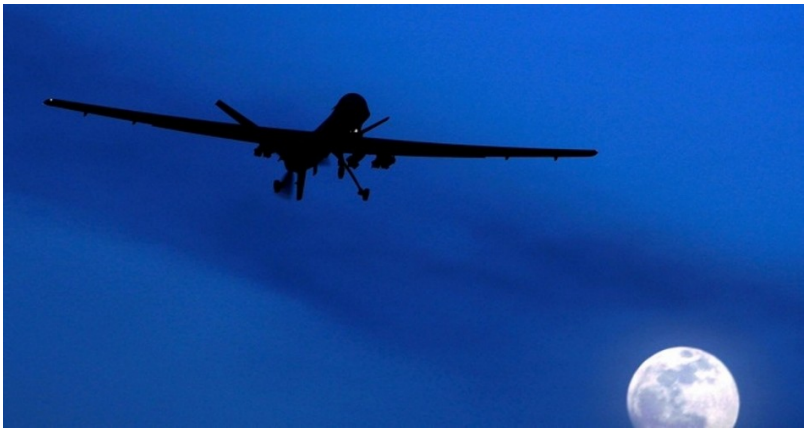
Written by **Joe Wolverton, II, J.D.** on November 1, 2012

$28 Device Makes Drone Video Feed Available to Anyone



Given the president's preference for using drones to deliver death to "suspected militants," it's reasonable to assume that the video captured by these remote control assassins is broadcast to the pilots over an *über*-secure frequency accessible only to those controlling the vehicle.

Not so much.

A story published October 29 by *Wired* magazine online reported:

> Four years after discovering that militants were tapping into drone video feeds, the U.S. military still hasn't secured the transmissions of more than half of its fleet of Predator and Reaper drones, Danger Room has learned. The majority of the aircraft still broadcast their classified video streams "in the clear" — without encryption. With a minimal amount of equipment and know-how, militants can see what America's drones see.

This is certainly disturbing news considering that first, the drone fleet is by far the most popular weapon in the "war on terror;" second, that the targets of the sorties should not be able to follow the weapons in flight using the very video feed monitored by pilots.

Imagine, for example, if a group of alleged al-Qaeda militants were able to access and avoid the flight plan of a Predator. This criminal cabal could then continue their activities without worrying about a surprise volley of Hellfire missiles lighting up their meeting place.

Michah Zenko, author of the drone war-monitoring blog, "Politics, Power, and Preventative Action," is quoted by Wired saying, "If somebody could obtain reliable access to real-time Predator or Reaper video — without attribution or alerting U.S. military — that would [be] a tremendous intel coup. There is an insatiable demand from Predator and Reaper imagery in Afghanistan and elsewhere. Any reluctance to use those for spying or missile strikes places operations in Afghanistan, Pakistan, Yemen, and Somalia at some risk."

How could the United States permit drone-obtained imagery to be so easily intercepted? There is no good answer coming from officialdom, but *Wired* writes that "military officials have known about — and mostly shrugged off — the vulnerability since the development of the Predator in the 1990s."

In 2008, the story recounts, video footage from U.S. drones was discovered on "Shi'ite militants'" computers recovered in Iraq. For a $26 piece of software, reportedly, a target becomes an observer.

A *Wall Street Journal* story from December 2009 reported the then-recent embarrassing discovery:

> Militants in Iraq have used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones, potentially providing them with information they need to evade or monitor U.S. military operations.
>
> Senior defense and intelligence officials said Iranian-backed insurgents intercepted the video feeds by taking advantage of an unprotected communications link in some of the remotely flown planes' systems. Shiite fighters in Iraq used software programs such as SkyGrabber — available for as little

> as $25.95 on the Internet — to regularly capture drone video feeds, according to a person familiar with reports on the matter.

The description of the SkyGrabber device provided on the company's website is eery, given the use to which the technology has been put:

> SkyGrabber is offline satellite internet downloader. It accepts free to air (FTA) satellite data (movie, music, pictures) by digital satellite TV tuner card (DVB-S/DVB-S2) and saves information onto a hard disk. So, you'll get new movie, best music and funny pictures for free.
>
> You don't have to keep an online internet connection. Just customize your digital satellite TV tuner card (DVB-S/DVB-S2) to satellite provider and start accepting free to air data. SkyGrabber has simple and attractive GUI, powerful filter system and flexible settings. If you want to have the newest legal software for free, SkyGrabber is your choice. SkyGrabber is a hobby for person who accepting free to air satellite data by digital satellite TV tuner card (DVB-S/DVB-S2) from satellite provider. SkyGrabber is for fun.

SkyGrabber is for fun? Not when you consider that those elements supposedly planning and perpetrating attacks on the United States can evade detection using this grabber of "funny pictures."

Of course, that *Wall Street Journal* story was published three years ago, and at the time a Defense Department official said that the downloads were "an issue that we can take care of and we're doing so" surely the Pentagon has patched the hole and tightened up the security and packaged the Predator video feed inside an impenetrable envelope of encryption.

Not so much.

Per the *Wired* article:

> Four years into the effort, however, only "30 to 50 percent" of America's Predators and Reapers are using fully encrypted transmissions, a source familiar with the retrofitting effort tells Danger Room. The total fleet won't see its communications secured until 2014. This source and others who work closely with drone operations say that drones flying overseas are among the first to get the newly secured equipment. They also noted that they are unaware of any incidents of militants using America's unmanned eyes in the sky to their advantage. "But I'm surprised I haven't," the source adds. "And that doesn't mean it's not happening."

That's not to say that the Pentagon provides no protection for its video transmission. According to the information published by *Wired*:

> Predators and the larger, better-armed Reapers transmit video and accept instructions in one of two ways. The first is via satellite, to remote pilots and sensor operators who are often on the other side of the planet; these satellite communications are encrypted, and are generally considered secure.
>
> The second is through a radio frequency signal called the Common Data Link, which is used to share the drone's video feed with troops on the ground. The CDL's carrier signal — its specific pattern of frequencies, in a given order and for a given length of time — tells both transmitter and receiver on how to function. The problem is that the Predators' version of the CDL carrier signal (also known as a "waveform") didn't include an order to encrypt the signal. So neither the transmitter on the drone nor the receivers that troops used on the ground employed encryption, either.

Common Data Link was designed in 1991 to be a secured military communications protocol. The Pentagon intended CDL to be the U.S. military's primary protocol for imagery and signals intelligence.

Turns out that a more robust encryption system would be too heavy for drone deployment, so the "Air Force made the conscious decision to leave off the crypto."

That was true of the original Predators, but the vehicle is now larger and more powerful and easily capable of carrying the bulkier encryption apparatus. The only obstacle remaining is the swapping out of older ground receivers (known as Rovers) with newer models programmed to interpret the more sophisticated scrambling of the video signal.

"The fleet-wide upgrade begins later this year and carries on for several years," says Major Mary Danner-Jones, an Air Force spokesperson in the *Wired* article. The Air Force is reportedly spending $12 million on the new equipment.

That's in addition to the $26 million paid to the General Atomics Aeronautical Systems, the maker of the Predator.

Since October 2010, General Atomics Aeronautical Systems has been awarded nearly $4 billion in contracts by the Department of Defense.

Regarding the future of the hackable drone fleet, *Wired* posits: "It's possible that none of the militants America is trying [to monitor] today are as sophisticated as the ones who intercepted that drone video in 2008. It's possible that the value of such footage-from-above is so fleeting that extremists have never again bothered to grab it."

Then again, perhaps neither the CIA nor the White House is worried about the prospect of Predator video being intercepted by "terrorists" because the point of the video feed is not to provide critical tactical data to troops on the ground, but to assist the pilot in carrying out the president's orders of execution. It's a fact that the condemned can't outrun the missile whether he can see it coming or not.