THE NEW ATLANTIS
A Journal of Technology & Society

Satellites at Risk

The Next Homeland Security Challenge May Be in Space

Even before the attacks of September 11, 2001, the growing threat of international terrorism prompted lawmakers to reevaluate the nation's approach to protecting its critical infrastructure. But a recent study by the General Accounting Office suggests that we have left one critical element of our communications infrastructure dangerously unprotected: our commercial satellites.

For most commercial purposes, the current basic security protections for satellites are adequate. But federal agencies frequently use commercial satellites, and at present

they must abide the low security standards even when using the satellites for national security purposes.

The GAO study, dated August 2002 but not widely published or reported until October, lists the potential threats facing satellites. Although hardened against the rigors of space—like radiation and debris—commercial satellites are still vulnerable to attacks from the ground, including "jamming" (blocking communication between a satellite and the ground) and "spoofing" (sending unauthorized signals to a satellite). These techniques can be used to disrupt a satellite's normal operations, to hijack a satellite, or even to destroy a satellite by sending false commands that could cause it to tumble from its orbit.

These are not just hypothetical threats. The study describes several incidents in which satellite services used for television, pagers, and GPS were hacked, jammed, or otherwise disrupted. And even when satellites aren't sabotaged, satellite traffic can be snooped on. The study reports that federal agencies like NASA and the FAA often don't encrypt satellite communications, both because of cost concerns and because the information being transmitted isn't sensitive. The military tends to use advanced encryption to protect its sensitive satellite communications, but sometimes there are slip-ups—as was the case in the summer of 2002, when it was revealed that live video streams from manned and unmanned surveillance planes in the Balkans were being transmitted unencrypted over a commercial satellite, readily accessible to anyone with regular satellite TV equipment.

Although the Pentagon emphasized that the video feed from the spy planes didn't compromise any critical information, that episode highlights the potential dangers of our military's reliance on vulnerable commercial satellites. The Department of Defense uses commercial satellites "to fulfill its communications and information transmission requirements for non-mission-critical data and to augment its military satellite capabilities," according to the GAO study. During the Desert Shield/Desert Storm conflict, commercial satellites carried 45 percent of all communications between the U.S. and the Persian Gulf region. Soon thereafter, during the operations in Somalia, there were no American satellites available to cover the region—neither military nor commercial—so Russian commercial satellites were used instead.

According to one Department of Defense official cited in the GAO study, the military's "reliance on commercial satellites is expected to grow through 2020." Despite that reliance, the military and all the other federal agencies that use satellites only constitute one-tenth of the commercial satellite market. As a result, commercial satellite companies have had little incentive to undertake the costly extra security measures that their private customers don't need. For instance, a government policy that went into effect in early 2001 requires the use of encryption technology on any commercial satellite transmitting national security information—but the GAO study says that "no commercial satellite is currently fully compliant" with the policy, since there is "no business case for voluntarily" following it and no mechanism for enforcing it.

Lurking in the wings is also an entirely new class of threat: space-based attacks on satellites. "Potential space-based weapons include interceptors, such as space mines and orbiting space-to-space missiles, and directed-energy weapons" like lasers. This may sound like science fiction, but it makes sense for potential enemies to seek new ways to exploit our growing dependence on

satellites. By crippling key satellites, enemies could disrupt commerce and civil society and vastly degrade our military capability.

This is why the Pentagon has paid increasing attention to defending our assets in space. Before becoming Secretary of Defense, Donald Rumsfeld served as chairman of the Commission to Assess United States National Security Space Management and Organization. According to that commission's report, issued in early 2001, the U.S. is "more dependent on space than any other nation," but we haven't made space defense a priority. Our assets in space make an "inviting target," the report said, and we are "an attractive candidate for a 'Space Pearl Harbor.'"

The commission made several suggestions related to bureaucratic reorganization, and it also recommended that the Department of Defense start to develop and deploy "systems in space to deter attack on and, if deterrence should fail, to defend U.S. interests on earth and in space." Many of the commission's recommendations are beginning to be implemented directly or reflected in Pentagon budget requests.