GlobalResearch
Center for Research on Globalization

U.S.-Israeli Cyber-Sabotage of Iran: Throwing the First Cyber-Stone

By Arjen Kamphuis
Global Research, March 25, 2013
Consortiumnews

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

Director of National Intelligence James Clapper calls cyber-attacks a top national security concern, but these U.S. alarms sound hypocritical after the joint U.S.-Israeli cyber-sabotage of Iran's nuclear industry.

A few years ago, Israeli and American intelligence developed a computer virus with a specific military objective: damaging Iranian nuclear facilities. Stuxnet was spread via USB sticks and settled silently on Windows PCs. From there it looked into networks for specific industrial centrifuges using Siemens SCADA control devices spinning at high-speed to separate Uranium-235 (the bomb stuff) from Uranium-238 (the non-bomb stuff).

Iran, like many other countries, has a nuclear program for power generation and the production of isotopes for medical applications. Most countries buy the latter from specialists like the Netherlands that produces medical isotopes in a special reactor. The Western boycott of Iran makes it impossible for Iran to purchase isotopes on the open market. Making them yourself is far from ideal, but the only option that remains.

Image: Cascade of gas centrifuges used to produce enriched uranium. (Photo credit: U.S. Department of Energy)

Why the boycott? Officially, according to the U.S., it's because Iran won't give sufficient openness about its weapons programs, in particular, military applications of its nuclear program. This concern is fairly recent and, for some reason, has only been reactivated after the U.S. attack on Iraq in 2003 (a lot of the original nuclear equipment in Iran was supplied by American and German companies with funding from the World Bank before the 1979 revolution).

The most curious aspect of the West's allegations about Iran is that they are never more than vague insinuations. When all 16 U.S. intelligence agencies in 2007 produced a joint study there was a clear conclusion: Iran is not developing a nuclear weapon. (To see a recent speech by the leader of this study, click here.)

And that's what's strange. For if the 16 American intelligence services and their Israeli colleagues, the Mossad, can all agree that Iran is not making nuclear weapons, how do you justify an attack against Iran's civilian industrial infrastructure via the Stuxnet computer virus? And this is the equivalent of a military attack as would be clear if you consider what would happen if Iran had been caught in a cyber-attack on Western installations

in Borssele or Indian Point.

Stuxnet is designed for a single purpose: the damage of nuclear enrichment facilities in Iran, a country that may just be performing these activities in accordance with the international agreements stipulated in the Non-Proliferation Treaty. Iran, like most other countries in the world, signed this Convention. The countries outside the NPT are Israel, India, Pakistan, North Korea (which withdrew) and the newly independent South Sudan.

Under the NPT, a civilian nuclear industry is allowed, a detail that sometimes escapes the attention of editors. I'm not saying the Iranian government is filled with darlings, but Iran has not attacked anyone in the past 200 years, unlike some NATO countries.

But Stuxnet has made some things very clear to Iran and the rest of the non-Western world. It does not matter that you abide by established agreements and treaties. It does not matter that you're not a threat to the West. It does not matter that the countries that accuse you most of violating the non-proliferation agreements (U.S. and Israel, for instance) are themselves egregious violators; U.S. by delivering plutonium to Israel and Israel by not signing the treaty and secretly holding 100-200 nuclear bombs.

So, there appears to be no reason for you to stick to agreements or treaties because doing so does not guarantee that the parties on the other side will do the same. Plus, it may offer a strategic disadvantage. And if you going to have the disadvantage of such alleged conduct (facing boycotts and threats of bombing when you're not building a nuclear weapon), it is logical that you might want the benefits.

It is almost rational for Iran to develop a military nuclear program. Certainly North Korea seems to get away with it. As a bonus, North Korea now has a few nuclear weapons and that is still the best guarantee that the U.S. will not be showing up with unsolicited packages of "democracy" (although a lack of oil wells also seems to help).

Similarly, the invasion of Iraq in violation of international laws against aggressive warfare showed that the U.S. again does not comply with the standards that it happily tries to impose on others. The attack on Iraq was carried out based on lies. Key U.S. and UK officials knew Saddam Hussein had no WMDs.

Now, with the U.S.-Israeli cyber-attack on Iran, it's clear that no one takes standards decrying offensive use of cyber-warfare seriously either. The world and cyberspace are becoming a Wild West shooting gallery.

And that's exactly what you do not want in a world where a handful of angry hackers from China, Russia, Iran, Iraq or any other country can anonymously and in secret take down your critical infrastructure. Western countries are much more vulnerable due to their high degree of automation than countries that have just outgrown their Third World status.

Cyber-weapons are relatively inexpensive and developing them is more difficult to detect than the construction of missiles and aircraft carriers. The best defense against cyber-war is the prevention of an arms race. Everybody loses in a cyber-war. Safety in such a context is created by moral leadership (starting with: follow your own rules) and actively working at de-escalation. And that is exactly what the U.S. and Israel have not done.

With such behavior, we are assured of a continuous stream of new enemies in countries that mainly want to be left alone, but that arm themselves just in case the "free West" is on the

prowl in their region. If you live in a glass house, not throwing stones (and not motivating others to do so) is the smarter move.

Arjen Kamphuis *is co-founder and Chief Technology Officer of Gendo. He studied Science and Policy at Utrecht University and worked for IBM and Twynstra Gudde as IT architect, trainer and IT strategy adviser. Since late 2001, Arjen has advised clients on the strategic impact of new technological developments.*

Articles by: **Arjen Kamphuis**