Iran should investigate Stuxnet virus, says atomic chief

Senior official says claims of major harm to power station need investigation, as Russia warns plant could be 'new Chernobyl'

- Charles Arthur and agencies


Iran's Bushehr nuclear power plant. Photograph: Atta Kenare/AFP/Getty Images

Iran should investigate claims that the Stuxnet computer virus has caused major harm to its first nuclear power station, a senior official said on Friday, following suggestions that the plant could become a "new Chernobyl".

The acting head of Iran's atomic energy organisation, Mohammad Ahmadian, said reports of major damage to the Bushehr plant were a malicious campaign by countries hostile to Tehran's nuclear programme, but that they should be looked into in any case.

"Many of these discussions raised in the media and world public opinion about the Stuxnet virus are an effort to create concern among the Iranian people and people of the region and delay the work of the nuclear power plant," he told the ISNA news agency. "Therefore it is necessary that experts in the field investigate to see how much truth there is in these discussions."

Many analysts believe Stuxnet was a cyber attack by the US and Israel aimed at disabling Iran's nuclear equipment and slowing down a programme they believe is aimed at making nuclear weapons.

Iranian officials have confirmed Stuxnet hit staff computers at Bushehr but said it did not affect major systems. They deny that they are manufacturing nuclear weapons.

Stuxnet is a computer worm that spreads through Windows networks and targets specific machinery called programmable logic controllers built by the German company Siemens. Those run software called Step-7; Stuxnet interferes with their operation in a way that can cause high-speed machinery to fail disastrously.

It was first spotted online in March 2010, though elements of it were spotted by computer virus experts in summer 2009. It spread through networks via infected USB memory sticks; it is believed that the infection at Bushehr originated from USB sticks brought there from Russia.

Last month the New York Times reported that the deployment of Stuxnet to target Bushehr had reduced the risks of a military strike on the country, and that the computer code had been tested at Israel's Dimona plant which uses the same uranium centrifuges, used to refine the fuel, as Bushehr.

Last week Russia's ambassador to Nato said the worm's effects "could lead to a new Chernobyl", referring to the 1986 nuclear accident at a plant in Ukraine, then part of the Soviet Union.

Russia built and supplied the fuel for Bushehr, which has yet to start injecting power onto Iran's national grid.

"If supposedly an incident with a damaging effect on [Bushehr] happens, it would have more impact on Russians than Iranians as it will harm their reputation as an actor who claims to be willing to participate in building other nuclear power plants in different countries," Ahmadian said. But, he added, "There is no significant delay ... in the startup of the Bushehr plant."

Yukiya Amano, the director general of the International Atomic Energy Agency, told Reuters on Tuesday he believed Russia and Iran were paying "enough attention" to prevent any accident, but expressed concern about cyber attacks on nuclear facilities.

Israeli Test on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER

Published: January 15, 2011

*This article is by **William J. Broad**, **John Markoff** and **David E. Sanger**.*

Nicholas Roberts for The New York Times

Ralph Langner, an independent computer security expert, solved Stuxnet.

The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear centrifuges and helped delay, though not destroy, Tehran's ability to make its first nuclear arms.

"To check out the worm, you have to know the machines," said an American expert on nuclear intelligence. "The reason the worm has been effective is that the Israelis tried it out."

Though American and Israeli officials refuse to talk publicly about what goes on at Dimona, the operations there, as well as related efforts in the United States, are among the newest and strongest clues suggesting that the virus was designed as an American-Israeli project to sabotage the Iranian program.

In recent days, the retiring chief of Israel's Mossad intelligence agency, Meir Dagan, and Secretary of State Hillary Rodham Clinton separately announced that they believed Iran's efforts had been set back by several years. Mrs. Clinton cited American-led sanctions, which have hurt Iran's ability to buy components and do business around the world.

The gruff Mr. Dagan, whose organization has been accused by Iran of being behind the deaths of several Iranian scientists, told the Israeli Knesset in recent days that Iran had run into technological difficulties that could delay a bomb until 2015. That represented a sharp reversal from Israel's long-held argument that Iran was on the cusp of success.

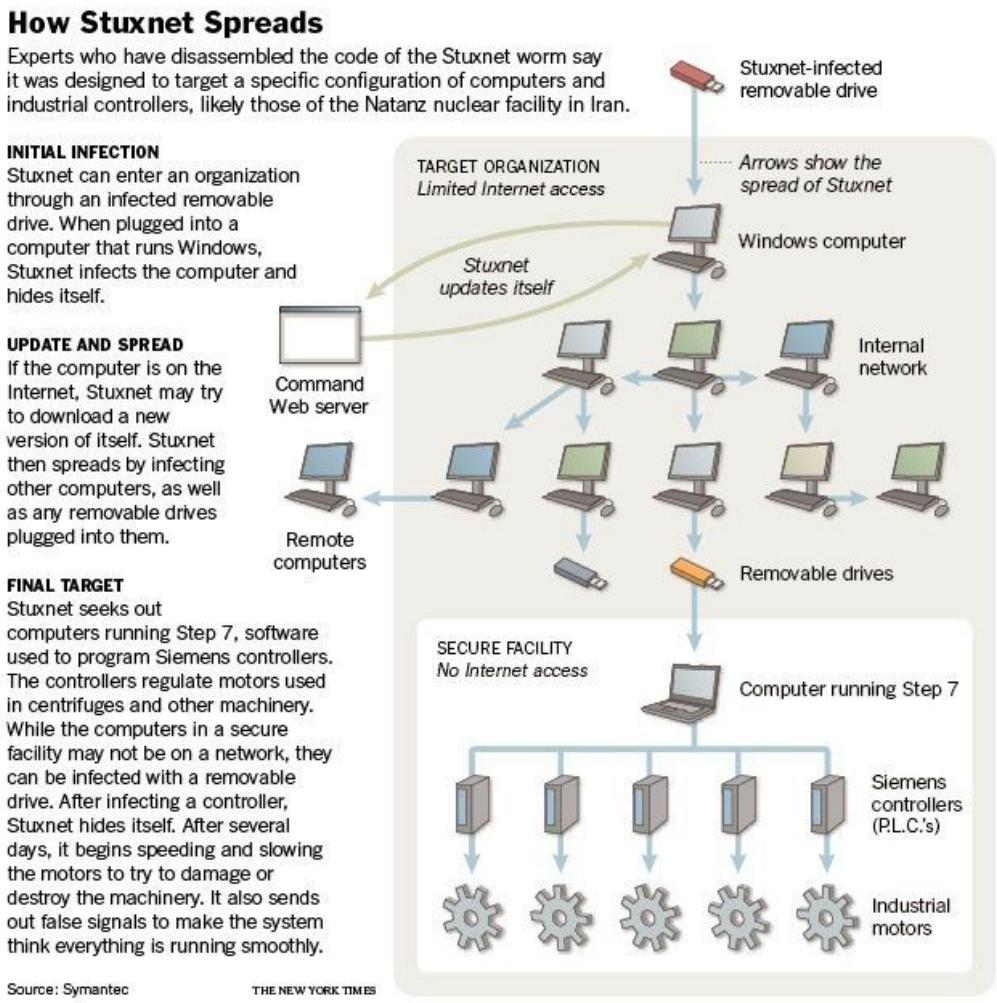
The biggest single factor in putting time on the nuclear clock appears to be Stuxnet, the most sophisticated cyberweapon ever deployed.

In interviews over the past three months in the United States and Europe, experts who have picked apart the computer worm describe it as far more complex — and ingenious — than anything they had imagined when it began circulating around the world, unexplained, in mid-2009.

Many mysteries remain, chief among them, exactly who constructed a computer worm that appears to have several authors on several continents. But the digital trail is littered with intriguing bits of evidence.

In early 2008 the German company Siemens cooperated with one of the United States' premier national laboratories, in Idaho, to identify the vulnerabilities of computer controllers that the company sells to operate industrial machinery around the world — and that American intelligence agencies have identified as key equipment in Iran's enrichment facilities.

Siemens says that program was part of routine efforts to secure its products against cyberattacks. Nonetheless, it gave the Idaho National Laboratory — which is part of the Energy Department, responsible for America's nuclear arms — the chance to identify well-hidden holes in the Siemens systems that were exploited the next year by Stuxnet.




President Mahmoud Ahmadinejad of Iran toured the Natanz plant in 2008.

The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart.

The attacks were not fully successful: Some parts of Iran's operations ground to a halt, while others survived, according to the reports of international nuclear inspectors. Nor is it clear the attacks are over: Some experts who have examined the code believe it contains the seeds for yet more versions and assaults.

"It's like a playbook," said Ralph Langner, an independent computer security expert in Hamburg, Germany, who was among the first to decode Stuxnet. "Anyone who looks at it carefully can build something like it." Mr. Langner is among the experts who expressed fear that the attack had legitimized a new form of industrial warfare, one to which the United States is also highly vulnerable.

Officially, neither American nor Israeli officials will even utter the name of the malicious computer program, much less describe any role in designing it.

But Israeli officials grin widely when asked about its effects. Mr. Obama's chief strategist for combating weapons of mass destruction, Gary Samore, sidestepped a Stuxnet question at a recent conference about Iran, but added with a smile: "I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated."

In recent days, American officials who spoke on the condition of anonymity have said in interviews that they believe Iran's setbacks have been underreported. That may explain why Mrs. Clinton provided her public assessment while traveling in the Middle East last week.

By the accounts of a number of computer scientists, nuclear enrichment experts and former officials, the covert race to create Stuxnet was a joint project between the Americans and the Israelis, with some help, knowing or unknowing, from the Germans and the British.

The project's political origins can be found in the last months of the Bush administration. In January 2009, The New York Times reported that Mr. Bush

authorized a covert program to undermine the electrical and computer systems around Natanz, Iran's major enrichment center. President Obama, first briefed on the program even before taking office, sped it up, according to officials familiar with the administration's Iran strategy. So did the Israelis, other officials said. Israel has long been seeking a way to cripple Iran's capability without triggering the opprobrium, or the war, that might follow an overt military strike of the kind they conducted against nuclear facilities in Iraq in 1981 and Syria in 2007.

Two years ago, when Israel still thought its only solution was a military one and approached Mr. Bush for the bunker-busting bombs and other equipment it believed it would need for an air attack, its officials told the White House that such a strike would set back Iran's programs by roughly three years. Its request was turned down.

Now, Mr. Dagan's statement suggests that Israel believes it has gained at least that much time, without mounting an attack. So does the Obama administration.

For years, Washington's approach to Tehran's program has been one of attempting "to put time on the clock," a senior administration official said, even while refusing to discuss Stuxnet. "And now, we have a bit more."

Finding Weaknesses

Paranoia helped, as it turns out.

Years before the worm hit Iran, Washington had become deeply worried about the vulnerability of the millions of computers that run everything in the United States from bank transactions to the power grid.

Computers known as controllers run all kinds of industrial machinery. By early 2008, the Department of Homeland Security had teamed up with the Idaho National Laboratory to study a widely used Siemens controller known as P.C.S.-7, for Process Control System 7. Its complex software, called Step 7, can run whole symphonies of industrial instruments, sensors and machines.

The vulnerability of the controller to cyberattack was an open secret. In July 2008, the Idaho lab and Siemens teamed up on a PowerPoint presentation on the controller's vulnerabilities that was made to a conference in Chicago at Navy Pier, a top tourist attraction.

"Goal is for attacker to gain control," the July paper said in describing the many kinds of maneuvers that could exploit system holes. The paper was 62 pages long, including pictures of the controllers as they were examined and tested in Idaho.

In a statement on Friday, the Idaho National Laboratory confirmed that it formed a partnership with Siemens but said it was one of many with manufacturers to identify cybervulnerabilities. It argued that the report did not detail specific flaws that attackers could exploit. But it also said it could not comment on the laboratory's classified missions, leaving unanswered the question of whether it passed what it learned about the Siemens systems to other parts of the nation's intelligence apparatus.

The presentation at the Chicago conference, which recently disappeared from a Siemens Web site, never discussed specific places where the machines were used.

But Washington knew. The controllers were critical to operations at Natanz, a sprawling enrichment site in the desert. "If you look for the weak links in the system," said one former American official, "this one jumps out."

Controllers, and the electrical regulators they run, became a focus of sanctions efforts. The trove of State Department cables made public by WikiLeaks describes urgent efforts in April 2009 to stop a shipment of Siemens controllers, contained in 111 boxes at the port of Dubai, in the United Arab Emirates. They were headed for Iran, one cable said, and were meant to control "uranium enrichment cascades" — the term for groups of spinning centrifuges.

Subsequent cables showed that the United Arab Emirates blocked the transfer of the Siemens computers across the Strait of Hormuz to Bandar Abbas, a major Iranian port.

Only months later, in June, Stuxnet began to pop up around the globe. The Symantec Corporation, a maker of computer security software and services based in Silicon Valley, snared it in a global malware collection system. The worm hit primarily inside Iran, Symantec reported, but also in time appeared in India, Indonesia and other countries.

But unlike most malware, it seemed to be doing little harm. It did not slow computer networks or wreak general havoc.

That deepened the mystery.

A 'Dual Warhead'

No one was more intrigued than Mr. Langner, a former psychologist who runs a small computer security company in a suburb of Hamburg. Eager to design protective software for his clients, he had his five employees focus on picking apart the code and running it on the series of Siemens controllers neatly stacked in racks, their lights blinking.

He quickly discovered that the worm only kicked into gear when it detected the presence of a specific configuration of controllers, running a set of processes that appear to exist only in a centrifuge plant. "The attackers took great care to make sure that only their designated targets were hit," he said. "It was a marksman's job."

For example, one small section of the code appears designed to send commands to 984 machines linked together.

Curiously, when international inspectors visited Natanz in late 2009, they found that the Iranians had taken out of service a total of exactly 984 machines that had been running the previous summer.

But as Mr. Langner kept peeling back the layers, he found more — what he calls the "dual warhead." One part of the program is designed to lie dormant for long periods, then speed up the machines so that the spinning rotors in the centrifuges wobble and then destroy themselves. Another part, called a "man in the middle" in the computer world, sends out those false sensor signals to make the system believe everything is running smoothly. That prevents a safety system from kicking in, which would shut down the plant before it could self-destruct.

"Code analysis makes it clear that Stuxnet is not about sending a message or proving a concept," Mr. Langner later wrote. "It is about destroying its targets with utmost determination in military style."

This was not the work of hackers, he quickly concluded. It had to be the work of someone who knew his way around the specific quirks of the Siemens controllers and had an intimate understanding of exactly how the Iranians had designed their enrichment operations.

In fact, the Americans and the Israelis had a pretty good idea.

Testing the Worm

Perhaps the most secretive part of the Stuxnet story centers on how the theory of cyberdestruction was tested on enrichment machines to make sure the malicious software did its intended job.

The account starts in the Netherlands. In the 1970s, the Dutch designed a tall, thin machine for enriching uranium. As is well known, A. Q. Khan, a Pakistani metallurgist working for the Dutch, stole the design and in 1976 fled to Pakistan.

The resulting machine, known as the P-1, for Pakistan's first-generation centrifuge, helped the country get the bomb. And when Dr. Khan later founded an atomic black market, he illegally sold P-1's to Iran, Libya, and North Korea.

The P-1 is more than six feet tall. Inside, a rotor of aluminum spins uranium gas to blinding speeds, slowly concentrating the rare part of the uranium that can fuel reactors and bombs.

How and when Israel obtained this kind of first-generation centrifuge remains unclear, whether from Europe, or the Khan network, or by other means. But nuclear experts agree that Dimona came to hold row upon row of spinning centrifuges.

"They've long been an important part of the complex," said Avner Cohen, author of "The Worst-Kept Secret" (2010), a book about the Israeli bomb program, and a senior fellow at the Monterey Institute of International Studies. He added that Israeli intelligence had asked retired senior Dimona personnel to help on the Iranian issue, and that some apparently came from the enrichment program.

"I have no specific knowledge," Dr. Cohen said of Israel and the Stuxnet worm. "But I see a strong Israeli signature and think that the centrifuge knowledge was critical."

Another clue involves the United States. It obtained a cache of P-1's after Libya gave up its nuclear program in late 2003, and the machines were sent to the Oak Ridge National Laboratory in Tennessee, another arm of the Energy Department.

By early 2004, a variety of federal and private nuclear experts assembled by the Central Intelligence Agency were calling for the United States to build a secret plant where scientists could set up the P-1's and study their vulnerabilities. "The notion of a test bed was really pushed," a participant at the C.I.A. meeting recalled.

The resulting plant, nuclear experts said last week, may also have played a role in Stuxnet testing.

But the United States and its allies ran into the same problem the Iranians have grappled with: the P-1 is a balky, badly designed machine. When the Tennessee laboratory shipped some of its P-1's to England, in hopes of working with the British on a program of general P-1 testing, they stumbled, according to nuclear experts.

"They failed hopelessly," one recalled, saying that the machines proved too crude and temperamental to spin properly.

Dr. Cohen said his sources told him that Israel succeeded — with great difficulty — in mastering the centrifuge technology. And the American expert in nuclear intelligence, who spoke on the condition of anonymity, said the Israelis used machines of the P-1 style to test the effectiveness of Stuxnet.

The expert added that Israel worked in collaboration with the United States in targeting Iran, but that Washington was eager for "plausible deniability."

In November, the Iranian president, Mahmoud Ahmadinejad, broke the country's silence about the worm's impact on its enrichment program, saying a cyberattack had caused "minor problems with some of our centrifuges." Fortunately, he added, "our experts discovered it."

The most detailed portrait of the damage comes from the Institute for Science and International Security, a private group in Washington. Last month, it issued a lengthy Stuxnet report that said Iran's P-1 machines at Natanz suffered a series of failures in mid- to late 2009 that culminated in technicians taking 984 machines out of action.

The report called the failures "a major problem" and identified Stuxnet as the likely culprit.

Stuxnet is not the only blow to Iran. Sanctions have hurt its effort to build more advanced (and less temperamental) centrifuges. And last January, and again in November, two scientists who were believed to be central to the nuclear program were killed in Tehran.

The man widely believed to be responsible for much of Iran's program, Mohsen Fakrizadeh, a college professor, has been hidden away by the Iranians, who know he is high on the target list.

Publicly, Israeli officials make no explicit ties between Stuxnet and Iran's problems. But in recent weeks, they have given revised and surprisingly upbeat assessments of Tehran's nuclear status.

"A number of technological challenges and difficulties" have beset Iran's program, Moshe Yaalon, Israel's minister of strategic affairs, told Israeli public radio late last month.

The troubles, he added, "have postponed the timetable."

15 February 2011 Last updated at 13:51 GMT

Stuxnet virus targets and spread revealed

By Jonathan Fildes Technology reporter, BBC News

Stuxnet may have been designed to target Iran's nuclear programme

A powerful internet worm repeatedly targeted five industrial facilities in Iran over 10 months, ongoing analysis by security researchers shows.

Stuxnet, which came to light in 2010, was the first-known virus specifically designed to target real-world infrastructure, such as power stations.

Security firm Symantec has now revealed how waves of new variants were launched at Iranian industrial facilities.

Some versions struck their targets within 12 hours of being written.

"We are trying to do some epidemiology," Orla Cox of Symantec told BBC News. "We are trying to understand how and why it spread."

Repeated attacks
The worm first grabbed headlines late last year after initial analysis showed that the sophisticated piece of malware had likely been written by a "nation state" to target Iran's nuclear programme, including the uranium enrichment centrifuges at the Natanz facility.

Russia's Nato ambassador recently said the virus "could lead to a new Chernobyl," referring to the 1986 nuclear accident.

Although speculation surrounds which countries may have been involved in its creation, the origins of the worm still remain a mystery.

Continue reading the main story

“Start Quote

One organisation was attacked three times, another was targeted twice”

End Quote Orla Cox Symantec
Iranian officials have admitted that the worm infected staff computers. However, they have repeatedly denied that the virus caused any major delays to its nuclear power programme, although its uranium enrichment programme is known to have suffered setbacks.

The new research, which analysed 12,000 infections collected by various anti-virus firms, shows that the worm targeted five "industrial processing" organisations in Iran.

"These were the seeds of all other infections," said Ms Cox.

The firm was able to identify the targets because Stuxnet collected information about each computer it infected, including its name, location and a time stamp of when it was compromised.

This allowed the researchers to track the spread of the virus.

Symantec declined to name the five organisations and would not confirm whether they had links to the country's nuclear programme.

However, Ms Cox, said that previous research confirmed that the worm could disrupt the centrifuges used to enrich uranium.

The five organisations were targeted repeatedly between June 2009 and April 2010, she said.

"One organisation was attacked three times, another was targeted twice," she said.

These waves of attacks used at least three different variants of the worm.

"We believe there was also a fourth one but we haven't seen it yet," she said.


The worm seeks out specific industrial hardware once inside an organisation
Analysis of the different strains and the time it took between the code being written and it making its first infection suggested that the virus writers had "infiltrated" targeted organisations, she said.

The researchers drew this conclusion because Stuxnet targeted industrial systems not usually connected to the internet for security reasons.

Instead, it infects Windows machines via USB keys - commonly used to move files around and usually plugged into a computer manually.

The virus therefore had to be seeded on to the organisation's internal networks by someone, either deliberately or accidentally.

The virus could have been spread between the organisations by contractors that worked for more than one of them, she said.

"We see threads to contractors used by these companies," she said. "We can see links between them."

Big picture
Once on a corporate network, the worm is designed to seek out a specific configuration of industrial control software made by Siemens.

The code can then reprogram so-called PLC (programmable logic control) software to give attached industrial machinery new instructions.

Previous analysis suggests that it targeted PLCs operating at frequencies between 807 and 1210Hz, a range that includes those used to control uranium enrichment centrifuges.

Subverting PLCs requires detailed knowledge and, although security researchers had raised concerns about exploits in the past, had not been seen before Stuxnet.

Ms Cox said the firm's analysis revealed incomplete code in Stuxnet that looked like it was intended to target another type of PLC.

"The fact that it is incomplete could tell us that [the virus writers] were successful in what they had done," she said.

The novelty of the virus, combined with attack mechanisms that targeted several previously unknown and unpatched vulnerabilities in Windows, have led

many to describe Stuxnet as "one of the most sophisticated pieces of malware ever".

However, research by Tom Parker from security firm Securicon says that elements of it were "not that advanced at all".

"I've compared this less advanced code to other malware and it does not score very highly," he said last year.

Ms Cox agrees that elements of the code and some of the techniques it uses are relatively simple. But, she says, that misses the bigger picture.

"If you look at the sum of its parts, then it is certainly very sophisticated," she said.