Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran

news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html

Kim Zetter and Huib Modderkolk

Yahoo News photo illustration; photos: AP, Getty Images. Shutterstock

For years, an enduring mystery has surrounded the Stuxnet virus attack that targeted Iran's nuclear program: How did the U.S. and Israel get their malware onto computer systems at the highly secured uranium-enrichment plant?

The first-of-its-kind virus, designed to sabotage Iran's nuclear program, effectively launched the era of digital warfare and was unleashed some time in 2007, after Iran began installing its first batch of centrifuges at a controversial enrichment plant near the village of Natanz.

The courier behind that intrusion, whose existence and role has not been previously reported, was an inside mole recruited by Dutch intelligence agents at the behest of the CIA and the Israeli intelligence agency, the Mossad, according to sources who spoke with Yahoo News.

An Iranian engineer recruited by the Dutch intelligence agency AIVD provided critical data that helped the U.S. developers target their code to the systems at Natanz, according to four intelligence sources. That mole then provided much-needed inside access when it came time to slip Stuxnet onto those systems using a USB flash drive.

The Dutch were asked in 2004 to help the CIA and Mossad get access to the plant, but it wasn't until three years later that the mole, who posed as a mechanic working for a front company doing work at Natanz, delivered the digital weapon to the targeted systems. "[T]he Dutch mole was the most important way of getting the virus into Natanz," one of the sources told Yahoo.

Neither the CIA nor the Mossad responded to inquiries from Yahoo News about the information. The AIVD declined to comment on its involvement in the operation.

The now famous covert operation known as "Olympic Games" was designed not to destroy Iran's nuclear program outright but to set it back for a while to buy time for sanctions and diplomacy to take effect. That strategy was successful in helping to bring Iran to the negotiating table, and ultimately resulted in an agreement with the country in 2015.

The revelation of Dutch involvement harkens back to a time when there was still extensive cooperation and strong, multilateral agreement among the U.S. and its allies about how to deal with the Iranian nuclear program — a situation that changed last year after the Trump administration pulled out of the hard-won nuclear accord with Tehran.

President Trump displays a document reinstating sanctions against Iran after announcing the U.S. withdrawal from the Iran nuclear deal, May 8, 2018. (Photo: Saul Loeb/AFP/Getty Images)

The Olympic Games operation was primarily a joint U.S.-Israel mission that involved the NSA, the CIA, the Mossad, the Israeli Ministry of Defense and the Israeli SIGINT National Unit, Israel's equivalent of the NSA. But the U.S. and Israel had assistance from three other nations, according to sources, hence the covert codename that gave nod to the five-ring symbol of the world's most famous international sporting event. Two of the three participating players were the Netherlands and Germany. The third is believed to be France, although U.K. intelligence also played a role.

Germany contributed technical specifications and knowledge about the industrial control systems made by the German firm Siemens that were used in the Iranian plant to control the spinning centrifuges, according to sources. France is believed to have provided intelligence of a similar sort.

But the Dutch were in a unique position to perform a different role — delivering key intelligence about Iran's activities to procure equipment from Europe for its illicit nuclear program, as well as information about the centrifuges themselves. This is because the centrifuges at Natanz were based on designs stolen from a Dutch company in the 1970s by Pakistani scientist Abdul Qadeer Khan. Khan stole the designs to build Pakistan's nuclear program, then proceeded to market them to other countries, including Iran and Libya.

The Dutch intelligence agency, known as AIVD, along with U.S. and British intelligence, infiltrated Khan's supply network of European consultants and front companies who helped build the nuclear programs in Iran and Libya. That infiltration didn't just involve old-school tradecraft but also employed offensive hacking operations being developed as part of the burgeoning field of digital espionage.

AIVD's cyber capabilities are well known now — last year it was revealed that AIVD was responsible for tipping off the FBI to the 2016 hack of the Democratic National Committee, knowledge it had acquired because its operatives had hacked into computers belonging to the Russian hacking group known as Cozy Bear in 2014 and were watching in 2015 when the Russians broke into computers at the U.S. State Department and the DNC.

But during the early days of Iran's nuclear program, AIVD's hacking team was small and still developing.

Nuclear physicist Adbul Qadeer Khan. (Photo: Robert Nickelsberg/Life Images Collection via Getty Images)

The Iranian program, which had been on the back burner for years, kicked into high gear in 1996, when Iran secretly purchased a set of blueprints and centrifuge components from Khan. In 2000, Iran broke ground at Natanz with plans to build a facility that would hold 50,000 spinning centrifuges for enriching uranium gas. That same year, AIVD hacked the email system of a key Iranian defense organization in an effort to obtain more information about Iran's nuclear plans, according to sources.

Israeli and Western intelligence agencies secretly monitored the progress at Natanz over the next two years, until August 2002, when an Iranian dissident group publicly exposed the Iranian program at a press conference in Washington, D.C., using information provided by the intelligence agencies. Inspectors for the International Atomic Energy Agency, the United Nations body that monitors nuclear programs around the world, demanded access to Natanz and were alarmed to discover that the Iranian program was much further along than believed.

Iran was pressed into agreeing to halt all activity at Natanz while the IAEA sought to obtain more information about the nuclear program, and the suspension continued throughout all of 2004 and most of 2005. But it was only a matter of time before operations at Natanz resumed, and the CIA and the Mossad wanted to be inside when they did.

The request to the Dutch for help with this came toward the end of 2004, when a Mossad liaison working out of the Israeli Embassy in the Hague and a CIA official based at the U.S. Embassy met with a representative from AIVD. There was no talk yet about inserting a digital weapon into the control systems at Natanz; the aim at that time was still just intelligence.

But the timing wasn't random. In 2003, British and U.S. intelligence had landed a huge coup when they intercepted a ship containing thousands of centrifuge components headed to Libya — components for the same model of centrifuges used at Natanz. The shipment provided clear evidence of Libya's illicit nuclear program. Libya was persuaded to give up the program in exchange for the lifting of sanctions, and also agreed to relinquish any components already received.

By March 2004, the U.S., under protest from the Dutch, had seized the components from the ship and those already in Libya and flown them to the Oak Ridge National Lab in Tennessee and to a facility in Israel. Over the next months, scientists assembled the centrifuges and studied them to determine how long it might take for Iran to enrich enough gas to make a bomb. Out of this came the plot to sabotage the centrifuges.

The Department of Energy complex at Oak Ridge, Tenn. (Photo: Cryptome.org)

The Dutch intelligence agency already had an insider in Iran, and after the request from the CIA and Mossad came in, the mole decided to set up two parallel tracks — each involving a local front company — with the hope that one would succeed getting into Natanz.

Establishing a dummy company with employees, customers and records showing a history of activity, takes time, and time was in short supply. In late 2005, Iran announced it was withdrawing from the suspension agreement, and in February 2006 it began to enrich its first batch of uranium hexaflouride gas in a pilot plant in Natanz. The Iranians ran into some problems that slowed them down, however, and it wasn't until February 2007 that they formally launched the enrichment program by installing the first centrifuges in the main halls at Natanz.

By then, development of the attack code was already long under way. A sabotage test was conducted with centrifuges some time in 2006 and presented to President George Bush, who authorized the covert operation once he was shown it could actually succeed.

By May 2007, Iran had 1,700 centrifuges installed at Natanz that were enriching gas, with plans to double that number by summer. But sometime before the summer of 2007, the Dutch mole was inside Natanz.

The first company the mole established had failed to get into Natanz — there was a problem with the way the company was set up, according to two of the sources, and "the Iranians were already suspicious," one explained.

The second company, however, got assistance from Israel. This time, the Dutch mole, who was an engineer by training, managed to get inside Natanz by posing as a mechanic. His work didn't involve installing the centrifuges, but it got him where he needed to be to collect configuration information about the systems there. He apparently returned to Natanz a few times over the course of some months.

"[He] had to get … in several times in order to collect essential information [that could be used to] update the virus accordingly," one of the sources told Yahoo News.

The sources didn't provide details about the information he collected, but Stuxnet was meant to be a precision attack that would only unleash its sabotage if it found a very specific configuration of equipment and network conditions. Using the information the mole provided, the attackers were able to update the code and provide some of that precision.

There is, in fact, evidence of updates to the code occurring during this period. According to the security firm Symantec, which reverse-engineered Stuxnet after it was discovered, the attackers made updates to the code in May 2006 and again in February 2007, just as Iran began installing the centrifuges at Natanz. But they made final changes to the code on Sept. 24, 2007, modifying key functions that were needed to pull off the attack, and compiled the code on that date. Compiling code is the final stage before launching it.

An aerial view of the Natanz fuel enrichment plant. (Photo: DigitalGlobe via Getty Images)

The code was designed to close exit valves on random numbers of centrifuges so that gas would go into them but couldn't get out. This was intended to raise the pressure inside the centrifuges and cause damage over time and also waste gas.

This version of Stuxnet had just one way to spread — via a USB flash drive. The Siemens control systems at Natanz were air-gapped, meaning they weren't connected to the internet, so the attackers had to find a way to jump that gap to infect them. Engineers at Natanz programmed the control systems with code loaded onto USB flash drives, so the mole either directly installed the code himself by inserting a USB into the control systems or he infected the system of an engineer, who then unwittingly delivered Stuxnet when he programmed the control systems using a USB stick.

Once that was accomplished, the mole didn't return to Natanz again, but the malware worked its sabotage throughout 2008. In 2009 the attackers decided to change tactics and launched a new version of the code in June that year and again in March and April 2010. This version, instead of closing valves on the centrifuges, varied the speed at which the centrifuges spun, alternatively speeding them up to a level beyond which they were designed to spin and slowing them down. The aim was to both damage the centrifuges and undermine the efficiency of the enrichment process. Notably, the attackers had also updated and

compiled this version of the attack code back on Sept. 24, 2007, when they had compiled the code for the first version — suggesting that intelligence the Dutch mole had provided in 2007 may have contributed to this version as well.

By the time this later version of the code was unleashed, however, the attackers had lost the inside access to Natanz that they had enjoyed through the mole — or perhaps they simply no longer needed it. They got this version of Stuxnet into Natanz by infecting external targets who brought it into the plant. The targets were employees of five Iranian companies — all of them contractors in the business of installing industrial control systems in Natanz and other facilities in Iran — who became unwitting couriers for the digital weapon.

“It’s amazing that we’re still getting insights into the development process of Stuxnet [10 years after its discovery],” said Liam O’Murchu, director of development for the Security Technology and Response division at Symantec. O’Murchu was one of three researchers at the company who reversed the code after it was discovered. “It’s interesting to see that they had the same strategy for [the first version of Stuxnet] but that it was a more manual process. ... They needed to have someone on the ground whose life was at risk when they were pulling off this operation.”

O’Murchu thinks the change in tactics for the later version of Stuxnet may be a sign that the capabilities of the attackers improved so that they no longer needed an inside mole.

“Maybe … back in 2004 they didn’t have the ability to do this in an automated way without having someone on the ground,” he said. “Whereas five years later they were able to pull off the entire attack without having an asset on the ground and putting someone at risk.”

But their later tactic had a different drawback. The attackers added multiple spreading mechanisms to this version of the code to increase the likelihood that it would reach the target systems inside Natanz. This caused Stuxnet to spread wildly out of control, first to other customers of the five contractors, and then to thousands of other machines around the world, leading to Stuxnet’s discovery and public exposure in June 2010.

International Atomic Energy Agency inspectors and Iranian technicians at the nuclear power plant in Natanz, Iran, in January 2014. (Photo: Kazem Ghane/AFP/Getty Images)

Months after Stuxnet's discovery, a website in Israel indicated that Iran had arrested and possibly executed several workers at Natanz under the belief that they helped get the malware onto systems at the plant. Two of the intelligence sources who spoke with Yahoo News indicated that there indeed had been loss of life over the Stuxnet program, but didn't say whether this included the Dutch mole.

While Stuxnet didn't significantly set back the Iranian program — due to its premature discovery — it did help buy time for diplomacy and sanctions to bring Iran to the negotiating table. Stuxnet also changed the nature of warfare and launched a digital arms race. It led other countries, including Iran, to see the value in using offensive cyber operations to achieve political aims — a consequence the U.S. has been dealing with ever since.

Gen. Michael Hayden, former head of the CIA and the NSA, acknowledged its groundbreaking nature when he likened the Stuxnet operation to the atomic bombs dropped on Hiroshima and Nagasaki.

"I don't want to pretend it's the same effect," he said, "but in one sense at least, it's August 1945."

Kim Zetter is a journalist and the author of Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. *Huib Modderkolk is a journalist with the Dutch newspaper de Volkskrant who broke the story last year of AIVD's hack of Cozy Bear; he is also the author of* Het is oorlog: maar niemand die het ziet (The Invisible War), *to be published this week in the Netherlands.*

_____