GlobalResearch
Center for Research on Globalization

Hackable Drones, Crumbling Empire

By Tom Burghardt
Global Research, January 01, 2010
Antifascist Calling... 1 January 2010
Theme: US NATO War Agenda

On the eve of the 2003 American invasion of Iraq, historian Chalmers Johnson observed in *The Sorrows of Empire*: "At this late date … it is difficult to imagine how Congress, much like the Roman senate in the last days of the republic, could be brought back to life and cleansed of its endemic corruption."

Drawing striking analogies between the fall of the Roman republic and America's decline as a global capitalist power, Johnson wrote: "Failing such a reform, Nemesis, the goddess of retribution and vengeance, the punisher of pride and hubris, waits impatiently for her meeting with us."

Judging by the fragile state of American sociopolitical life, that meeting may not be as far off as most of us think.

America's Hackable Drones

In this light, it was hardly surprising to read in ***The Wall Street Journal*** last week that "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."

The *Journal* revealed that the Pentagon's "potential drone vulnerability lies in an unencrypted downlink between the unmanned craft and ground control." Investigative journalists Siobhan Gorman, Yochi Dreazen and August Cole disclosed that the "U.S. government has known about the flaw since the U.S. campaign in Bosnia in the 1990s."

But since feeding the corporatist beast, in this case **General Atomics Inc.**, is priority number one for **grifters** in Congress, the problem was allowed to fester until the boil finally popped.

Considering that the Obama administration "has come to rely heavily on the unmanned drones" for imperial machinations across the entire Eurasian "Arc of Crisis" or any number of other "theaters" where the U.S. military and the corporate masters they serve, steal other people's resources (known as "Keeping America Safe" in our debased political lexicon), this news will probably come as quite a shock.

After all, we've been to led to believe that the *heimat's* occupying armies, like ancient Roman legionnaires, are "invincible."

But as the *Journal* reported "the stolen video feeds also indicate that U.S. adversaries continue to find *simple ways* of counteracting sophisticated American military technologies." (emphasis added)

Contemplate and savor that phrase, dear readers. While wags in the Pentagon Borg hive may believe "resistance is futile," insurgent hackers using off-the-shelf software and cheap, easy to rig antennas were able to determine, in real-time no less, tactical information transmitted to U.S. troops on the ground. As the *Journal* noted, unencrypted video feeds from drones in Afghanistan and Pakistan also "appear to have been compromised."

Another surveillance drone deployed both in Iraq and Afghanistan, the ScanEagle manufactured by Boeing subsidiary **Insitu**, is plagued by similar problems.

In a follow-up piece, the *Journal* **reported** that the ScanEagle "can stay aloft for 24 hours and carries electro-optical and infrared cameras up to an altitude of 16,000 feet."

But as with the Predator and Reaper attack drones, the ScanEagle's "video feed hasn't been encrypted," primarily "because military officials have long assumed no one would make the effort to try to intercept it."

An Insitu spokesperson told the *Journal* that the firm was in the "advanced stages of development of a technical solution for video data encryption for ScanEagle."

Writing in *Wired For War*, analyst P.W. Singer describes the "next generation of the Predator," the MQ-9 Reaper as "four times bigger and nine times more powerful" than its predecessor. Claiming that the attack drone comes "close to flying itself," Singer touts the ability of the aircraft to "recognize and categorize human and human-made objects. It can even make sense of the changes in the target it is watching, such as being able to interpret and retrace footprints or even lawn mover tracks."

"As of 2008," Singer informs us, "two Reaper prototypes were already deployed to Afghanistan" and we can presume Pakistan as well. Investigative journalist Jeremy Scahill revealed last month in ***The Nation*** that the mercenary firm Blackwater is working on the CIA and Joint Special Operations Command's "drone bombing program in Pakistan."

According to Scahill's military intelligence source, while CIA operations are subject to congressional oversight, "parallel JSOC bombing are not." The source told Scahill, "Contractors and especially JSOC personnel working under a classified mandate are not [overseen by Congress], so they just don't care. If there's one person they're going after and there's thirty-four people in the building, thirty-five people are going to die. That's the mentality."

What other "mentality" is operative here, particularly amongst journalists wowed by the technology but indifferent to the death and destruction they inflict on defenseless civilians? *Aviation Week's* Bill Sweetman told Singer when queried about Reaper deployments in the "Afpak" theater: "It may not be unreasonable to assume they are standing alert somewhere in case a certain high-priority target pops his head out of his cave."

Leaving aside Sweetman's dubious stab at humor, in light of last week's revelations one must ask, why bother to pop your head out of a cave, when a small, commercially-available satellite dish and a cheap laptop will do the trick? But what make these reports so telling is that "the Pentagon assumed local adversaries wouldn't know how to exploit it." Where have we heard *that* before? Dien Bien Phu? The Bay of Pigs? The "cakewalk" In Iraq, perhaps?

While history doesn't repeat, although tragedies and farces abound, the Joint Chiefs of Staff, and the giant defense firms who line their pockets upon retirement, as *USA Today* **revealed**

last month, mix their whiskeys with net-centric kool-aid, and have staked their careers (and the lives of their economic conscripts and the victims of these indiscriminate drone attacks) on quixotic, dubious theories of robowar.

But with a U.S. Defense Department budget that tops $685 billion for fiscal year 2010, and considering that drones will account for a whopping 36% of the Air Force's acquisition budget, why would Pentagon policy planners assume otherwise? After all, how could a motley crew of shepherds, day laborers and "Saddam dead-enders" outfox America's mighty imperial army? How, indeed!

According to ***Air Force Times***, although the Pentagon knew that UAV feeds were being hacked since 2008 and probably earlier, top Air Force generals, acceding to the wishes of their political masters in the Defense Department, notably former Secretary of Defense Donald Rumsfeld and his coterie of neocon yes-men, did nothing to upset the high-tech apple cart and sought instead to hit the corporate "sweet spot."

Former Air Force Secretary Michael Wynne was fired in 2008 when it was revealed that a B-52 Stratofortress bomber flew some 1,500 miles from Minot Air Force base in North Dakota to Barksdale Air Force base in Louisiana with nuclear-tipped cruise missiles fixed to its wings. Compounding the scandal, for nearly six hours the Air Force was unable to account for the weapons. Commenting on the hacked UAV drone feeds, *Air Force Times* disclosed:

Wynne took part in meetings with the Office of the Secretary of Defense in 2004 and 2005 about concerns with the links, but the consensus from the meetings was to field the UAVs as quickly as possible.

"I would say people were aware of it [the vulnerability], but it wasn't disturbing," Wynne said. "It wasn't yet dangerous; it certainly didn't disrupt an operation, so why make a huge deal of it?" (Michael Hoffman, John Reed and Joe Gould, "Fixes on the Way for Nonsecure UAV Links," *Air Force Times*, December 20, 2009)

Meanwhile, former Air Force Chief of Staff General T. Michael Moseley, fired along with Wynne over the loose nuke incident, attended the same DoD conclave with his boss and *capo tutti capo* Rumsfeld. Moseley told the publication "his worry" was "about the security of the aircraft's datalinks."

"My question from the beginning was … 'What is our confidence level that links are secure?' Not just the imaging that comes off, but also the command and flying links. The answer was 'We're working that' from the General Atomics folks," Moseley said.

San Diego-based General Atomics Inc., No. 36 on ***Washington Technology's*** "2009 Top 100 List of Prime Federal Contractors" is plush with revenue totaling $593,742,395. Major customers include the Navy, Air Force, Army, the Department of Homeland Security and NASA, and the bulk of their business these days comes from manufacturing the MQ-1 Predator and MQ-9 Reaper drones.

When queried by *Journal* reporters about the UAV's vulnerabilities, a company spokeswoman told the journalists that for "security reasons," the firm couldn't comment on "specific data link capabilities and limitations."

Could their lack of transparency have something to do perhaps with the fact that the Air Force plans to buy some 375 Reaper drones at a cost of some $10-12 million each? I guess they're "working that" too!

Other Systems Vulnerable

But the problem is worse, far worse than the Pentagon has acknowledged. *Wired* **reported** that "tapping into drones' video feeds was just the start."

Investigative journalists Noah Shachtman and Nathan Hodge disclosed that the "U.S. military's primary system for bringing overhead surveillance down to soldiers and Marines on the ground is also vulnerable to electronic interception, multiple military sources tell Danger Room." According to *Wired*, this means "militants have the ability to see through the eyes of all kinds of combat aircraft–from traditional fighters and bombers to unmanned spy planes."

The military initially developed the Remotely Operated Video Enhanced Receiver, or ROVER, in 2002. The idea was let troops on the ground download footage from Predator drones and AC-130 gunships as it was being taken. Since then, nearly every airplane in the American fleet–from F-16 and F/A-18 fighters to A-10 attack planes to Harrier jump jets to B-1B bombers has been outfitted with equipment that lets them transmit to ROVERs. Thousands of ROVER terminals have been distributed to troops in Afghanistan and Iraq.

But those early units were "fielded so fast that it was done with an unencrypted signal. It could be both intercepted (e.g. hacked into) and jammed," e-mails an Air Force officer with knowledge of the program. In a presentation last month before a conference of the Army Aviation Association of America, a military official noted that the current ROVER terminal "receives only unencrypted L, C, S, Ku [satellite] bands." (Noah Shachtman and Nathan Hodge, "Not Just Drones: Militants Can Snoop on Most U.S. Warplanes," *Wired*, December 17, 2009)

The Pentagon discovered this "problem" late last year when a Shiite militant's laptop "contained files of intercepted drone video feeds."

And last summer, unnamed "senior officials" told the *Journal* that the military found "days and days and hours and hours of proof" that video feeds from Predator drones, but also from other U.S. systems, including attack aircraft, were vulnerable to interception.

In a follow-up **piece** December 21, Shachtman reported that Air Force officers initially claimed the video intercepts "were no big deal." Why? Because "without the metadata to go along with, the footage was extremely hard to interpret."

"Well," Shachtman writes, "now it turns out that intercepting the metadata isn't much harder than tapping the video itself. Because 'there is also mission control data carried inside the satellite signal to the ground control stations,' according to an analysis carried by **Wikileaks**."

The Wikileaks document avers: "It is theoretically possible to read off this mission control data both in the intercepted video feed and saved video data on harddisks." This means that the "control and command link to communicate from a control station to the drone" and the "data link that sends mission control data and video feeds back to the ground control station," for both "line-of-sight communication paths and beyond line-of- sight

communication paths" are hackable by whomever might be listening.

Indeed, "line-of-sight links are critical for takeoffs and landings of the drone. These links utilize a C-Band communication path." We are told that "beyond line-of-sight communication links operate in the Ku-Band satellite frequency. This allows the UAV to cover approx. 1500 miles of communication capability."

"So this explains somewhat" the analyst continues, "why the insurgents were able to intercept the Predator video feeds when they were sent unencrypted to the ground station." Therefore, "the only thing needed" by a savvy technoguerrilla "is a C-Band or Ku-Band antenna which can read traffic. Sending traffic to a satellite for example is not needed in this case."

"An important note," and what make Pentagon planners' assumptions about their adversaries all the more ludicrous "is that our research shows that most if not all metadata inside the MPEG Stream is for its own not encrypted if the MPEG Stream itself is not encrypted."

In other words *Wired* concludes, "everything, from target locations to drone headings to sensor angles can be pulled off of the satellite transmission, too." Shachtman writes, "the more this security breach is examined, the bigger it becomes."

And considering that an "unnamed senior official" told *Journal* reporters that the simple software package is "part of their kit now," is it only a matter of time before militant groups figure out how to hijack a drone and crash it, or even launch a Hellfire missile or two at a U.S. ground station?

We are told by military experts this is not possible; however, who would have thought that the Achilles heel of Pentagon robo warriors, blinded by their own arrogance and racist presumptions about the "Arab Mind" was something as simple as their own hubris.

The neocon ***Middle East Quarterly*** assures us that "Arab resentment of the West … particularly in terms of the technology invasion" is "at every level," according to the absurdist meme of Raphael Patai, author of *The Arab Mind*, "a daily reminder of the inability of the Middle East to compete."

Claiming that the "Arab view of technology" reflects an inherent "cultural weakness" that "has been amply supported over the last decades," we are told that "Arabs" while "clearly enthusiastic users of technology, particularly in war weaponry … nevertheless remain a lagging producer of technology."

Indeed, Patai's book is *assigned reading* at the John F. Kennedy Special Warfare School. Col. Norvell B. De Atkine, an instructor in Middle East studies, informs us that in order "to begin a process of understanding the seemingly irrational hatred that motivated the World Trade Center attackers, one must understand the social and cultural environment in which they lived and the modal personality traits that make them susceptible to engaging in terrorist actions."

Col. De Atkine avers "at the institution where I teach military officers, *The Arab Mind* forms the basis of my cultural instruction."

Judging by the coverage in corporate media, endlessly repeating similar imperial tropes, this

hilarious security breach, one I might add of the Pentagon's *own creation*, has come as quite a shock. It shouldn't have. After all, the same "hajis" who were able to grind the American military machine to a halt by their imaginative use of decades' old ordnance, garage door openers (!) and cell phones fabricated into IEDs have created a "Revolution in Military Affairs" (**RMA**) of their own.

Talk about unintended consequences!

Net-Centric Warfare, Meet the Countermeasures!

Dr. Andrew Marshall, the Director of the Defense Department's Office of Net Assessment, defines RMA as "a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations."

But as Durham University professor of geography Stephen Graham points out, in light of the Iraq debacle, RMA theorists sought to get a handle on complex urban geographies to attain what they believed would be "Persistent Area Dominance" through the use of satellites, drones and an array of sensors "networked" onto the battlefield. Graham writes:

The first involves programmes designed to saturate such cities with myriads of networked surveillance systems. …

This leads neatly to the second main area of defence research and development to help assert the dominance of US forces over global south cities: a shift towards robotic air and ground weapons. When linked to the persistent surveillance and target identification systems … these weapons will be deployed to continually and automatically destroy purported targets in potentially endless streams of state killing. Here, crucially, fantasies of military omniscience and omnipotence, which blur seamlessly into wider sci-fi and cyberpunk imaginations of future military technoscience, become indistinguishable from major US military research and development programmes. The fantasies of linking sentient, automated and omnipotent surveillance–which bring God-like levels of 'situational awareness' to US forces attempting to control intrinsically devious global south megacities–to automated machines of killing, pervades the discourses of the urban turn in the RMA. (Stephen Graham, "Surveillance, urbanization, and the 'Revolution in Military Affairs'," in David Lyon (ed) *Theorizing Surveillance: The Panopticon and Beyond*, London: Willan, 2006, pp. 251, 254-255)

But what happens when global resistance forces get a handle on the game America and their allies are playing and begin leveraging the weaknesses of such systems, not of least of which are the ideological blind spots plaguing their developers, into a wholly subversive high-tech détournement in a bid to level the playing field?

This is no idle speculation, but rather a possible glimpse into the future of what has been called by military theorists "asymmetric warfare." The classic examples of this type of uneven combat between states and insurgent forces are the various communist guerrilla armies that toppled colonial or neocolonial governments backed by the United States, e.g. China, Vietnam, Cuba, Angola, Zimbabwe, Nicaragua.

Today however, the same "persistent surveillance and target identification systems" that

have seemingly given the U.S. military an edge over their adversaries, e.g. the development of robotic killing machines capable of "compressing the kill chain" as ***Airforce Magazine*** describes the process in near pornographic terms fail to mention that "in Iraq," as Stephen Graham reminds us, "even rudimentary high-tech devices have routinely failed due to technical malfunctions or extreme operating conditions."

As a result of Pentagon-sponsored research, contemporary military operations aim for "defined effects" through "kinetic" and "non-kinetic" means: leadership decapitation through preemptive strikes combined with psychological operations designed to pacify (terrorize) insurgent populations. This deadly combination of high- and low tech tactics is the dark heart of the Pentagon's **Unconventional Warfare** doctrine.

But as Graham points out, the "often wild and fantastical discourses" of high-tech military theorists have run into a brick, not a silicon, wall: the will to resist. Graham writes: "The relatively high casualty rates of US forces–forced to come down from 40,000 ft, or withdraw from ceramic armour, to attempt to control and 'pacify' violent insurgencies within sprawling Iraqi cities–are a testament to the dangerous wishful thinking that pervades all military fantasies of 'clean', 'automated' or 'cyborganized' urban 'battlespace'."

Nevertheless, such fantasies persist and will continue to drive military spending and American strategies of conquest even as imperialism's political project goes to ground.

And so we return to Chalmers Johnson's warning. "We are on the cusp of losing our democracy" Johnson laments, "for the sake of keeping our empire."

"Once a nation is started down that path" the historian cautions, "the dynamics that apply to all empires come into play–isolation, overstretch, the uniting of forces opposed to imperialism, and bankruptcy.

Barring a dramatic transformation of American economic, political and social relations, not the ersatz "change" promised by the current regime, a rank mendacity that amounts to little more than a band-aid over gangrene, "Nemesis stalks our life as a free nation."

Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and ***Global Research****, his articles can be read on* ***Dissident Voice****,* ***The Intelligence Daily****,* ***Pacific Free Press****,* ***Uncommon Thought Journal****,* ***Information Clearing House*** *and the whistleblowing website* ***Wikileaks****. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by* ***AK Press****.*

Articles by: Tom Burghardt

http://antifascist-calling.blogspot.com/