GlobalResearch
Center for Research on Globalization

A Precursor to War? As Washington Renews Military Threats Against Iran, Cyber Attacks Escalate

By Tom Burghardt
Global Research, November 06, 2011
Antifascist Calling... 6 November 2011

Theme: Intelligence
In-depth Report: IRAN: THE NEXT WAR?

As evidence mounts that the U.S. secret state is launching cyber weapons against official enemies, while carrying out wide-ranging spy ops against their "friends," Gen. Keith Alexander, the dual-hatted overlord of the National Security Agency and U.S. Cyber Command, says that the Obama administration is "working on a system" that will "help" ISPs thwart malicious attacks.

Speaking at the Security Innovation Network (SINET) "Showcase 2011" shindig at the National Press Club in Washington, Alexander told security grifters eager to gouge taxpayers for another piece of lucrative "cybersecurity" pie: "What I'm concerned about are the destructive attacks. Those are the things yet to come that cause us a lot of concern."

That's rather rich coming from the head of a secretive Pentagon satrapy suspected of designing and launching the destructive Stuxnet virus which targeted Iran's civilian nuclear program.

According to fresh evidence provided by IT security experts it now appears that the same constellation of shadowy forces which unleashed Stuxnet are at it again with the newly discovered Duqu spy Trojan.

In a follow-up analysis, Kaspersky Lab researcher Alex Gostev wrote that "the highest number of Duqu incidents have been recorded in Iran. This fact brings us back to the Stuxnet story and raises a number of issues."

Not least of which is the continuing demonization of the Islamic Republic by an unholy alliance of U.S. militarists, their Israeli pit bulls and congressional shills hyping the "Iran threat."

War Drums Beating

With the United States and the other capitalist powers incapable of digging the world economy out from under the slow-motion meltdown sparked by 2008's market collapse, and with tens of millions of enraged citizens rejecting austerity measures that will further enrich financial elites at their expense, will the Obama administration "go for broke" and set-off a new conflagration in the Middle East?

Ratcheting up bellicose rhetoric, John Keane, a retired four-star general, former Vice Chief of Staff of the U.S. Army now currently perched on the board of General Dynamics, a major purveyor of cyber attack tools for the government, told the House Homeland Security Committee October 26, "We've got to put our hand around their throat now. Why don't we

kill them? We kill other people who are running terrorist operations against the United States."

AFP reported that "Iran made a formal protest" over Keane's remarks which urged "the targeted assassination of members of its elite Quds Force military special operations unit," over a fairy-tale plot allegedly cooked-up by Tehran, which employed a failed used-car salesman, a DEA snitch and members of the Zetas drug gang in a scheme to assassinate the Saudi ambassador in Washington.

While the plot lines are as preposterous as allegations prior to the 2003 Iraq invasion that Saddam Hussein's regime was involved in the 9/11 attacks, one cannot so easily dismiss the *propaganda value* of such reports by administration "information warriors." The same can be said of the series of controlled leaks emanating from London, Tel Aviv and Washington urging immediate air strikes against Iran's nuclear facilities.

The Guardian reported that "Britain's armed forces are stepping up their contingency planning for potential military action against Iran amid mounting concern about Tehran's nuclear enrichment programme."

Chillingly, the "Ministry of Defence believes the US may decide to fast-forward plans for targeted missile strikes at some key Iranian facilities. British officials say that if Washington presses ahead it will seek, and receive, UK military help for any mission, despite some deep reservations within the coalition government."

On the same day that MoD's sanctioned leak appeared in the British press, *Haaretz* disclosed that "Prime Minister Benjamin Netanyahu and Defense Minister Ehud Barak are trying to muster a majority in the cabinet in favor of military action against Iran, a senior Israeli official has said. According to the official, there is a 'small advantage' in the cabinet for the opponents of such an attack."

"Strategic Affairs Minister Moshe Ya'alon said he preferred an American military attack on Iran to an Israeli one. 'A military move is the last resort,' he said."

The *Associated Press* reported that as Netanyahu moved to persuade his cabinet to "authorize a military strike against Iran's suspected nuclear weapons program," Israel successfully test-fired "a missile believed capable of carrying a nuclear warhead to Iran."

Adding to the disinformational witch's brew, *The Washington Post* reported that "a new spike in anti-Iran rhetoric and military threats by Western powers is being fueled by fears that Iran is edging closer to the nuclear 'breakout' point, when it acquires all the skills and parts needed to quickly build an atomic bomb if it chooses to," anonymous "Western diplomats and nuclear experts said Friday."

Post stenographer Joby Warrick informed us that a "Western diplomat who had seen drafts of the report" told him "it will elaborate on secret intelligence collected since 2004 showing Iranian scientists struggling to overcome technical hurdles in designing and building nuclear warheads."

And late last week *Reuters* disclosed that "a senior U.S. military official said on Friday Iran had become the biggest threat to the United States and Israel's president said the military option to stop the Islamic republic from obtaining nuclear weapons was nearer."

"'The biggest threat to the United States and to our interests and to our friends … has come into focus and it's Iran,' said the U.S. military official, addressing a forum in Washington." Conveniently, "reporters were allowed to cover the event on condition the official not be identified."

While some critics argue that Israel does not presently have the capacity to launch such an attack, and that "the volume of the war hysteria is being turned up with one purpose in mind: the Israelis want the US to do their dirty work for them," such reasoning is hardly reassuring.

Indeed, as the *World Socialist Web Site* points out, "the Israeli government has already made advanced preparations for an attack on Iran."

"On the military front," analyst Peter Symonds warned that "Israeli warplanes last week conducted a long-range exercise–of the type required to reach Iran–using a NATO airbase on the Italian island of Sardinia." In other words, the IDF drill was not a "rogue" exercise unilaterally conducted by Israel, but further evidence of Washington's "desperate bid to offset its economic decline by securing its hegemony over the energy-rich regions of the Middle East and Central Asia."

In the context of escalating tensions over Iran's nuclear enrichment program, seeded by manufactured "terror" plots, the imperialist powers may choose the "cyber" route prior to launching devastating missile and bomber strikes against Iranian military installations and civilian infrastructure.

Pentagon planners now believe that attack tools have reached the point where blinding Iran's air defenses while sowing chaos across population centers with power outages and the shutdown of financial services may now be a viable option.

This is not idle speculation. During the run-up to the 2003 Iraq invasion, the *National Journal* disclosed that Central Command "considered a computerized attack to disable the networks that controlled Iraq's banking system, but they backed off when they realized that those networks were global and connected to banks in France."

Facing growing opposition at home and abroad to endless wars and imperial adventures, would the Obama administration have such qualms today?

Attack Tools Already in Play

As *Antifascist Calling* previously reported, when the Duqu virus was discovered last month, analysts at Symantec believed that the remote access Trojan (RAT) "is essentially the precursor to a future Stuxnet-like attack."

"The threat was written by the same authors (or those who have access to the Stuxnet source code) and appears to have been created since the last Stuxnet file was recovered," researchers averred.

Since their initial reporting, Symantec, drawing on research from CrySyS lab at the Budapest University of Technology and Economics in Hungary, the organization which discovered the malware, reported they located an installer file in the form of a Microsoft Word document which exploits a previously unknown zero-day vulnerability.

Like Stuxnet, Duqu's stealthiness is directly proportional to its uncanny ability to capitalize on what are called zero-day exploits hardwired into it's digital DNA; security holes that are unknown to everyone until the instant they're used in an attack.

Similar to other dubious commodities traded on our dystopian "free markets," zero-days are bits of tainted code sought by criminal hackers, financial and industrial spies and enterprising security agencies that can sell for up to $250,000 a pop on the black market.

When Stuxnet appeared in dozens of countries last year, targeting what are called programmable logic controllers (PLCs) on industrial computers manufactured by Siemens that control everything from water purification and food processing to oil refining and potentially deadly chemical processes, researchers found it was designed to harm only one specific target: PLCs processing uranium fuel at a nuclear facility in Iran.

As *Wired Magazine* reported, when Symantec analysts who had been picking Stuxnet apart convinced internet service providers who controlled "servers in Malaysia and Denmark" where the virus "phoned home" each time it infected a new machine, to reroute the virus to a secure "sinkhole," they were in for a shock.

"Out of the initial 38,000 infections," journalist Kim Zetter wrote, "about 22,000 were in Iran. Indonesia was a distant second, with about 6,700 infections, followed by India with about 3,700 infections. The United States had fewer than 400. Only a small number of machines had Siemens Step 7 software installed–just 217 machines reporting in from Iran and 16 in the United States."

"The sophistication of the code," *Wired* averred, "plus the fraudulent certificates, and now Iran at the center of the fallout made it look like Stuxnet could be the work of a government cyberarmy–maybe even a United States cyberarmy.

"This made Symantec's sinkhole an audacious move," Zetter wrote. "In intercepting data the attackers were expecting to receive, the researchers risked tampering with a covert U.S. government operation."

Writing in the *Journal of Strategic Studies*, Thomas Rid, a former RAND Corporation employee and "Reader in War Studies at Kings College in London," who has close ties to the Western military establishment, observed in relation to Stuxnet that network "sabotage, first, is a deliberate attempt to weaken or destroy an economic or military system. All sabotage is predominantly *technical* in nature, but of course may use social enablers."

"The resources and investment that went into Stuxnet could only be mustered by a 'cyber superpower', argued Ralph Langner, a German control system security consultant who first extracted and decompiled the attack code."

In an interview with National Public Radio, Langer said that the "level of expertise" behind Stuxnet "seemed almost alien. But that would be science fiction, and Stuxnet was a reality."

"Thinking about it for another minute, if it's not aliens, it's got to be the United States."

"For the time being it remains unclear how successful the Stuxnet attack against Iran's nuclear program actually was" Rid noted. "But it is clear that the operation has taken computer sabotage to an entirely new level."

Researcher Vikram Thakur, commenting on the latest Duqu discoveries reported: "The Word document was crafted in such a way as to definitively target the intended receiving organization." And whom, pray tell, was being targeted by Duqu? Why Iran, of course.

"Once Duqu is able to get a foothold in an organization through the zero-day exploit, the attackers can command it to spread to other computers."

Thakur wrote, "the Duqu configuration files on these computers," which did not have the ability to connect to the internet and the author's command and control (C&C) server, "were instead configured not to communicate directly with the C&C server, but to use a file-sharing C&C protocol with another compromised computer that had the ability to connect to the C&C server."

"Consequently," Thakur concluded, "Duqu creates a bridge between the network's internal servers and the C&C server. This allowed the attackers to access Duqu infections in secure zones with the help of computers outside the secure zone being used as proxies."

As Kaspersky Lab researchers pointed out, "in each of the four instances of Duqu infection a unique modification of the driver necessary for infection was used."

"More importantly," analysts averred, "regarding one of the Iranian infections there were also found to have been two network attack attempts exploiting the MS08-067 [MS Word] vulnerability. This vulnerability was used by Stuxnet too."

"If there had been just one such attempt, it could have been written off as typical Kido activity–but there were two consecutive attack attempts: this detail would suggest *a targeted attack on an object in Iran*." (emphasis added)

Simply put, before the Pentagon decides to "kill them" as Gen. Keane indelicately put it, battlefield preparations via directed cyber attacks and other forms of sabotage may be part of a preemptive strategy to decapitate Iranian defenses prior to more "kinetic" attacks.

'Boutique Arms Dealers'

Despite media hype about future cuts in the so-called "defense" budget, *Defense Industry Daily* disclosed that "the US military has announced plans to spend billions on technology to secure its networks."

According to the Defense Department's FY 2012 budget proposal, "the Pentagon said it plans to spend $2.3 billion on cybersecurity capabilities."

However, when *NextGov* "questioned why the Air Force's $4.6 billion 2012 budget request for cybersecurity was $2.3 billion more than Defense's servicewide spending proposal, Pentagon officials upped their total figure from $2.3 billion to $3.2 billion."

Why the discrepancy? A "Pentagon spokesperson explained that the service's estimate differed dramatically because the Air Force included 'things' that are not typically considered information assurance or cybersecurity."

What kind of "things" are we talking about here?

As *BusinessWeek* reported in July, firms such as Northrop Grumman, Raytheon, and General

Dynamics, “the stalwarts of the traditional defense industry,” are “helping the U.S. government develop a capacity to snoop on or disable other countries’ computer networks.”

Capitalizing on the Defense Department’s desire to develop “hacker tools specifically as a means of conducting warfare,” this “shift in defense policy gave rise to a flood of boutique arms dealers that trade in offensive cyber weapons.”

Investigative journalists Mike Riley and Ashlee Vance averred that “most of these are ‘black’ companies that camouflage their government funding and work on classified projects.”

As last winter’s hack of HBGary Federal by Anonymous revealed, “black” firms, including those like Palantir which received millions of dollars in start-up funding from the CIA’s venture capital arm In-Q-Tel, hacker tools, such as sophisticated Trojans and stealthy rootkits, believed to be the route used to introduce the Stuxnet virus, have also been used to target political activists and journalists in the United States at the behest of financial institutions such as the Bank of America and the right-wing U.S. Chamber of Commerce.

As researcher Barrett Brown revealed, “Team Themis was a consortium made up of HBGary, Palantir, and Berico (with Endgame Systems serving as a ‘silent partner’ and providing assistance from the sidelines) that was set up in order to provide offensive intelligence capabilities to private clients.”

Although Endgame Systems “went dark” after Anonymous released thousands of HBGary files, *The Register* disclosed that the firm “helps US intelligence identify and hack into vulnerable networks, and is targeting a similar role in Britain’s nascent national cyber security operations.”

The Register noted that the “limited publicly information currently available on the firm hints at its further role assisting clandestine government cyber operations by identifying targets and developing exploits.”

As *BusinessWeek* revealed, the firm is “a major supplier of digital weaponry for the Pentagon. It offers a smorgasbord of wares, from vulnerability assessments to customized attack technology, for a dizzying array of targets in any region of the world.”

Unsurprisingly, this was a major draw for venture capital firms “Bessemer Venture Partners and Kleiner Perkins Caufield & Byers,” who collectively fronted Endgame some $30 million. According to Riley and Vance, “what really whet the VCs’ appetites, though, according to people close to the investors, is Endgame’s shot at becoming the premier cyber-arms dealer.”

While a client list has yet to emerge, it’s safe to assume that secret state agencies on both sides of the Atlantic are lining up to purchase Endgame’s toxic products.

Although no definitive answer has emerged as to whom might targeting Iran with Duqu, as *BusinessWeek* revealed Endgame “deals in zero-day exploits. Some of Endgame’s technology is developed in-house; some of it is acquired from the hacker underground. Either way, these zero days are militarized–they’ve undergone extensive testing and are nearly fail-safe.”

“People who have seen the company pitch its technology–and who asked not to be named because the presentations were private–say Endgame executives will bring up maps of

airports, parliament buildings, and corporate offices."

According to Riley and Vance, "the executives then create a list of the computers running inside the facilities, including what software the computers run, and a menu of attacks that could work against those particular systems."

Indeed, "Endgame weaponry comes customized by region–the Middle East, Russia, Latin America, and China–with manuals, testing software, and 'demo instructions.' There are even target packs for democratic countries in Europe and other U.S. allies."

"The quest in Washington, Silicon Valley, and around the globe is to develop digital tools both for spying and destroying," *BusinessWeek* observed. "The most enticing targets in this war are civilian–electrical grids, food distribution systems, any essential infrastructure that runs on computers."

"This stuff is more kinetic than nuclear weapons," Dave Aitel, the founder of a computer security company in Miami Beach called Immunity told Riley and Vance. "Nothing says you've lost like a starving city."

While Aitel and a host of other "little Eichmanns" who enrich themselves servicing the American secret state refused to discuss his firm's work for the government, a source told the publication that Immunity "makes weaponized 'rootkits': military-grade hacking systems used to bore into other countries' networks," and that Aitel's clients "include the U.S. military and intelligence agencies."

We do not know if, or when, the United States, NATO and Israel will opt for a military "solution" to the so-called "Iranian problem."

We do know however, as the *World Socialist Web Site* warned, "as global capitalism lurches from one economic and political crisis to the next, rivalry between the major powers for markets, resources and strategic advantage is plunging humanity towards a catastrophic conflict that would devastate the planet."

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, The Intelligence Daily, 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/