Revisiting Stuxnet: The Israeli-American Computer Virus that Started Cyber-Warfare

By Philip Giraldi

Global Research, September 09, 2019

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

New evidence has surfaced to demonstrate how both American and Israeli intelligence services, aided by European partners, have long been targeting Iran in spite of clear evidence that it constituted no threat. The story involves the Stuxnet virus or "worm," which was first employed in 2007 and eventually identified and exposed by cybersecurity experts in 2010. It constituted one of the first effective uses of a cyber-weapon, carried out in secret by two countries against a third country with which the two were not at war.

Stuxnet was one of a series of viruses developed by Israel and the United States shortly after the turn of the century to target and disrupt specific operating systems in computers by accessing what are referred to as the programmable logic controllers, which operate and manage machinery, to include the centrifuges that are employed in separating and enriching nuclear material. The systems are accessed through Microsoft Windows operating systems and networks, which in turn provide access to the Siemens software that was in use at the Iranian nuclear research facility at Natanz. The centrifuges themselves could be ordered by the virus to speed up and spin wildly, causing them in many cases to tear themselves apart.

The insertion of Stuxnet in the Iranian computers in 2007 by means of a thumb drive reportedly ruined twenty percent of Iran's existing centrifuges, more than 1,000 machines, but it also spread and infected several hundred thousand computers using Microsoft and Siemens software and eventually wound up in large numbers of machines outside Iran. Though the Stuxnet virus had been designed with safeguards to prevent its spread, it did eventually infect other computers and propagate worldwide. Its use by its developers was regarded as particularly reckless after it was discovered and identified.

Ironically, two comprehensive studies by the American Government's Central Intelligence Agency (CIA) conducted in 2007 and 2012 determined that no Iranian nuclear weapons program existed and that Iran had never taken any serious steps to initiate such research. Israel was also aware that there was no program but it was active in planting fabricated information suggesting that a secret facility existed that was engaged in weapon development. It has frequently been observed that Israel's **Prime Minister Benjamin Netanyahu** has been warning for twenty years that Iran is "six months away" from having an atomic bomb.

Nevertheless, even though the Iranian nuclear threat was known to be a fantasy by 2007 at the latest, the Israeli government, sometimes working in collusion with American intelligence agencies, took steps to interfere with Iran's existing and completely legal and open to inspection civilian atomic energy program. A multifaceted plan was developed and executed that included using surrogates to identify then kill Iranian scientists and technicians while also developing and introducing viruses into the country’s computer systems. This was in spite of the fact that Iran was fully compliant with international norms on nuclear research and had its facilities regularly inspected by the International Atomic Energy Agency (IAEA). Iran was also a signatory to the Nuclear Non-Proliferation Treaty (NPT), which Israel, possessing its own nuclear arsenal consisting of as many as 200 weapons, had refused to sign.

All of the backgrounds to Stuxnet has been known for some time, but one mystery remained: how did the virus get introduced into the Natanz computers as the research center was “quarantined” and not connected to the internet so that it could not be attacked from outside? That question has now been answered.

The Dutch external intelligence service AIVD had been approached by the U.S. and Israel in 2004 to provide help in locating a suitable Iranian to be groomed for the project. At that time, Holland had a large expat Iranian community and it was a relatively easy country for Iranian travelers to enter. Eventually, an Iranian engineer was identified, recruited and trained to plant the Stuxnet virus at the Natanz Iranian nuclear research site in 2007, with the objective of sabotaging the uranium enrichment centrifuges in what was to be the first-ever major use of a cyber-weapon.

The actual insertion of the thumb drive was part of a broader operation which began with a thorough debriefing of the engineer, who had previously been a contractor at Natanz, regarding the location of the centrifuges and other hardware within the facility, making it possible to write code that could target the centrifuges and their control systems specifically.

The Israeli-American-Dutch agent/mole, who was responding to an offer of considerable money and resettlement in the West, set up a computer systems maintenance and repair company in Iran that eventually was able to obtain contract work at Natanz. The agent made several visits to the facility to fine-tune his approach to installing the virus prior to actually doing so.

According to the media report, the operation was called the “Olympic Games” after the five-ring Olympian symbol because it wound up including the intelligence agencies of five countries after Germany and France joined in on the effort. It should be noted that Holland, Germany and France all had nominally friendly relations with Iran at the time. Then U.S. **President George W. Bush** personally approved the attack after his concerns that the virus might escape from Iran and cause a major international crisis were addressed by technical experts.

There were several arrests and executions at Natanz after the virus was discovered and it is not known if the Dutch mole ever collected on his money and the promised resettlement. More recently, Iran entered into the Joint Comprehensive Plan of Action (JCPOA) with the U.S., the United Nations, Britain, Germany, France, China and Russia in 2015. **President Donald Trump** withdrew from the arrangement last year for reasons best described a fatuous and, as of now, JCPOA is still in place but under considerable strain from all sides.

One might argue that the continuing Iran nuclear crisis all started with the reckless deployment of Stuxnet, which was based on a flawed assessment, did not have to be done, and was executed for all the wrong reasons, primarily consisting of pressure from Israel on Washington to "do something." It also demonstrated that cyber-warfare was for real and could do great damage to infrastructure, a genie that has been let out of the bottle and has made the world a much less safe place. It has, in fact, become a global problem that continues to vex politicians and national security experts worldwide.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

This article was originally published on American Herald Tribune.

***Philip M. Giraldi** is a former CIA counter-terrorism specialist and military intelligence officer who served nineteen years overseas in Turkey, Italy, Germany, and Spain. He was the CIA Chief of Base for the Barcelona Olympics in 1992 and was one of the first Americans to enter Afghanistan in December 2001. Phil is Executive Director of the Council for the National Interest, a Washington-based advocacy group that seeks to encourage and promote a U.S. foreign policy in the Middle East that is consistent with American values and interests. He is a frequent contributor to Global Research.*

Featured image is from Graham Cluley/ Twitter

The original source of this article is Global Research

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Philip Giraldi**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca