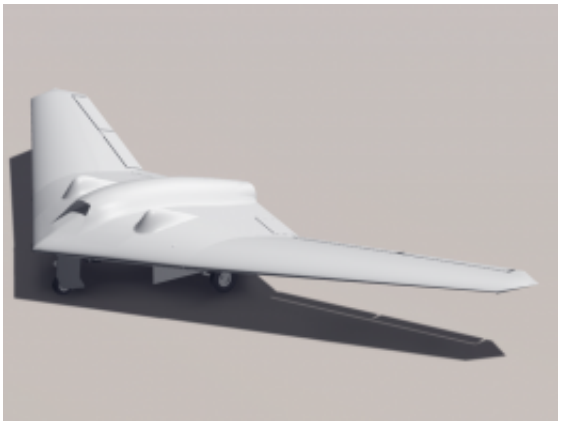
RQ-170 drone's ambush facts spilled by Iranian engineer

December 17 2011, by Nancy Owano



RQ-170 Sentinel. © TruthDowser / Wikimedia Commons / CC-BY-SA-3.0

(PhysOrg.com) -- In the aftermath of the Iran capture of a US military drone earlier this month now come arguments over how Iran managed to pull it off. An Iranian engineer's exclusive interview with *The Christian Science Monitor* has been published, which details how the Iranians captured the drone through jamming. An opposing camp says the story is just that, a story, while others schooled in GPS systems say that the Iranians' technique is technically possible but they would not bet on it.

Iran's story about the electronic ambush of America's sophisticated drone, the RQ-170 Sentinel, is that their experts used their technology savvy to trick the drone into landing where the drone thought was its actual base in Afghanistan but instead they made it land in Iran. They

used reverse engineering techniques that they had developed after exploring less sophisticated American drones captured or shot down in recent years. They were able to figure how to exploit a navigational weakness in the drone's system. "The GPS navigation is the weakest point," the Iranian engineer told the newspaper.

Iranian electronic warfare specialists were able to cut off the communications link by jamming on the communications. The engineer said that they forced the drone into autopilot. That state is where "the bird loses its brain." The Iranians reconfigured the drone's GPS coordinates and they used precise latitudinal and longitudinal data to force the drone to land on its own. In doing so the Iranian team did not have to bother about cracking remote control signals and communications from a control center in the U.S., and the RQ170 suffered only minimal damage, according to the report.

Adding strength and credibility to that story were military experts saying that even a combat-grade GPS system is vulnerable to manipulation. According to a GPS expert at the University of New Brunswick in Canada, Richard Langley, it's theoretically possible to take control of a drone by jamming.

GPS satellites transmit on two legacy radio frequencies. The unencrypted code used by most civilian GPS units is transmitted only on the L1 frequency. The encrypted P code for military users is transmitted on both the L1 and L2 frequency. If the Iranians could jam the encrypted military code on the L1 and L2 frequencies then the drone's GPS receiver might reach out to use the less secure code to get directions. Without encryption, it would be possible for an enemy to fool a drone into thinking it was elsewhere.

While possible in theory, other GPS experts say it is a difficult feat and they express doubt that the exploit happened.

Some analysts think another possibility is that the aircraft malfunctioned independent of any Iranian electronic interference. Further doubt is expressed not only over whether it was technologically possible for them to overtake the navigation system but also to bring it down with such minimal damage to it. John Pike, defense expert from GlobalSecurity.org, was quoted as saying he thought the drone exhibited by the Iranians looked like a parade float in that it was remarkably intact.