The Washington Post

Back to previous page

U.S. documents detail al-Qaeda's efforts to fight back against drones

By Craig Whitlock and Barton Gellman, Published: September 4

Al-Qaeda's leadership has assigned cells of engineers to find ways to shoot down, jam or remotely hijack U.S. drones, hoping to exploit the technological vulnerabilities of a weapons system that has inflicted huge losses upon the terrorist network, according to top-secret U.S. intelligence documents.

Although there is no evidence that al-Qaeda has forced a drone crash or interfered with flight operations, U.S. intelligence officials have closely tracked the group's persistent efforts to develop a counterdrone strategy since 2010, the documents show.

Al-Qaeda commanders are hoping a technological breakthrough can curb the U.S. drone campaign, which has killed an estimated 3,000 people over the past decade. The airstrikes have forced al-Qaeda operatives and other militants to take extreme measures to limit their movements in Pakistan, Afghanistan, Yemen, Somalia and other places. But the drone attacks have also taken a heavy toll on civilians, generating a bitter popular backlash against U.S. policies toward those countries.

Details of al-Qaeda's attempts to fight back against the drone campaign are contained in a classified intelligence report provided to The Washington Post by Edward Snowden, the fugitive former National Security Agency contractor. The top-secret report, titled "Threats to Unmanned Aerial Vehicles," is a summary of dozens of intelligence assessments posted by U.S. spy agencies since 2006.

U.S. intelligence analysts noted in their assessments that information about drone operational systems is available in the public realm. But The Post is withholding some detailed portions of the classified material that could shed light on specific weaknesses of certain aircraft.

Under President Obama and his predecessor, George W. Bush, drones have revolutionized warfare and become a pillar of the U.S. government's counterterrorism strategy, enabling the CIA and the military to track down enemies

in some of the remotest parts of the planet. Drone strikes have left al-Qaeda's core leadership in Pakistan scrambling to survive.

U.S. spy agencies have concluded that al-Qaeda faces "substantial" challenges in devising an effective way to attack drones, according to the top-secret report disclosed by Snowden. Still, U.S. officials and aviation experts acknowledge that unmanned aircraft have a weak spot: the satellite links and remote controls that enable pilots to fly them from thousands of miles away.

In July 2010, a U.S. spy agency intercepted electronic communications indicating that senior al-Qaeda leaders had distributed a "strategy guide" to operatives around the world advising them how "to anticipate and defeat" unmanned aircraft. The Defense Intelligence Agency (DIA) reported that al-Qaeda was sponsoring simultaneous research projects to develop jammers to interfere with GPS signals and infrared tags that drone operators rely on to pinpoint missile targets.

Other projects in the works included the development of observation balloons and small radio-controlled aircraft, or hobby planes, which insurgents apparently saw as having potential for monitoring the flight patterns of U.S. drones, according to the report.

Al-Qaeda cell leaders in the tribal areas of northwestern Pakistan were "determining the practical application of technologies being developed for battlefield applications," analysts from the DIA wrote. The analysts added that they believed al-Qaeda "cell leadership is tracking the progress of each project and can redirect components from one project to another."

The technological vulnerabilities of drones are no secret. The U.S. Air Force Scientific Advisory Board issued an unclassified report two years ago warning that "increasingly capable adversaries" in countries such as Afghanistan could threaten drone operations by inventing inexpensive countermeasures.

The board said insurgents might try to use "lasers and dazzlers" to render a drone ineffective by blinding its cameras and sensors. It also predicted that insurgents might use rudimentary acoustic receivers to detect drones and "simple jammer techniques" to interfere with navigation and communications.

Researchers have since proved that the threat is not just theoretical. Last year, a research team from the University of Texas at Austin demonstrated to the Department of Homeland Security that it was possible to commandeer a small civilian drone by "spoofing" its GPS signal with a ground transmitter and charting a different navigational course.

Trained engineers

Al-Qaeda has a long history of attracting trained engineers and others with a scientific background. Khalid Sheik Mohammed, the self-proclaimed architect of the Sept. 11, 2001, attacks, holds a mechanical-engineering degree and is such an inveterate tinkerer that the CIA allowed him to fiddle around with new designs for a vacuum cleaner after he was captured a decade ago.

In 2010, the CIA noted in a secret report that al-Qaeda was placing special emphasis on the recruitment of technicians and that "the skills most in demand" included expertise in drones and missile technology. In July of that year, Atiyah Abd al-Rahman, an al-Qaeda operations chief, told a jihadist Web site that the network did not need "ordinary fighters" and that it was looking instead for "specialist staff" to join the organization.

That same year, authorities in Turkey said they arrested an al-Qaeda member who was developing plans to shoot down small NATO surveillance drones in Afghanistan. The suspect, a 23-year-old mathematics student, was using software to conduct ballistics research for drone attacks, according to Turkish officials.

Al-Qaeda leaders have become increasingly open about their anti-drone efforts. In March, a new English-language online jihadist magazine called Azan published a story titled "The Drone Chain." The article derided drone armaments as "evil missiles designed by the devils of the world" but reassured readers that jihadists had been working on "various technologies" to hack, manipulate and destroy unmanned aircraft.

At the same time, the magazine indicated that those efforts needed a boost, and it issued an emergency plea for scientific help: "Any opinions, thoughts, ideas and practical implementations to defeat this drone technology must be communicated to us as early as possible because these would aid greatly . . . against the crusader-zionist enemy."

In the absence of a high-tech silver bullet, al-Qaeda affiliates around the world have taken to sharing hard-earned lessons about the importance of basic defensive measures.

Islamist extremists in North Africa this year distributed a photocopied tipsheet with 22 recommendations for avoiding drone strikes. Among the suggestions are several ideas for camouflage as well as dubious advice on using radio or microwave transmitters to "confuse the frequencies used to control the drone."

The Associated Press in February found a copy of the tipsheet in Mali, left behind by Islamist fighters fleeing the city of Timbuktu. It was written by a jihadist in Yemen two years earlier and has circulated among al-Qaeda franchises since then.

'GPS jamming capability'

In January 2011, U.S. intelligence agencies detected an unusual electronic signal emanating from near Miran Shah, a jihadist haven in North Waziristan, Pakistan. The DIA called the signal "the first observed test of a new terrorist GPS jamming capability."

The test apparently did not pose a threat to military GPS frequencies or encrypted communications links. In addition, whoever was beaming the mysterious signal mistakenly thought that jamming ground-based GPS receivers would interfere with drones' ability to aim missiles or munitions at fixed targets, according to the DIA report.

Despite such missteps, al-Qaeda has been undeterred. In a separate 2011 report, the DIA stated that affiliates in Miran Shah and the Pakistani city of Karachi were pursuing other "R&D projects," including one effort to shoot down drones with portable shoulder-fired missiles, known as manpads.

Army intelligence analysts uncovered similar projects, including attempts to develop laser detectors that could give warning whenever a U.S. Predator drone was about to fire a laser-guided Hellfire missile, according to a summary of a classified Army report.

In 2011, the DIA concluded that an "al-Qaeda-affiliated research and development cell currently lacks the technical knowledge to successfully integrate and deploy a counterdrone strike system." DIA analysts added, however, that if al-Qaeda engineers were to "overcome these substantial design challenges, we believe such a system probably would be highly disruptive for U.S. operations in Afghanistan and Pakistan."

The Air Force and CIA rely heavily on Predator and Reaper drones to hunt for al-Qaeda targets and other insurgents in several countries. Both aircraft can stay aloft for more than 20 hours to conduct surveillance missions and can be armed with Hellfire missiles.

The drones are flown by remote control via satellite data links, usually by pilots and sensor operators stationed thousands of miles away at bases in the United States. Those satellite links are encrypted, which makes the connections extremely difficult to hack.

It is only slightly less of a challenge for al-Qaeda fighters to spot a high-flying drone with the naked eye. Predators and Reapers loiter at altitudes above 20,000 feet, and their powerful cameras focus on objects several miles over the horizon, so their presence is hard to detect.

The satellite links, however, are the Achilles' heel of drone operations. "Lost link" incidents — triggered when a satellite moves out of range or a drone drops a signal — are relatively common. The connections are usually reestablished within seconds

or minutes. The aircraft are programmed to fly in a loop pattern or return to their launching spot during prolonged disruptions.

On several occasions, however, lost links have led to crashes. In September, an Air Force Predator slammed into mountainous terrain along the Iraq-Turkey border after the satellite data links were lost and the drone crew could no longer communicate with the aircraft.

In December 2011, a stealth U.S. spy drone operated by the CIA crashed in Iranian territory. Iran said it downed the advanced RQ-170 drone in an "electronic ambush." U.S. officials said they did not believe that the drone had been hacked or jammed. They said a technical malfunction was probably to blame.

Although the navigational satellite links are encrypted, other drone transmissions are sometimes left unprotected.

In 2009, the U.S. military discovered that Iraqi insurgents had hacked into video feeds from Predator and Shadow drones using off-the-shelf software. The drones had been transmitting full-motion video to U.S. troops on the ground, but the Air Force had not encrypted those data links, leaving them vulnerable.

Air Force officials acknowledged the flaw and said they would work to encrypt all video feeds from its fleet of Predator drones by 2014. In their classified assessments, U.S. intelligence agencies sought to play down the insurgents' hacking handiwork. Although analysts were concerned about the interceptions of the video feeds, they said there was no sign that insurgents had been able to seize control of the drone itself.

"While the ability of insurgent forces to view unencrypted or to break into encrypted data streams has been a concern for some time, indications to date are that insurgents have not been able to wrest [drone] control from its mission control ground station," a 2010 report concluded.

The report went on to suggest that allowing insurgents to intercept video feeds might actually have "a deterrent effect" by demonstrating the extent to which U.S. forces were able to watch their movements.

Growing unease

Still, summaries of the classified reports indicate a growing unease among U.S. agencies about al-Qaeda's determination to find a way to neutralize drones.

"Al-Qaida Engineers in Pakistan Continue Development of Laser-Warning Systems in Effort To Counter UAV Strikes," read the headline of one report in 2011, using the military acronym for unmanned aerial vehicles.

Beyond the threat that al-Qaeda might figure out how to hack or shoot down a drone, however, U.S. spy agencies worried that their drone campaign was becoming increasingly vulnerable to public opposition.

Intelligence analysts took careful note of al-Qaeda's efforts to portray drone strikes as cowardly or immoral, beginning in January 2011 with a report titled "Al-Qa'ida Explores Manipulating Public Opinion to Curb CT Pressure."

Analysts also questioned whether they were losing the rhetorical battle in the media, the courts and even among "citizens with legitimate social agendas." One 2010 report predicted that drone operations "could be brought under increased scrutiny, perceived to be illegitimate, openly resisted or undermined."

In response, intelligence agencies floated their own ideas to influence public perceptions. One unclassified report said the phrase "drone strike" should never be uttered, calling it "a loaded term."

"Drones connote mindless automatons with no capability for independent thought or action," the report said. "Strikes connote a first attack, which leaves the victim unable to respond. Other phrases employed to evoke an emotional response include 'Kill List,' 'Hit Squads,' 'Robot Warfare,' or 'Aerial Assassins.'"

Instead, the report advised referring to "lethal UAV operations." It also suggested "elevating the conversation" to more-abstract issues, such as the "Inherent Right of Self-Defense" and "Pre-emptive and Preventive Military Action."

Greg Miller contributed to this report.