JCS Chief General Dempsey's last hurrah in Israel amidst alleged Israeli Cyber Spying on Iran Talks

JCS Chief Gen. Martin Dempsey and IDF Chief of Staff Gen. Gadi Eizenkot, Tel Aviv, June 9, 2015

Source: Reuters

Outgoing Chairman of the US Joint Chiefs of Staff, Gen. Martin Dempsey made his last visit to Tel Aviv to meet with IDF counterparts. Ostensibly this trip by outgoing JCS chief Dempsey was to assure the IDF that the US would live up to its pledge to maintain the Qualitative Military Edge superiority of the IDF in the Middle East. This was about Israeli concerns raised over advanced weapons systems like the F-35 being offered to Gulf Cooperation Council, notably Saudi Arabia. Saudi Arabia is caught between Iran's hegemony over four Arab capitals, the threats of ISIS infiltrating the Kingdom perpetrating suicide bombings and the current conflict against Iranian trained Houthi rebels in Yemen. Somehow we are lent the impression that he may have been there to promote the benefits of a looming P5+1 deal against a nuclear Iran, trusting that any deal with Islamist Iran threatening to wipe Israel off the map of the word wouldn't interfere with the long coveted exchange of intelligence and cyber-security information between the two allies.

Kaspersky Labs Moscow-based cyber security firm

Source; Reuters/Sergei Karpukhin

That impression was dispelled by news from Moscow-based Kaspersky Laboratories, a premier cyber security firm detecting a new malware, called Duqu Bet, named after the second alphabet in the Hebrew alphabet alleging possible Israeli development of a powerful cyber spy software system. A *Wall Street Journal* report suggested that Duqu Bet was allegedly targeting posh hotels used for private US Iranian negotiations in Switzerland and Austria. In a February 2015 Iconoclast post we noted Duqu 1.0 as a key component in the Equation group discovered by cyber security firm Kaspersky Labs based in Russia:

> The Equation Group according to Kaspersky has a powerful and geographically distributed network covering more than 300 web domains involving over 100 servers located in the US, UK, Italy, Germany, Netherlands, Panama, Costa Rica, Malaysia, Colombia and the Czech Republic. Since 2001, it has infected tens of thousands of "high profile victims" in over 30 countries. Examples include: "Government and diplomatic institutions, Telecommunications, Aerospace, Energy, Nuclear research, Oil and Gas, Military, Nanotechnology, Islamic activists and scholars, Mass media, Transportation, Financial institutions and companies developing encryption technologies."

Business Insider noted the hypocrisy of Kaspersky disclosing this latest alleged Israeli Malware:

> "The use of Duqu by Israel against Iran is not the question we should be asking," Jeff Bardin, chief intelligence officer of Treadstone 71, told Business Insider. "The question should be why Kaspersky only finds code of this type by nation-states it does not consider friendly to Russia or those aligned to the West." Is it because there is no code of this type [Duqu] coming out of Russia?" Bardin asks, "Or is it because disclosing code of this type that is Russian made and in use against target

> nation-states would place Eugene Kaspersky at risk of countering his country's cyber espionage efforts and, at risk of incurring the wrath of Putin?"
>
> The firm's billionaire founder and CEO, Eugene Kaspersky, used to work for the KGB and reportedly maintains relationships with former and current Russian intelligence officials.
>
> "Kaspersky releases this information as a political tool," Bardin said. "The absence of any photos of Kaspersky with Putin on the internet is itself evidence of direct alignment. Can you be a billionaire in Russia today without the direct scrutiny of Vladimir Putin?"
>
> A Bloomberg analysis of Kaspersky's work generally supports Bardin's suspicions: "While Kaspersky Lab has published a series of reports that examined alleged electronic espionage by the U.S., Israel, and the U.K., the company hasn't pursued alleged Russian operations with the same vigor

Doubtless the Israeli military and national security echelons harrumphed about US cybersecurity expertise given Chinese and Russian hacking of US government and White House files. *The Wall Street Journal* reported Israel building a $5.9 billion cyber communication security complex near Beersheba in the Negev to house military high tech echelons including the fabled Unit 8200. That has attracted US high tech and defense firms like EMC, Oracle and Lockheed Martin to build facilities in the planned development.

The Pentagon recently announced "restocking" of supplies of tens of thousands of rockets, missiles, and quantities of ammunition held back at White House request during last

summer's Operation Defense Edge. That may not include so-called bunker busters or the Boeing developed CHAMP non-nuclear EMP cruise missile capable of destroying computers and communication nets of Iran's nuclear program without loss of life. The Pentagon promoted this latest offering as an increase of weapons under the $1.8 billion military grant.

However, Dempsey's leave taking and his successor, Marine General Marine Corps Gen. Joseph F. Dunford Jr. arrival under Pentagon civilian chief, Secretary of Defense Ashton Carter may have a different agenda. With 18 months left in the President's second term and a possible diplomatic deal with Iran over its nuclear program releasing tens of billions of funds, Israel is clearly concerned. Concerned that Iran may already have achieved a nuclear threshold and been given funds to support state terrorism enabling delivery of more weapons to proxies, Hezbollah and Hamas. Hezbollah's Sheik Nasrallah threatened "displacement of Millions of Israelis" in any future conflict with Israel raining down hundreds of thousands of Iranian supplied rockets and missiles on the Jewish nation.

Meanwhile, the alleged solid intelligence and security alliance between the US and Israel appears tattered, awaiting a successor to President Obama in January 2017 who may return the previously productive relationship to solid footing.