GlobalResearch
Center for Research on Globalization

IRAN-DRONEGATE: Empires Don't Apologize: Iran in the Imperial Crosshairs

By Tom Burghardt
Global Research, December 18, 2011
Antifascist Calling... 18 December 2011

Region: Middle East & North Africa, USA
Theme: Militarization and WMD, US NATO War Agenda
In-depth Report: IRAN: THE NEXT WAR?

After first denying that the Iranian military had captured the CIA's RQ-170 Sentinel spy drone, and then reluctantly acknowledging the fact only after PressTV aired footage of the killer bot, the Associated Press reported that "the Obama administration said Monday it has delivered a formal request to Iran" that they return it.

"We have asked for it back," Obama said. "We'll see how the Iranians respond."

A huge embarrassment to the CIA and the Pentagon, U.S. Secretary of State Hillary Clinton told reporters during a State Department briefing: "We submitted a formal request for the return of our lost equipment as we would in any situation to any government around the world."

Cheekily, Clinton said although the U.S. government has little prospect of getting their $6 million toy back because of "recent Iranian behavior," she then threatened the Islamic Republic saying, "the path that Iran seems to be going down is a dangerous one for themselves and the region."

In Washington's bizarro world where war is peace the United States, which has Iran surrounded with a string of military bases and where nuclear-armed aircraft carrier battle groups and submarines ply the waters of the Mediterranean and the Persian Gulf, the aggressor is magically transformed into the aggrieved party.

The Secretary said, "given Iran's behavior to date we do not expect them to comply but *we are dealing with all of these provocations and concerning actions taken by Iran* in close concert with our closest allies and partners." (emphasis added)

Talk about chutzpah!

Firing back, the head of Iran's Judiciary, Ayatollah Sadeq Amoli Larijani told *PressTV* that "the US has violated our country's territory and has waged an intelligence war, and now expects us to return the aircraft."

Noting the absurdity of U.S. demands Larijani said, "Iran has the right to deal with this blatant crime in any way [it deems necessary] and the US should forget about getting the spy aircraft back."

By all accounts, the "intelligence war" is heating heating up. On Thursday, *Haaretz* reported that the "Israel Defense Forces is forming a command to supervise 'depth' operations,

actions undertaken by the military far from Israel's borders."

In a follow-up piece published Sunday, *Haaretz* informed us that the new corps, "has already earned the somewhat overstated sobriquet 'the Iran Command'."

The newspaper's chief military correspondent, Amos Harel, wrote that the new unit "could, in the future, assist in mobilizing special forces in the Iranian context."

"More important," Harel averred, "it will have the job of planning and leading operations in areas far beyond the borders, operations that are connected to the covert war against terror organizations (and, indirectly, against Iran)."

Whether the IDF's newly-launched "Iran Command," will prove any more effective than the CIA or Mossad, which suffered major set-backs when their intelligence nets were rolled-up in Iran and Lebanon as *Asia Times Online* recently reported, is an open question.

War "by other means" however, will continue.

On Wednesday, the U.S. House of Representatives passed by a vote of 283-136 the Iran Threat Reductions Act (H.R. 1905), a draconian piece of legislative detritus which hopes to crater Iran's Central Bank.

The following day, the U.S. Senate followed suit, approving the legislation by an 86-13 vote. President Obama has said he would sign the bill, cobbled-together by war hawks as part of the massive $670 billion 2012 Defense Authorization Act.

Spinning the Story

U.S. military and CIA operations today involve far more than simply "putting steel on the target." Increasingly, covert actions and clandestine operations rely on what the Pentagon has described as "information operations."

With few exceptions, corporate media in Europe and the U.S. have played accessory roles in ginning-up the so-called "Iranian threat," a decades' long program to secure hegemony over the energy-rich regions of Central Asia and the Middle East.

When initial reports surfaced that the drone had gone missing deep inside Iran, "CIA press officials declined to comment on the downed drone and reporters were directed toward a statement from the military," *The Washington Post* reported.

Indeed, the International Security Assistance Force (ISAF), the NATO-led alliance currently occupying Afghanistan, dismissed Iran's claims that the drone was operating over their territory. "The UAV to which the Iranians are referring may be a U.S. unarmed reconnaissance aircraft that had been flying a mission over western Afghanistan late last week," the ISAF statement read.

Deep inside the media echo chamber, CNN informed us earlier this month that the drone had been "tasked to fly over western Afghanistan and look for insurgent activity, with no directive to either fly into Iran or spy on Iran from Afghan airspace."

"A U.S. satellite quickly pinpointed the downed drone, which apparently sustained significant damage," the "senior official" told the network.

CNN quoted the unnamed "senior official" as saying, "the Iranians have a pile of rubble and are trying to figure what they have and what to do with it." According to this reading, "the drone crashed solely because its guidance system failed, the official said."

While first claiming that the CIA drone had strayed off-course, CNN reported *after* the Sentinel was publicly displayed, that unnamed "U.S. military officials" re-calibrated their tale and now said that the drone "was on a surveillance mission of suspected nuclear sites" in Iran.

Anonymous officials told CNN that "the CIA had not informed the Defense Department of the drone's mission when reports first emerged that it had crashed," and that the U.S. military "'did not have a good understanding of what was going on because it was a CIA mission'."

As with their earlier reporting, CNN's latest explanation was a fabrication.

The *Los Angeles Times* reported two days after the incident, "though the drone flight was a CIA operation, U.S. military personnel were involved in flying the aircraft, said the official, who spoke on condition of anonymity because of the secrecy involved."

In fact, as *The Washington Post* disclosed in September, the CIA and the Pentagon's Joint Special Operations Command (JSOC) are thick as thieves.

"Their commingling at remote bases is so complete, the *Post* informed us, "that U.S. officials ranging from congressional staffers to high-ranking CIA officers said they often find it difficult to distinguish agency from military personnel."

"'You couldn't tell the difference between CIA officers, Special Forces guys and contractors'," an unnamed "senior U.S. official" told the *Post*. "'They're all three blended together. All under the command of the CIA."

"Their activities occupy an expanding netherworld between intelligence and military operations." One can presume that these "blended" units have been tasked by Washington with the "Iranian brief."

"Sometimes their missions are considered military 'preparation of the battlefield'," the *Post* reported, "and others fall under covert findings obtained by the CIA. As a result, congressional intelligence and armed services committees rarely get a comprehensive view," which of course is precisely what the Agency and Pentagon fully intend.

In light of recent statements by U.S. Defense Secretary Leon Panetta to *The New York Times*, that "surveillance flights *over Iran* would continue despite the loss of the drone," reporting by U.S. media stenographers, are blatant misrepresentations of the basic facts surrounding the entire affair. (emphasis added)

Now sensing the jig was up and that a face-saving meme had to be injected into the news cycle, a "former intelligence official" continued to discount Iranian assertions that their armed forces had brought the drone down.

"It simply fell into their laps," he told CNN.

However, much to the consternation of American officials, Iranian spin doctors were running

their own info op, one which cast U.S. claims in a most unflattering light.

The *Associated Press* reported that "Iran deliberately delayed its announcement that it had captured an American surveillance drone to test U.S. reaction, the country's foreign minister said Saturday."

"Ali Akbar Salehi said Tehran finally went public with its possession of the RQ-170 Sentinel stealth drone to disprove contradictory statements from U.S. officials," AP reported.

"When our armed forces nicely brought down the stealth American surveillance drone, we didn't announce it for several days to see what the other party (U.S.) says and to test their reaction," Salehi told the official IRNA news agency. "Days after Americans made contradictory statements, our friends at the armed forces put this drone on display."

Unlike American and Israeli assertions that Iran is taking steps to "go nuclear," Iranian officials at least had hard evidence on their side that the United States was violating their territorial integrity–the captured U.S. drone.

Electronic Countermeasures

Although Western "defense experts" have ridiculed claims that Iran's electronic warfare specialists have captured the Sentinel rather than recovering the downed craft from a crash site, a report by *The Christian Science Monitor* shed new light on Iran's apparent capabilities.

Investigative journalists Scott Peterson and Payam Faramarzi disclosed that an Iranian engineer now working on the captured drone, said that the military "exploited a known vulnerability and tricked the US drone into landing in Iran."

According to the *Monitor*, "Iran guided the CIA's 'lost' stealth drone to an intact landing inside hostile territory by exploiting a navigational weakness long-known to the US military."

Earlier reports suggested that Iran, which had recently been supplied with the Russian-built Kvant 1L222 Avtobaza Electronic Intelligence (ELINT) systems, may have been a factor in the drone's capture.

The Israeli defense industry publication, *Defense Update*, informed us that the Avtobaza is "capable of intercepting weapon datalink communications operating on similar wavebands. The new gear may have helped the Iranians employ active deception/jamming to intercept and 'hijack' the Sentinel's control link."

The *Monitor* investigation however, suggests that the Iranians had accomplished this feat on their own.

Regardless of the means employed, statements by U.S. officials that all the Iranians had was "a pile of rubble" were blatant falsehoods.

According to the *Monitor*, Iran's military experts were able to do so by cutting off "communications links of the American bat-wing RQ-170 Sentinel, says the engineer, who works for one of many Iranian military and civilian teams currently trying to unravel the drone's stealth and intelligence secrets, and who could not be named for his safety."

Armed with knowledge "gleaned from previous downed American drones and a technique proudly claimed by Iranian commanders in September, Peterson and Faramarzi disclosed that "the Iranian specialists then reconfigured the drone's GPS coordinates to make it land in Iran at what the drone thought was its actual home base in Afghanistan."

It would seem then, if this account is accurate, that Iranian defense experts had already "figure[d] out what they have and what to do with it" from earlier captures.

"The GPS navigation is the weakest point," the Iranian engineer said. "By putting noise [jamming] on the communications, you force the bird into autopilot. This is where the bird loses its brain."

Once military engineers had "spoofed" the American drone, "which took into account precise landing altitudes, as well as latitudinal and longitudinal data," they were able to make "the drone 'land on its own where we wanted it to, without having to crack the remote-control signals and communications' from the US control center."

Peterson and Faramarzi reported that the techniques employed "were developed from reverse-engineering several less sophisticated American drones captured or shot down in recent years," as well as by taking advantage "of weak, easily manipulated GPS signals, which calculate location and speed from multiple satellites."

Former U.S. Navy electronic warfare specialist Robert Densmore told the *Monitor* that "'modern combat-grade GPS [is] very susceptible' to manipulation," saying it is "certainly possible" to "'recalibrate the GPS on a drone so that it flies on a different course'."

As *Antifascist Calling* reported in 2009, Iraqi insurgents battling the U.S. occupation had deployed $26 off-the-shelf spy kit which enabled them to intercept live video feeds from Predator drones.

What the Iranians claim to have done, according to defense experts, are orders of magnitude greater than simply capturing a video feed. Indeed, if this report is credible, it would have wide-reaching implications for other U.S., Israeli and NATO aircraft and missiles which similarly rely on GPS to guide them towards their targets.

Why is this the case? As WikiLeaks revealed in a 2009 report on the earlier Iraqi revelations that "it is theoretically possible to read off this [drone] mission control data both in the intercepted video feed and saved video data on harddisks."

In plain English, 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.

Leaked Pentagon Document

On December 13, the secret-shredding web site Public Intelligence, published a leaked U.S. Air Force document, *USAF Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare*, SAB-TR-10-03, dated April 2011.

Classified "For Official Use Only," the 110-page report issued by the United States Air Force Scientific Advisory Board (SAB), revealed that drones or "remotely piloted aircraft" (RPA) are

subject to a number of vulnerabilities.

Air Force analysts averred that “in spite of current low RPA losses, inexpensive physical threats (e.g., MANPADS, low-end SAMs, air-to-air missiles) and electronic threats (e.g., acoustic detectors, low cost acquisition radars, jammers) threaten future operations.”

Relevantly, “sensor/data downlinks for some RPAs have not been encrypted or obfuscated.”

However, the RQ-170 Sentinel, which can operate at 50,000 feet would not have been vulnerable to “MANPADS” or “low-end SAMs,” and was certainly not brought down by an Iranian air-to-air missile; therefore, a valid explanation of its capture would be the one offered by Iran: electronic countermeasures developed by the Islamic Republic.

Amongst the more salient findings of the Air Force report are the following:

Section 2.4.3 Threat to Communication Links

1. Jamming of commercial satellite communications (SATCOM) links is a widely available technology. It can provide an effective tool for adversaries against data links or as a way for command and control (C2) denial.

2. Operational needs may require the use of unencrypted data links to provide broadcast services to ground troops without security clearances. Eavesdropping on these links is a known exploit that is available to adversaries for extremely low cost.

3. Spoofing or hijacking links can lead to damaging missions, or even to platform loss.

Section 2.4.4 Threat to Position, Navigation, and Guidance

1. Small, simple GPS noise jammers can be easily constructed and employed by an unsophisticated adversary and would be effective over a limited RPA operating area.

2. GPS repeaters are also available for corrupting navigation capabilities of RPAs.

3. Cyber threats represent a major challenge for future RPA operations. Cyber attacks can affect both on-board and ground systems, and exploits may range from asymmetric CNO [computer network operation] attacks to highly sophisticated electronic systems and software attacks.

Jeffrey Carr, a U.S. cybersecurity expert who maintains the Digital Dao web site wrote that the timing of document’s release to Public Intelligence was “very interesting.”

“Clearly,” Carr wrote, “someone with FOUO access wanted this information to be made public to inform the controversy surrounding the incident.”

Commenting on the Air Force report, Carr averred that “the capture of the RQ-170 by Iranian forces needs to be evaluated fairly and not dismissed as some kind of Iranian scam for reasons that have more to do with embarrassment than a rational assessment of the facts.”

“Theft of this technology via cyber attacks against the companies doing R&D and manufacture of the aircraft is ongoing,” Carr noted.

"Whether or not the Iranians got lucky or have acquired the ability to attack the C2 of the drone in question, there's obviously some serious errors in judgment being made at very high levels and secrecy about it is only serving the ones guilty of making those bad decisions."

While Carr's observations are true as far as it goes, the "serious errors in judgement" begin with chest-thumping U.S. and Israeli politicians who believe they have a monopoly when it comes to dictating policies or invading other countries, killing people on an industrial scale, stealing their resources and reducing their cities to smoking ruins as was done in both Gaza and Fallujah.

To make matters worse for technophilic Western militaries hell-bent on attacking Iran, *Tehran Times* reported Thursday that "Iran plans to put foreign spy drones it has in its possession on display in the near future."

According to unnamed sources quoted by the newspaper, which reflects the views of the Iranian government, "the foreign unmanned aircraft that Iran has are four Israeli and three U.S. drones."

Back in September, *The Christian Science Monitor* disclosed, "Gen. Moharam Gholizadeh, the deputy for electronic warfare at the air defense headquarters of the Islamic Revolutionary Guard Corps (IRGC), described to Fars News how Iran could alter the path of a GPS-guided missile–a tactic more easily applied to a slower-moving drone."

According to Peterson and Faramarzi, Gholizadeh told the news agency that "we have a project on hand that is one step ahead of jamming, meaning 'deception' of the aggressive systems," … such that "we can define our own desired information for it so the path of the missile would change to our desired destination."

While it is not possible to verify these claims, indeed they may be nothing more than propaganda offerings from Iranian spinmeisters, if their assertions are accurate, a technological leap such as this would pose a serious threat to any attacking force.

As I wrote back in 2009, since cheap and readily-obtainable software packages were now part of the spy-kit of Iraqi insurgent forces, I wondered whether it was "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 were told by military experts this was not possible; however, who would have dreamed that the Achilles' heel of Pentagon robo-warriors, blinded by their own arrogance and racist presumptions about the "Arab" or "Persian mind" was something as simple as their own imperial hubris.

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, he is a Contributing Editor with Cyrano's Journal Today. His articles can be read on Dissident Voice, Pacific Free Press, Uncommon Thought Journal, and the whistleblowing website WikiLeaks. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by AK Press and has contributed to the new book from Global Research, The Global Economic Crisis: The Great Depression of the XXI Century.

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/