

# Insurgents Hack U.S. Drones

SIOBHAN GORMAN, YOCHI J. DREAZEN and AUGUST COLE

*Editor's Note: This is absurd. Why are they allowing any insecure links on a military RPV? Every single telemetry line, regardless of function, should have been encrypted from the very beginning. Why don't they apply some kind of encryption (as well as [TEMPEST](#)) [1] regulation to the area of military robots? The Predator's (and that of other aerial RPV's) ability to operate undetected from the ground is its greatest strength. Capturing its video feed removes the elements of stealth and surprise, literally emasculating the effort. Hopefully this will be taken as a learning experience by the military, and other potential chinks in our electronic armor. What if the insurgents could capture the video from wireless ground observation posts as well?*



WASHINGTON ([WSJ](#)) [2] -- 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.

U.S. officials say there is no evidence that militants were able to take control of the drones or otherwise interfere with their flights. Still, the intercepts could give America's enemies battlefield advantages by removing the element of surprise from certain missions and making it easier for insurgents to determine which roads and buildings are under U.S. surveillance.

The drone intercepts mark the emergence of a shadow cyber war within the U.S.-led conflicts overseas. They also point to a potentially serious vulnerability in Washington's growing network of unmanned drones, which have become the

## **Insurgents Hack U.S. Drones**

Published on Electronic Component News (<http://www.ecnmag.com>)

---

American weapon of choice in both Afghanistan and Pakistan.

The stolen video feeds also indicate that U.S. adversaries continue to find simple ways of counteracting sophisticated American military technologies.

U.S. military personnel in Iraq discovered the problem late last year when they apprehended a Shiite militant whose laptop contained files of intercepted drone video feeds. In July, the U.S. military found pirated drone video feeds on other militant laptops, leading some officials to conclude that militant groups trained and funded by Iran were regularly intercepting feeds.

In the summer 2009 incident, the military found "days and days and hours and hours of proof" that the feeds were being intercepted and shared with multiple extremist groups, the person said. "It is part of their kit now."

[Click Here](#) [3] for the rest of the article.

**Source URL (retrieved on 11/25/2014 - 3:57pm):**

<http://www.ecnmag.com/news/2009/12/insurgents-hack-us-drones>

### **Links:**

[1] <http://en.wikipedia.org/wiki/TEMPEST>

[2] <http://online.wsj.com/>

[3] [http://online.wsj.com/article/SB126102247889095011.html?mod=WSJ\\_hpp\\_MID\\_DLETopStories](http://online.wsj.com/article/SB126102247889095011.html?mod=WSJ_hpp_MID_DLETopStories)