We may look back on the present hacker attacks as the good old days.

Threats to the

Nets

By Michael C. Sirak

THE power to gain information superiority over any foe and ensure unimpeded delivery of information to American armed forces are key parts of US warfighting doctrine as spelled out in Joint Vision 2020. More and more, the Pentagon relies on computer networks to drive its worldwide array of sensors, communications links, and analysis tools and to disseminate information around the globe. And as this reliance grows, so too, do the dangers associated with network vulnerabilities.

Secretary of Defense Donald Rumsfeld has warned, "Our dependence on computer-based information networks makes those networks attractive targets for new forms of cyber-attack."

In fact, the Pentagon's networks have already come under heavy bombardment. Last year, DOD's unclassified computer systems experienced 23,662 detected "events," or attempted intrusions, which is up from 22,000 cases reported in 1999. The upward trend is continuing. In just

the first three months of this year, DOD said its computer sleuths detected 16,482 events. Even taking into account more comprehensive reporting methods and better monitoring capabilities, the total number of attacks will wind up showing a hefty increase this year.

Officials said that, to date, they mostly have been successful in thwarting intruders. However, they acknowledge that there is growing concern about the increasing sophistication and frequency of the attacks.

Today's attackers range from lone hackers and hacker groups to what DOD considers more refined intrusions staged by criminal gangs, terrorist organizations, and sophisticated state-sponsored enterprises. "We are under attack every day," said a Pentagon intelligence analyst with regard to the low-level hacker-type threats. To date, most hacker attacks have sought to disrupt, but not destroy, DOD's operations, the analyst noted.

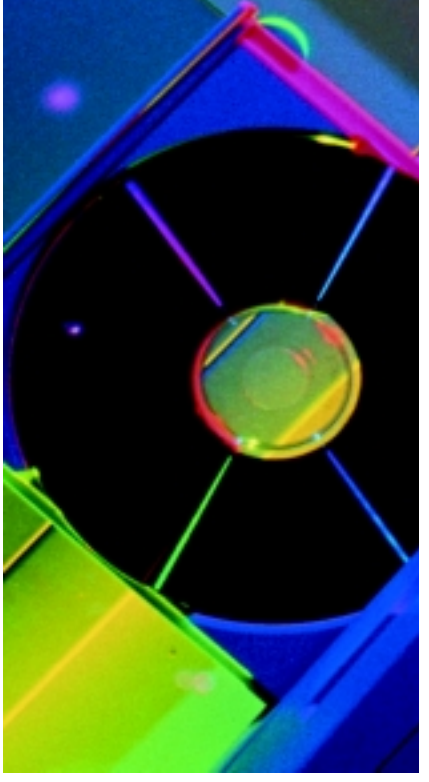
More ominous, however, is the specter of state-sponsored attacks. A recent study by DOD's Defense Science Board reported that some 20 nations are pursuing capabilities for information warfare. Topping the list is China, which announced openly its intent to devote large resources to this area as an asymmetric means of countering US conventional military strength. Unlike the hackers, who usually are thrill seekers in a quest for fame and notoriety, state-sponsored attackers seek to extract information while lurking undetected.

At risk, in the DSB's view, is the Pentagon's vast assemblage of networks, known as the Global Information Grid or GIG.

The New Arms Race

"The GIG is a weapon system and must be treated as such," said the DSB report. "The nation is in an arms race with regard to superiority of such capabilities. Experience suggests that as US defensive capabilities increase, so will the adversary's offense."

To counter the threats, DOD is mounting a comprehensive effort, under the leadership of US Space Command, to establish a coordinated Computer Network Defense system. While the emphasis today is focused on fielding a potent defense, the command is also working simultaneously



on incorporating into US warfighting doctrine the capability to target an adversary's own computer networks. The goal, command officials said, is to have warfighting commanders come to rely on Computer Network Attack operations as an effective tool at their disposal just like any other weapon system.

US Space Command officials, headquartered at Peterson AFB, Colo., said they are making significant strides in standing up the tactics, techniques, and procedures needed for effective CND and CNA operations. Still, they said, this mission forces DOD into uncharted territory, with many challenges ahead. "We are starting from a blank sheet of paper here," said Army Lt. Gen. Edward Anderson, US Space Command's deputy Commander in Chief. "This is not something [where] we can open up some books or open up some file folders and see how it used to be done, because basically, it is a new task for the military."

In its study, the DSB chronicled the defensive challenges ahead. Among its main findings was the study's claim that DOD remains too focused on low-level hacker-type attacks. The Pentagon, it said, "cannot today defend itself from an information operations attack by a sophisticated nation–state adversary" that understands how to exploit compromised data. The science board further asserted that there is "a serious shortage" of information technology professionals within the Pentagon, with the expectation that the shortage will become even more acute.

Needed: $3 Billion

Annual expenditures of some $3 billion—roughly twice the current amount—are needed to adequately protect DOD's systems, the board noted. "If Joint Vision 2020 is to be the path to the future, these vulnerabilities and shortfalls must be addressed," stated the board.

The latest version of the Pentagon's Unified Command Plan, dated Oct. 1, 1999, assigned US Space Command immediate responsibility for Computer Network Defense. Army Gen. Henry H. Shelton, Chairman of the Joint Chiefs of Staff, said the command was "a logical fit," given its global perspective and its collection of experts adept at operating computers, communications systems, and space assets. Exactly one year later, on Oct. 1, 2000, the command acquired the mission of conducting Computer Network Attack.

As part of all of these changes, SPACECOM was given authority over Joint Task Force–Computer Network Defense, which the Pentagon had set up in late 1998 to coordinate and direct defense of its computer systems. However, the task force did not have any role in attack. That changed in April 2001, when US Space Command expanded the task force's mission and gave it operational control of both CND and CNA, changing the name to Joint Task Force–Computer Network Operations. In the beginning, it had a staff of about 25, but it will expand to 145 personnel.

The JTF–CNO works with the services, the Defense Information Systems Agency and its DOD–Computer Emergency Response Team, National Security Agency, Defense Intelligence Agency, and other entities. It develops methods to assess the operational impact of intrusions, identifies proper responses, coordinates actions with appropriate organizations, prepares response plans, and—with US Space Command approval—executes the plans through the command's service components.

For example, the task force oversees all Information Assurance Vulnerability Alerts, which DOD–CERT issues whenever it identifies vul-

nerabilities that require immediate corrective action such as software patches.

SPACECOM is responsible only for protecting networks belonging to DOD or the armed services and not those of other government or private organizations. It coordinates its activities, however, with other cyber-defense entities. The main federal effort centers on the FBI's National Infrastructure Protection Center in Washington. The NIPC, established in 1998, works with the federally funded CERT Coordination Center at Carnegie Mellon University to detect, assess, and develop responses to cyber-attacks.

There is no question, however, that the Defense Department ranks as the major target. The Pentagon's GIG comprises the Non-Secure Internet Protocol Router Network (NIPRNET), the Secret Internet Protocol Router Network (SIPRNET), the Joint Worldwide Intelligence Communications System, and each service's tactical command, control, communications, and intelligence system.

Army Maj. Gen. J. David Bryan, commander of JTF–CNO and vice director of DISA, said NIPRNET currently serves more than 2.5 million users through 1,503 post, camp, and station connections. Since 1996, its customer base has grown 20 percent and its total traffic has expanded by 400 percent, he noted. SIPRNET, said the general, has become "the most critical data system supporting the warfighter today." Currently, it serves approximately 125,000 users at more than 900 connections. Over the past five years, it has experienced a 200 percent increase in customers and more than 600 percent increase in traffic.

Sources of Danger

Potentially hostile nations such as China, Russia, Cuba, Iran, Iraq, Libya, and North Korea are developing capabilities to attack this system. Also developing their own cyberwar powers are several US allies and friends such as France, Israel, and Britain. Even some of the world's most significant neutrals such as India and Brazil are getting into the act.

Anderson, US Space Command's deputy CINC, said, "Major countries, Russia and China, have openly said that they are undertaking activities because they see our dependence upon [our computer networks] and they see the possibility of using it" to their advantage.

State sponsorship affords an intruder a base of operations, protection, time, resources, and a clear focus, explained one top DOD intelligence analyst. "Once you get to the state-sponsored level, they understand the repercussions of what they are doing," he said. "That is a very conscious effort and needs a very conscious response."

Anderson said the command faces the major challenge of trying to prepare for unknown, never-before-seen types of network attack. "It is ... the 'we-don't-know-what-we-don't-know' problem because these capabilities will not have been seen" until they are employed, he said. "We are doing a lot with a lot of different agencies as far as working this problem and we have come a long way, but at the same time, we still realize that we have a long way to go."

Hacker groups are cause for concern, Anderson added.

"I think it is reasonable to expect that, as they develop capabilities, [and] they then start to try to market those, they could market them to potential adversaries," he said. Further, he said, "Hacker groups could market themselves, and not just their tools, but themselves as mercenaries." Anderson made clear that, thus far, he has seen no evidence that such activities have occurred, though it is "within the realm of the possible."

Attackers seek to exploit the weak link in any network chain. "To attack a large number of systems, an adversary need only find and attack a single exploitable connection to the system (through the use of a wide and growing variety of commonly available and inexpensive hacker tools)," stated Linton Wells, who was acting assistant secretary of defense for command, control, communications, and intelligence when he testified to Congress in May. "Once inside a system, an adversary can exploit it and the systems networked to it."

This has, in fact, happened. Take the case known to investigators as Solar Sunrise. In 1998, two teenagers from California and one from Israel combined forces to penetrate computer systems at 11 Air Force and Navy bases. The hackers succeeded in disturbing the normal operations of those systems, causing DOD to rethink its lax security measures.

Menace by Moonlight

To date, the largest apparent intrusion of DOD's networks occurred under a case known variously as Moonlight Maze and Storm Cloud. Starting in early 1998 and continuing into this year, millions of unclassified yet sometimes sensitive documents have been sucked out of Pentagon systems and into computers traced back to Russia. Whether the intrusions have occurred at the behest of the Russian government or criminal elements inside Russia remains undetermined, US officials have said.

Further details of this strange case were provided by James Adams, head of a cyber-intelligence and risk-management firm and member of the NSA's advisory board. Writing in a recent issue of *Foreign Affairs*, Adams noted:

"The attacks appear to be coming from seven Russian Internet addresses, but it is unclear whether the initiative is state-sponsored. Last year, Washington issued a demarche to the Russian government and provided Russian officials with the telephone numbers from which the attacks appeared to be originating. Moscow said the numbers were inoperative and denied any prior knowledge of the attacks.

"Meanwhile, the assault has continued unabated. The hackers have built 'backdoors' through which they can re-enter the infiltrated systems at will and steal further data. They have also left behind tools that reroute specific network traffic through Russia.

"Despite all the investigative effort, the United States still does not know who is behind the attacks, what additional information has been taken and why, to what extent the public and private sectors have been penetrated, and what else has been left behind that could still damage the vulnerable networks."

Another wave of attacks occurred after the collision this year of a Navy EP-3 reconnaissance aircraft and a Chinese fighter aircraft off the coast of Hainan Island. The crash resulted

in the death of the Chinese pilot. In the weeks and months following the incident, US and Chinese hackers engaged in a cyber-battle, each side trying to deface and disrupt Web sites in the other's country. Chinese efforts were said to have occurred with at least the tacit support of the Beijing government. Chinese hackers subsequently archived an extensive set of hacking tools at a freely accessible Web site.

This summer, DOD was hit with the new Code Red virus. Those who unleashed Code Red did not directly target DOD networks, yet the virus still forced the department, as a precaution, to shut off public access to many of its unclassified sites on several occasions for several days at a time.

Potential Havoc

The Air Force's Air Intelligence Agency, the service's operational arm for information warfare, reported 45 incidents of attempted disruption or exploitation of Air Force operations in the year 2000. In 15 of these 45 incidents, intruders succeeded in fully penetrating some Air Force systems and could have wreaked havoc, had they not been detected, the agency said.

The task of differentiating between an attack and other random computer anomalies remains difficult, SPACECOM officials said. "It's important to remember that network malfunctions and attacks have the same symptoms and effects," said Brig. Gen. Dale W. Meyerrose, the Air Force officer who directs command-and-control systems within the command. "However, the corrective action for a malfunction may differ greatly from a defensive action when the source of the problem is an enemy and the intent is to harm or disable DOD networks."

USAF Gen. Ralph E. Eberhart, the head of US Space Command, said DOD possesses capabilities to counter the intruder, once it knows its computer networks are under attack. However, this "burglar alarm" technique, as the general calls it, is a passive approach. The US must wait on an attacker to make the first move.

A more effective defense, he said, must incorporate predictive and active, pre-emptive measures, making better use of intelligence and allowing the defenders to take steps to prevent, deflect, or minimize the effects of any hostile action. Eberhart calls this a "neighborhood watch" capability.

Anderson noted that acquiring such an "indications and warning" capability is no easy task. "That is a huge challenge for both technology as well as the Intelligence Community to be able to provide those kinds of things," he said. "We don't have that kind of capability right now."

US net warriors face another enormous challenge—making accurate attribution of specific acts to specific individuals or entities. It is surprisingly difficult to trace the path of an attack back to its source and thereby identify the malefactor. The difficulty of making accurate and timely attribution calls stems not only from the immature state of technology but also from the strictures of US law.

According to Air Force Lt. Col. John Pericas, chief of the CND operations branch at SPACECOM, current law bars the Department of Defense from tracing an intruder's attack back through more than one Internet service provider address—or "hop." At that point, law enforcement must be brought in. At times, said an intelligence official, DOD may have technologies that would permit more accurate tracing, but the legal framework lags behind, sapping the initiative. "We can't conduct recon outside our networks," he said. "We'd like to, but we can't."

The DSB report highlighted these and other problems that limit the Pentagon's ability to defend its computer networks. In fact, said DSB, such defense won't be possible without extensive and concerted effort. "Incremental modifications to our existing institutions and processes will not produce the adaptation we need," stated the DSB study.

GIG Bite

The GIG is becoming increasingly vulnerable, the board found, stating, "Development and deployment of new network technology has greatly outpaced information assurance technology, thereby increasing the vulnerability of DOD systems."

The DSB report recommended that the Pentagon and the armed services move all of their public Web sites off the NIPRNET and into a more controlled environment, characterized by encryption and digital identification keys. A public key infrastructure with public key-enabled applications "must be a key component of the GIG security architecture," said the study.

The board deemed it critical for DOD to develop certain technologies that can be used after an attack to help recover and restore networks and the data they contain. Unfortunately, "today DOD has no methodology for dealing with the consequences of a successful attack and restoring integrity in its systems," noted the study.

Greater investment in CND and CNA research and development is essential, the board found, noting that the Pentagon should focus funding on global access control, malicious code detection and mitigation, mobile code security, fault tolerance, integrity restoration, and recovery and reconstitution.

The study also cited a need for DOD to establish a distributed test bed to evaluate information assurance measures. It urged Pentagon officials to assign priorities within parts of critical infrastructure, including certain private-sector assets on which it relies. Many of these could prove to be highly vulnerable to attack and exploitation.

What the Pentagon needs, board members concluded, is a defense in depth, consisting of layered security measures that are more likely than any single system to detect an attack. The DSB study pointed out that, over the past several years, National Security Agency "Red Teams" secretly staged mock assaults on DOD networks. Some 99 percent of them went undetected, even though the Red Teams attacked with known tools.

The board, recognizing the damage that one disgruntled computer network "insider" could cause, recommended an increase in background checks and security training. It also called for a better system to train DOD operators to replace the fragmented one now in place. Further, it cited a need for greater efforts to attract and retain skilled information technology professionals.

The board also called for the creation of a "national coordinator for

Continued on p. 28.

Continued from p. 26.

Defensive Information Operations" to oversee all of the nation's cyber-defense efforts. It also suggested a "Commander in Chief–like organization" to coordinate government and industry defensive actions.

Loosen Up

The board called on the FBI to drop the institutional and political barriers surrounding the NIPC and make available the kinds of information that could be critical to DOD in carrying out its defensive mission. The FBI has a reputation in the field for refusing to share critical information with anyone, including US defense authorities. As the task force concluded, "These barriers should be removed, and soon, if DOD is to continue to support and rely upon NIPC. Unless NIPC, FBI, and Justice overcome their narrow crime fighting perspectives—in a formal high-level agreement with the Defense Department—then DOD and the Intelligence Community should consider pulling out of NIPC to create an independent center for gathering and sharing information about the most serious network attacks. But this should only be a measure of last resort."

In spite of the challenges and current shortcomings highlighted in the DSB study, US Space Command continues to refine and improve CND capabilities, command officials said. The command is working to put in place later this year a revised alert system in which all DOD command echelons will have standard guidelines for reacting to protect their networks.

The focus of the new alert system is to keep the networks up and running to maintain the flow of information to the warfighter while network defensive operations are being carried out to thwart the intruder. Under the previous alert system—DOD's first attempt at a standardized warning capability—operators would shut down the networks as part of the defensive countermeasures.

That was not smart. As Pericas noted, it not only thwarted attackers but halted the flow of critical information to American forces. "There is just no way that you are going to gain information superiority or information dominance on the battlefield if you are already creating a self-denial-of-service [situation]," said Pericas. "We are going to stay connected throughout."

The system calls for declaring a state of alert—an Information Operations Condition or INFOCON—that can be raised or lowered based on intelligence warnings, before a network intrusion has been confirmed. These INFOCON levels range from Normal to Delta, the highest state of CND activities. Between them lie Alpha, Bravo, and Charlie levels.

The new guidelines clearly define the roles of the operational commanders in protecting the networks and go beyond merely recommending defensive measures and instead establish a baseline of action across DOD for each INFOCON level, Pericas said. They will help to codify how the US military will share networks and information with allies and coalition partners.

The command also recently conducted a headquarters-level, internal INFOCON exercise, called Ambitious Immortal, to assess the operational impact of carrying out the defensive measures prescribed for each INFOCON level. The exercise was a first step toward building a capability to conduct realistic CND exercises. It could serve as a model for a similar DOD–wide exercise, perhaps in 2002, SPACECOM officials said.

Command officials said they want to operationalize CND and CNA missions. For example, the Air Force earlier this year placed Air Intelligence Agency under authority of Air Combat Command, not only to merge intelligence gathering and information operations into combat operations but also to institutionalize information warfare as a legitimate weapon for combat.

One important step at DOD–wide level will be the inclusion in coming months of the CND and CNA missions in the Joint Monthly Readiness Reviews prepared by warfighting commands for the JCS Chairman. "It allows us to give [the Chairman] a report card on how well we are executing this mission," said Pericas.

Further, DOD is also establishing a Joint Computer Emergency Response Team Database to centrally track cyber-events, officials said.

Mutually Assured Crashes

Some day, network defense may well come to include the element of deterrence. DOD certainly has the wherewithal to stage retaliatory strikes at enemy computers. These offensive tools are among the Pentagon's most highly classified technologies, but the department is said to possess a potent array of so-called logic bombs, worms, and other cyber-war tools that can trigger malicious codes, reproduce themselves to cause networks to overload, and eavesdrop and steal data from a "foreign" network.

CNA operations touch on sensitive legal issues that still need to be resolved. US Space Command officials said the US side would have to carefully weigh a retaliatory counterstrike against a foreign government for an attack on DOD's networks. However, if the attacker is deemed to be a civilian, he would be considered a criminal under US law and therefore would become a problem for law enforcement officers. In addition, a US cyber-attack response against a foreign government to disable civilian infrastructure also raises thorny legal issues, according to officials. ■

Michael C. Sirak is a Washington, D.C.–based staff reporter with Jane's Defence Weekly, *an international defense magazine. This is his first article for* Air Force *Magazine.*