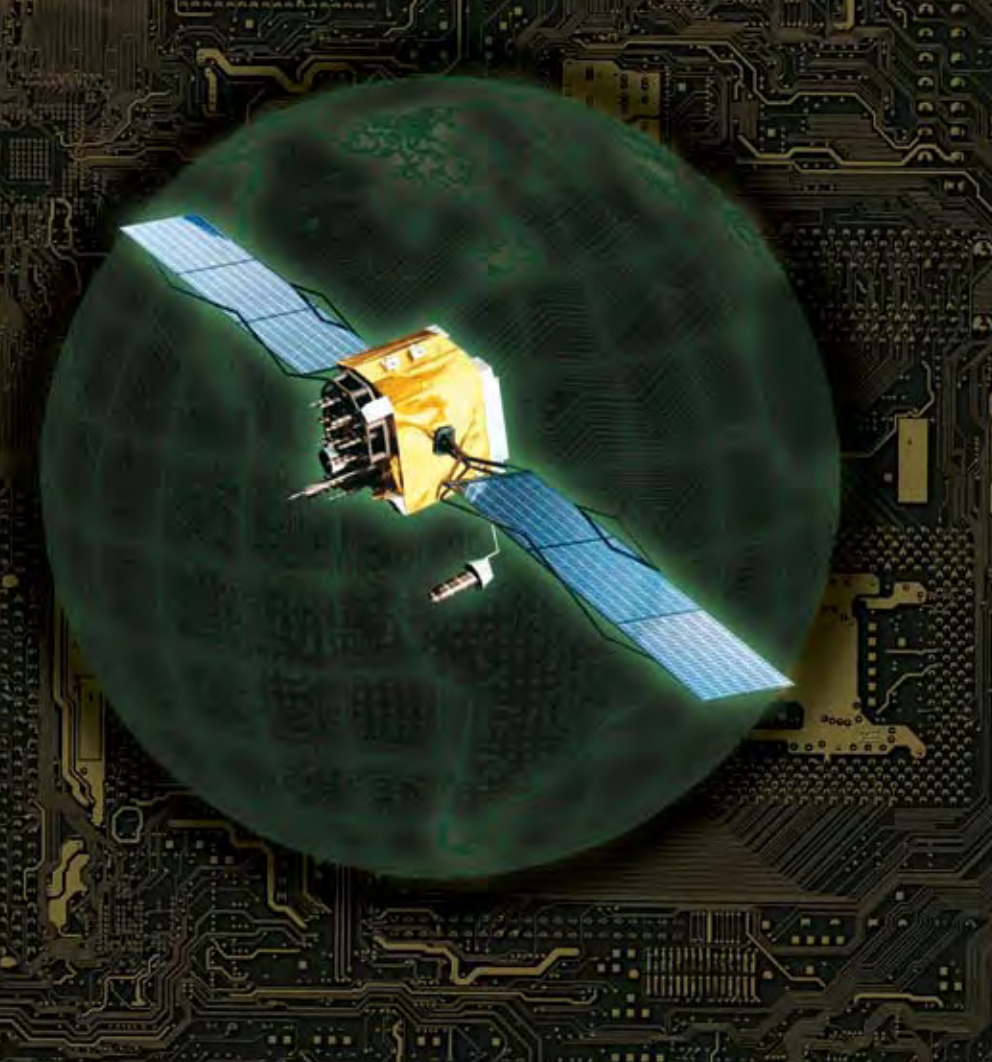
Chilton later said: “The kind of attack that you would worry about is [what] we saw in Estonia [in April 2007]—a denial-of-service attack, where they flood the system with so many e-mail ‘botnets’ you don't shut the system down, but you slow it down to the point that it's unusable.”

Russia is not the only problem. China is also on the move. There, cyberspace operations already have been incorporated into a sophisticated “layered” national defense strategy, the point of which is to confuse Taiwan's military reactions to any Chinese aggression and to slow down the anticipated deployment of US forces in response.

***Airmen and other Air Force cyber personnel are briefed at USAF's Global Cyberspace Integration Center at Langley AFB, Va.***



USAF photo by Amelia Donnell



Staff illustration by Zaur Eylanbekov

Lt. Gen. David A. Deptula, USAF's deputy chief of staff for intelligence, surveillance, and reconnaissance, had this to say: "In terms of computer network operations, the PRC remains the greatest state-sponsored threat." Deptula went on to call attention to China's proliferating abilities to deny, degrade, and disrupt cyberspace operations, labeling it a "major threat" to joint force operations.

The greatest nightmare for the US is that of an intrusion by a software program able to reach command and control or early warning systems. The November attack did not appear to reach that level, but its success was still worrisome.

At home, Washington launched a multistep program to put cyber security on a more urgent footing. President Bush in early 2008 signed a directive expanding Intelligence Community powers to monitor Internet traffic and repel mounting attacks on federal government computer systems.

The classified memorandum—National Security Presidential Directive 54/Homeland Security Presidential Directive 23—applies to several agen-

cies, including the Department of Homeland Security and the National Security Agency. It authorized a new task force, headed by the director of national intelligence, which now manages US efforts to identify the source of cyber-attacks against government systems. DHS will work to protect the computer systems; the Pentagon will prepare plans for counterattacks.

### **A Big Change of Course**

The approval of the combined NSPD/HSPD marked the most far-reaching effort to date by the United States government to neutralize threats in cyberspace. Meanwhile, the Air Force and Navy both tightened their focus on cyberspace with key organizational changes to cyberspace commands, while NATO stood up a cyber response organization.

The shock of the cyber-attacks' scope and magnitude was a point of consensus among top government officials.

With threats on the rise, the Air Force and the wider defense, intelligence, and security community spent much of the past year juggling how they will

organize to meet cyber challenges. A series of major reviews, international events, and a big change of course for the Air Force shook out more details of this new warfighting domain.

Concluded a February 2008 report of the Defense Department's inspector general: "DOD mission-critical systems may not be able to sustain warfighter operations during a disruptive or catastrophic event."

"The most important conclusion we reached is that credible offensive capabilities are necessary to deter potential attackers," testified James A. Lewis, lead author of a new report on cyberspace for President Obama.

The task of coping with cyberspace attacks never ends. As a result, the cyber defense mission is less about stopping cyber-attacks than it is about configuring and training national military forces to be able to fight through them.

Chilton has said that the US needs to be able to operate, defend, and attack in the domain, and also across various domains.

For the Air Force in particular, this crucial domain is a source of opportunity and vulnerability. USAF is the quintessential "net-centric" force. What that means, in practical terms, is that virtually all data and information of value pass at some point through cyberspace.

Brig. Gen. Mark O. Schissler, director for cyber operations on the Air Staff, explained that cyber was a bit like electricity. "Many assume it's always available," he said by way of comparison. "I assume we'll have to work to have it."

The constellation of cyber capabilities is too important—and too tempting a military target—for the Air Force ever to take it for granted. "It's not if we'll be attacked, it's if we'll be prepared for the attack," said Schissler.

With that and other operational imperatives in mind, USAF had planned to stand up in late 2008 a new major command responsible for cyber operations and defense.

Yet the service was in for a big course correction. In August 2008, Schwartz, the new USAF Chief of Staff, put that plan on indefinite hold. "Transfers of manpower and resources, including activation and reassignment of units, shall be halted," a memo from USAF headquarters stated.

There were a number of motives for the stop order. First, the Air Force's



**DOD conducts both offensive and defensive network warfare operations at the National Security Agency at Ft. Meade, Md.**

efforts to consolidate its extensive cyberspace units and budgets generated pushback almost from the start. Some in other service branches derided the planned stand-up of Air Force Cyber Command as a power grab by the Air Force.

The move toward a major command was controversial within the service, too. Indeed, the internal debate over the best way to structure cyber organizations had a bit of a history.

In 1999, for example, USAF seriously considered standing up a numbered air force to present cyber and information operations as a combat unit. “You go to war with a NAF, not a major command,” noted one general who was involved in the decisions then.

That logic remained compelling to many. In fact, according to Schissler, forging a numbered air force was one of the original options presented by the Secretary of the Air Force Cyberspace Task Force in 2006. Many cyber planners remained convinced a NAF was the best way for the Air Force to go.

The Air Force’s cyber plans have been “largely misunderstood,” said Schissler, who characterized the strategy of then-Secretary of the Air Force Michael W. Wynne as “a wake-up call, not a takeover.”

Gordon England, the recently departed deputy secretary of defense,

spelled out a broad Pentagon view in a May 2008 memo. It stated: “Because all combatant commands, military departments, and other defense components need the ability to operate unhindered in cyberspace, the domain does not fall within the purview of any one particular department or component.”

At the Corona conference in fall 2008, the Air Force put the cyber mission back on track toward the numbered air force solution. Under the new plan, USAF will stand up the new 24th Air Force under Air Force Space Command in mid-2009.

### Natural Fit

This NAF thus will become the Air Force’s cyber combat element. It will combine network operations as well as offensive and defensive cyberspace capabilities for presentation to the joint warfighter, US Strategic Command.

Although this decision was announced at about the same time as USAF’s choice to create the new MAJCOM-level Air Force Global Strike Command, the decisions were actually unrelated.

Among the key elements that will move under 24th Air Force are the existing 67th Network Warfare Wing and the Air Force Information Operations Center, both located at Lackland AFB, Tex. The two units currently fall under 8th Air Force, which is part of Air Combat Command. When those

units become part of the new 24th Air Force, however, they will align under Space Command.

While the stand-up of 24th Air Force tracks with earlier thinking, the choice of Air Force Space Command as the home for cyber is an about-face on how to manage the new domain.

Previously, some worried that linking cyber to space would blur the budget authority and career path for cyber-warriors. The old decision to tuck cyber into Air Combat Command reflected those concerns.

In 2007, Gen. Ronald E. Keys, then commander of ACC, explained the logic of keeping cyber within the combat command. “There’s a dynamic in Washington, when you have something new [like Cyber Command]: Either they will stiff you, or they will run with you because they think there’s money they can get from you,” he said. “So we have hooked all the cyber/Internet systems into Air Combat Command.”

Missionwise, the cyber world may have a more logical connection with Space Command, however. “It’s a natural fit,” commented Schissler.

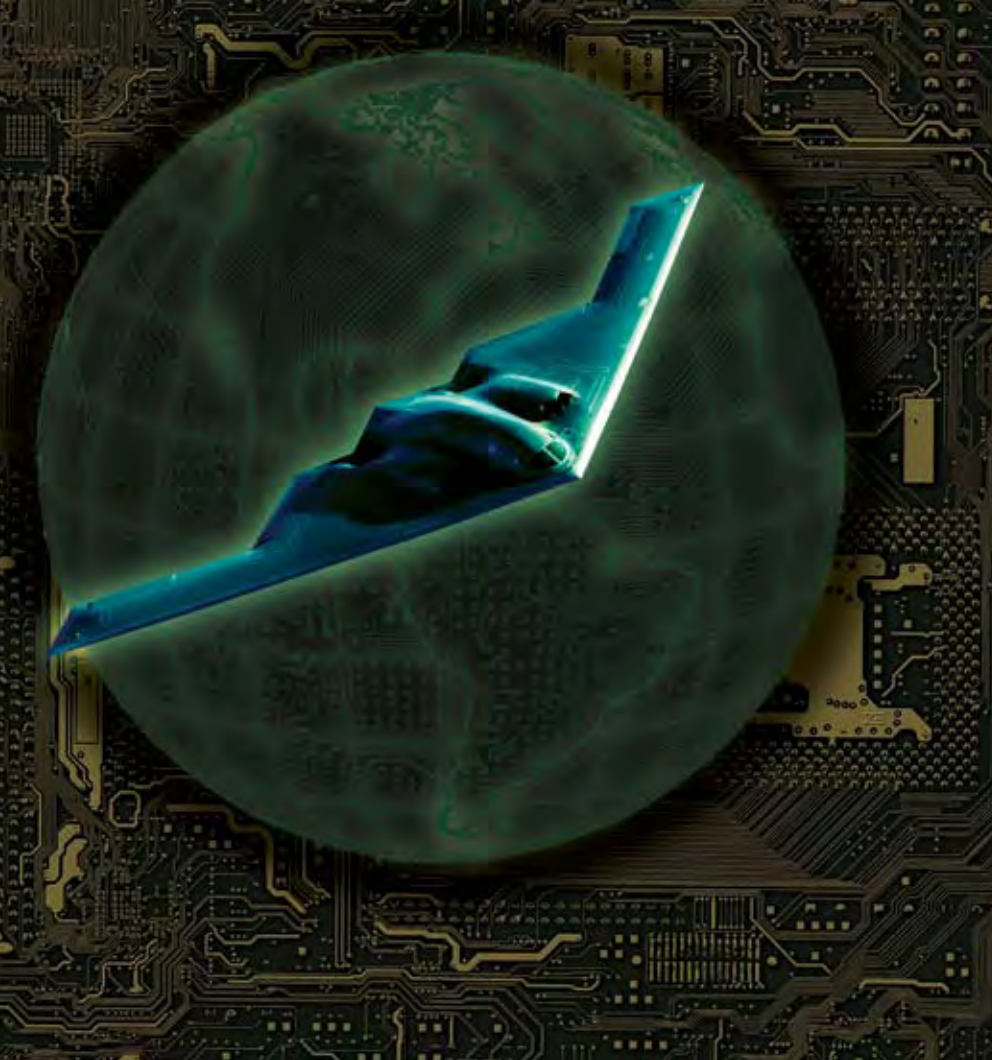
As many as 8,000 airmen will become part of 24th Air Force. Many of these are in place at other organizations, and Air Force units host cyber specialists from other organizations. The Air Force has announced six possible locations for the headquarters of 24th Air Force. A final decision is expected by June, an Air Force news release said.

Schissler also envisions a big role for Guard and Reserve forces. “They have remarkable capabilities and potential,” he said. Many Guardsmen and Reservists work in private-sector information technology positions. Meanwhile, many of the nation’s Total Force units are slated to lose their traditional flying missions.

Other parts of the cyber bureaucracy were in motion, too. Two particular changes were aimed at strengthening cyber security by recasting the battlespace.

The first focused on the Department of Homeland Security. The second involved the agency at the core of US cyberspace missions: the National Security Agency, home of elite cryptologists and those most skilled in offensive and defensive operations.

January 2008 brought a new Comprehensive National Cyber Security Initiative (CNCI). It wasn’t exactly



Staff illustration by Zaur Eylanbekov

unveiled, as the initiative is classified, but some of its content seeped out in appropriations discussions and other settings.

Released on Jan. 8, 2008, the classified, joint directive reportedly authorized a 12-step program to improve the overall security situation. The steps took aim at everything from intrusion detection and trusted Internet connections to classified network security and global supply chain security.

The CNCI also tasked NSA to monitor all federal networks to improve cyber intrusion detection. Those not complying could have their access turned off.

Early in 2009 came word of another decision with great significance for cyber warfare. This was the move to put the NSA director in charge of US Strategic Command's Joint Task Force for Global Network Operations.

For many years, a network warfare component has resided within the supersecret cryptological agency based at Ft. Meade, Md. This component has focused mostly on defense of national networks from intrusion and exploitation. Personnel from various armed

services work at NSA in cyber warfare roles. The Air Force, in particular, has a large number of cyber specialists working there within that component.

What's new is the formal assignment of both offensive and defensive cyber roles to a component at NSA.

The Air Force's Schissler observed that this new national arrangement is actually building on a proven pattern: It mirrors the organizational concept embodied in the Air Force's 67th Network Warfare Wing, in that it puts "the main exploiters" and the "main defenders" together under one roof.

### Determining Attribution

Outsiders cannot tell at present exactly what NSA will do with this authority. Schissler said one prospect was for NSA to create a national cyber center resembling the National Counterterrorism Center, a multiagency organization within the Office of the Director of National Intelligence.

In Schissler's view, the goal would be to forge a single, joint monitoring center combining the intelligence, military, homeland security, and law enforcement cyber specialists. It could also serve as a command post for offensive and defensive cyber options. With the current fragmented system, Schissler noted, "we make it work," but it's not easy.

Many think the United States needs to do more to develop an offensive cyber-war capability rather than just focus on defending its networks from attack.

Yet the concept of military campaigns in cyberspace is still hung up on the issue of attack attribution.

"We have a tremendous amount of trouble determining attribution: ... where an attack actually came from, who was responsible, who might have been behind that computer," former White House cyber security official Paul Kurtz told the House Intelligence Committee in recent testimony. "And we have a very, very long way to go on that. Until we start to get clarity in that piece, it's going to be very difficult to contemplate the military option, of responding appropriately."

Schissler confirmed the difficulties of knowing "who in a country has attacked you." Any peer is likely to have strong network capabilities, he said, and "our most dangerous opponents are the militaries and intelligence services of foreign governments."

One thing is certain: The services will continue to provide a large share of the personnel dedicated to cyberspace. "Secretary of Defense [Robert M.] Gates has told us to fill all the seats" at joint cyber schoolhouses, noted Schissler.

Cyberspace still is not part of DOD Directive 5100.1, an omnibus document covering official department responsibilities and authorities. Thus, neither the Air Force nor any other service has a special claim on it. Yet it is the services that have recognized their dependence on the cyber domain and set out to organize, train, and equip forces for cyber operations.

The way is wide open for someone to step forward and give shape to the new challenge. Said Schissler, "It's a Billy Mitchell moment." ■

---

*Rebecca Grant is a senior fellow of the Lexington Institute and president of IRIS Independent Research. She has written extensively on airpower and serves as director, Mitchell Institute, for AFA. Her most recent article for Air Force Magazine was "The Murky Future of Stealth," which appeared in the February issue.*