



February 15, 2011

Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report¹

By David Albright, Paul Brannan, and Christina Walrond

Overview

In the [December 22, 2010 ISIS report on Stuxnet](#), ISIS found that this malware contained important evidence indicating that its target was the IR-1 centrifuges at the Fuel Enrichment Plant (FEP) at Natanz. ISIS focused on the attack sequences generated by a Siemens S7-315 programmable logic controller (PLC) connected to frequency converters of a particular type. The ISIS analysis centered on the rotational frequencies listed in these detailed attack sequences. These frequencies matched, in two cases identically, key frequencies characteristic of the IR-1 centrifuge at the FEP.

A further analysis of another attack sequence has revealed that this code contains a description of what appears to be an exact copy of the IR-1 cascade at the FEP. The attack is titled “Sequence C” by Symantec, the computer security company that has conducted the most thorough and reliable open analysis of the malware’s code, or “417 code” after the advanced Siemens S7-417 programmable logic controller that Stuxnet targets.² However, the 417 code is not activated and thus unable to launch an attack.³ Moreover, key data is missing from the code available to Symantec that would define exactly what is affected or sabotaged.⁴ Symantec has assessed that the 417 code is likely unfinished, perhaps a work in progress.

Additional analysis also lends more support to the conclusion that the Stuxnet malware is aimed principally at destroying centrifuges, not manipulating parameters of the centrifuge cascades so as to lower the production of low enriched uranium (LEU) on a sustained basis. To date, Stuxnet is known to have had at least one successful attack. It is increasingly accepted that, in late 2009 or early 2010, Stuxnet destroyed about 1,000 IR-1 centrifuges out of about 9,000 deployed at the site. The effect of this attack was significant. It rattled the Iranians, who were unlikely to know what caused the breakage, delayed the expected expansion of the plant, and further consumed a limited supply of centrifuges to replace those destroyed. Nonetheless, Iran took steps in the aftermath of the attack that likely reduced further damage by Stuxnet, principally shutting down many centrifuge cascades for months. The shutdown lasted long enough for the malware to be discovered publicly, by which time Iran could have found Stuxnet on the Natanz control systems.

¹ David Albright, Paul Brannan, and Christina Walrond, [Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment](#), ISIS Report, December 22, 2010

² Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier version 1.4*, Symantec, February 2011.

³ *W32.Stuxnet Dossier*, op. cit.

⁴ Researchers are limited to studying the Stuxnet code that has emerged on the internet. It is possible that an older version of the code exists that is more complete than the available samples of Stuxnet. However, this older version would also likely be much less able to spread outside a targeted facility. In addition, the latest sample of the code is dated April 2010, so a later version could exist, although this too should have propagated widely.

Symantec has established that Stuxnet first infected four Iranian organizations in June and July 2009.⁵ After the 2009/2010 attack, and before Stuxnet's public discovery, the malware's operators tried to attack again. Symantec found that in March, April, and May 2010, two of the original organizations were again infected. In May, a new Iranian organization was also infected. Were the Stuxnet operators dissatisfied with destroying only 1,000 centrifuges, or were they encouraged by their success? In any case, they were improving the code's ability to spread by the spring of 2010, according to Symantec. These improvements undoubtedly sought to enable the program to again breach Iran's security on its gas centrifuge program and destroy more centrifuges.

Symantec has decided not to release the names of these organizations because of the company's privacy policies. But it characterized these companies as involved in industrial systems and work on "normal" industrial projects. A fraction of them deal with programmable logic controllers. Some are on lists of suspected violators of non-proliferation conditions and, by implication, involved in procuring for Iran's sanctioned programs. Natanz is not one of the first infected entities, given the number of initial infections. Kalaye Electric Company is also unlikely to be one of these companies. According to Symantec, none of the companies are publicly associated with Natanz and all the companies lack any publicly traceable history of being associated with Natanz. Therefore, the infection would have spread from these organizations to Natanz. To increase the chance of success, Stuxnet's creators appear to have targeted the domestic portion of Iran's supply chain for industrial control systems. Finding a way to infect systems in an Iranian supplier would be easier than doing so directly at the Natanz enrichment plant.

Because of sanctions and trade controls, Iran operates international smuggling rings to obtain industrial control equipment, including the Siemens 315 and 417 PLCs. Although foreign intelligence agencies could infect or sabotage these PLCs abroad, they would have far greater chance of ultimately infecting Natanz by inserting Stuxnet in the core of Iran's supply chain for the centrifuge program's control systems.

Contrary to several recent media reports, Stuxnet does not appear to be designed to attack the Bushehr nuclear power reactor. Stuxnet has spread easily on Windows-based computers, so it is not surprising that computers at other Iranian facilities, namely the Bushehr nuclear power reactor, would contain this malware. But the code's attack sequences do not appear targeted at a nuclear power reactor or its associated systems.

A cyberattack like Stuxnet is an uncharted method to damage and delay Iran's nuclear efforts. Without a diplomatic settlement with Iran, such attacks are likely to continue against Iran's centrifuge program. They provide an alternative to military strikes against Iran's known nuclear sites, a tactic that most see as likely to be ineffectual or counterproductive.

"War is ugly, awfully ugly," Israeli Deputy Prime Minister Dan Meridor recently told diplomats and journalists at the think tank Jerusalem Center for Public Affairs.⁶ He added that "the cyberworld...becomes more important in the conflict between nations. It is a new battleground, if you like, not with guns but with something else," he said. It is strategy, he implied, that would be waged in secret by intelligence agencies. Thus, more attacks can be expected in the future. Governments are likely to increase their offensive and defensive cyberwar capabilities.

But nations need to pause before diving into cyberwar against nuclear facilities. Stuxnet is now a model code for all to copy and modify to attack other industrial targets. Its discovery likely increased the risk of similar cyber attacks against the United States and its allies. While it has delayed the Iranian centrifuge program at the Natanz plant in 2010 and contributed to slowing its expansion, it did not stop it or even delay the continued buildup of LEU. A much broader debate, involving the public, needs to weigh the pros and cons of developing this new type of warfare.

⁵ W32.Stuxnet Dossier, op. cit.

⁶ Dan Williams, "Israeli official sees cyber alternative to 'ugly war,'" Reuters. February 3, 2011.

New Findings and Updates to December ISIS Report

New Information on 2009/2010 Attack on Natanz

ISIS published in its December 22, 2010 report⁷ that Stuxnet may have destroyed about 1,000 centrifuges at the Natanz Fuel Enrichment Plant in late 2009 or early 2010. Since this report, more information has emerged that increases the likelihood that the part of Stuxnet centered on Siemens S7-315 programmable logic controllers caused this damage. However, the relatively limited damage implies that destroying centrifuges through a cyberattack may be more difficult to do than commonly perceived.

The Washington Post has learned new important information supporting Stuxnet as the cause of the damaged IR-1 centrifuges, which Iran removed over the course of a few weeks. Moreover, the numbers removed were over and above the normal failure rate, which occurs at a rate of 10 percent per year.

The International Atomic Energy Agency (IAEA) cannot determine conclusively the origin of a decommissioned centrifuge at the FEP, although it is better able to establish the number removed from the cascade areas. In August 2009, the IAEA stepped up its surveillance at the FEP to better ensure that Iran could not remove equipment in or out of the cascades without IAEA verification, perhaps undermining the inspections.⁸ As a result, Iran agreed to allow the IAEA to enhance its camera surveillance of the cascade areas and retain all items taken from the cascades at a central location until IAEA inspectors could view them. In practice, about every few weeks, IAEA inspectors verify and count the items that left the cascade area. Thus, the IAEA has a relatively accurate count of the number of centrifuges removed from the cascade areas of the FEP. However, the IAEA does not receive information about the original locations of the removed centrifuges. The IAEA cannot therefore determine from which cascade, or module, the decommissioned centrifuges originated. In addition, IAEA surveillance cameras control only the perimeter of the cascade areas, so inspectors do not see the replacement of the centrifuges.

According to The Washington Post, Iran tried to downplay the significance of the removal of so many centrifuges. It told inspectors that the removed centrifuges were undergoing maintenance and originated in module A28, which contained centrifuges not yet under vacuum or spinning (see table 1). IAEA inspectors did not believe the Iranians, independently assessing that the centrifuges were likely already spinning and damaged beyond repair, according to officials close to the IAEA. Adding to suspicions about Iran's story, the inspectors witnessed Iran moving quickly to replace all these broken centrifuges, something Iran is less prone to do for non-spinning centrifuges in module A28.

The data in the IAEA safeguards reports suggests that the broken centrifuges actually came from cascades in module A26 that were spinning but not enriching.⁹ During this period, Iran took eleven non-enriching A26 cascades off-line and kept them off-line for several months (see table 1). As of August 2010, six of these cascades were still off-line.

However, decommissioned centrifuges could have also originated in the enriching cascades in module A26, if they were quickly replaced. Because the production of LEU increased during the late fall 2009 and early 2010, it is doubtful that 1,000 out of almost 4,000 enriching centrifuges at the FEP were out of service for long. Stuxnet does not appear to have attacked module A24, which is responsible for the vast bulk of LEU produced at Natanz.

⁷ David Albright, Paul Brannan, and Christina Walrond, [Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment](#), ISIS Report, December 22, 2010

⁸ The strengthened safeguards followed an episode in the spring of 2009, when the IAEA noticed substantial removal of equipment from the cascade area.

⁹ See ISIS December 22 report.

Media reports have stated that Stuxnet destroyed all the centrifuges in six cascades, or 984 centrifuges. However, Iran has not provided such a number, and the IAEA does not appear to be able to make such a precise estimate. Some centrifuges have entered and left the cascade area without the inspectors' knowledge, according to senior officials close to the IAEA, complicating any IAEA effort to determine a precise number. Nonetheless, this value is plausible since it is close to the actual number destroyed. Yet, the number of cascades controlled by a S7-315 PLC remains unclear.¹⁰ The 417 code is more explicit in establishing that each S7-417 PLC may control six cascades, for a total of 984 centrifuges. However, this code is not active and thus would not be expected to have caused the damage at Natanz.

Because the launch of the Stuxnet attack in Iran started in June and July 2009, an attack at Natanz prior to late 2009 cannot be excluded, but it appears unlikely. If an earlier attack on the FEP succeeded in destroying a large number of centrifuges, Iran would have needed to remove the centrifuges without the knowledge of the IAEA. This is unlikely, because the IAEA's bolstered inspection capabilities instituted in early August 2009 were aimed specifically at more accurately determining the number and type of items leaving the cascade area.

Impact of Stuxnet. At the time of the attack, the Natanz FEP contained a total of almost 9,000 IR-1 centrifuges. The destruction of 1,000 out of 9,000 centrifuges may not appear significant, particularly since Iran took steps to maintain and increase its LEU production rates during this same period. However, the IAEA safeguards data (see table 1) support that the attack delayed Iran from expanding the number of enriching centrifuges, in essence keeping large sections of the plant idle for many months.

[Iran is also facing shortages of raw materials to build IR-1 centrifuges.](#) It may have the materials to build only 12,000 to 15,000 IR-1 centrifuges. With 9,000 centrifuges already deployed at Natanz, and an estimated 1,000 centrifuges broken during routine operation, adding in the 1,000 centrifuges destroyed by Stuxnet brings the total to 11,000 centrifuges deployed over the lifetime of the FEP.¹¹ Iran may be approaching a limit on the number of IR-1 centrifuges it can build, making those destroyed by Stuxnet more significant than the number would imply.

There are also other, less tangible deleterious effects. To the extent it did not know what caused the destruction, Iran would have faced multiple questions about its centrifuge operations. In particular, a failure of this magnitude would have been a direct challenge to the program's quality assurance program, which is fundamental to successfully operating these high-precision machines. Iran has spent considerable effort in creating a reliable quality assurance program, where specialists carefully test each centrifuge component looking for out-of-spec parts. Without knowing the cause was malware, Iran would have struggled to understand this failure and likely would have lost valuable time worrying about more failures.

¹⁰ A S7-315 PLC controls six communication modules, each of which in turn controls up to 31 peripherals, for a total of 186 items, according to Symantec. Thus, each communication module may in theory control one cascade, and therefore a single S7-315 PLC could control six cascades. There is unlikely to be many frequency converters per cascade. Each cascade needs only a handful of frequency converters that can raise and lower the frequency of rotation of the centrifuges. However, it is also possible that one S7-315 controls only one cascade and the six communication modules are needed to control a variety of frequency converters and associated equipment that controls each of the 164 centrifuges. For example, the communication modules may also control additional frequency converter drives or related equipment that take over for the main frequency converters once at the desired operating frequency and provide sufficient power to the centrifuges to keep them running. In addition, in case of a centrifuge breaking, there should be a way to turn off the power to that individual centrifuge. This may require additional peripherals that lead to one S7-315 for each cascade.

¹¹ This value is derived from the failure rate of the IR-1 centrifuges, which is reportedly 10 percent per year. The failures occur mainly because of the difficulty of operating aluminum-based P1 centrifuges, the design which Iran obtained from the Khan network.

Once Iran learned of the reason for the failure of so many centrifuges, it must have felt a heightened sense of vulnerability to outside attack. The immense detail in Stuxnet about the Natanz enrichment plant must have also unsettled the Iranians, as it demonstrated that foreign intelligence agencies had learned a considerable amount of information about their secret operations, far beyond what the IAEA knew. Only an insider could have obtained so much detail. One official at a Western intelligence agency said that since outsiders knew so much about Natanz, Iran would tend to hesitate about building a secret centrifuge plant out of fear of getting caught. That fear was already magnified after Western intelligence agencies exposed the secret gas centrifuge plant near the holy city of Qom in October 2009.

Iran must also feel less secure about the goods its smuggling networks acquire abroad for its nuclear programs. It may need to resort to relying more heavily on reverse engineering and domestic production of a greater variety of advanced industrial goods for its centrifuge program. However, Iran has limited advanced industrial capabilities and has encountered difficulties in successfully reverse engineering equipment and technology. Thus, such a strategy would cause delays in its centrifuge program and require Iran to use goods of far less quality that are more prone to failure.

New Finding: Evidence of Targeting Natanz in Sequence C or 417 Code

Soon after the publication of the ISIS December 22 report, Ralph Langner, a German security expert, contacted ISIS after noticing that each of the Natanz centrifuge cascades contained 164 centrifuges. He said that the 417 code, or sequence C, is grouped in six arrays of 164 units each, perhaps representing six cascades, each with 164 centrifuges.

Based on Symantec's analysis of this array, ISIS discovered that this array is identical to an IR-1 centrifuge cascade at the FEP. This evidence is perhaps the strongest evidence that Stuxnet is aimed at Natanz.

This attack sequence targets a Siemens S7-417 programmable logic controller, which acts independently of the attack sequences targeting a Siemens S7-315 PLC, the focus of ISIS's December 22, 2010 report.¹² However, Symantec has determined that the 417 code is disabled and not able to infect S7-417 PLCs.¹³

Sequence C is also missing key code, including a block of data that would change the behavior of the centrifuges.¹⁴ As a result, the code does not reveal what is sabotaged and how the attack progresses.

The attack would last about seven minutes and repeat about every 35 days.¹⁵ Unlike the 315 code, the 417 code orders few checks of specific operational constants before launching an attack. But like the 315 code, the 417 code would also send false data to the operator's consoles during the attack, masking its sabotage.

The code describes six arrays of 164 objects organized into 15 clusters. Table 2, derived by Symantec from the 417 code, summarizes this information. The 15 clusters are numbered from 0 to 14, and the table lists the number of objects in each cluster.

This array corresponds exactly to the design of the IR-1 centrifuge cascades at the Natanz plant, according to senior officials close to the IAEA (see table 3). The only difference is that authors of the code started their numbering of the stages at the product end of the cascade, which has no special significance since an array does not have an implicit direction. The product stage is cluster 0, the feed stage is cluster 9, and the waste stage is cluster 14.

A reasonable interpretation is that each S7-417 PLC would control six cascades, each with 164 centrifuges. So, a module of 18 cascades would require three such controllers. In an attack, Stuxnet should be able to attack all the cascades operated by these controllers.

Table 2 also shows the number of objects in each cluster that would be affected, if the code were active. The attack appears to start at the product end of the cascade and work its way down the stages of the cascade, skipping the centrifuges in the feed stage. In total, 110 out of 164 centrifuges would be affected.

But with key data missing, one can only speculate about what the 417 code aims to sabotage. According to Symantec, the data sent to the cascades appear more aimed at flipping a series of on/off values rather than sending a packet of commands like the 315 code sends to frequency converters.

¹² *W32.Stuxnet Dossier*, op. cit.

¹³ *W32.Stuxnet Dossier*, op. cit and Symantec private communication. Stuxnet is a Windows binary that self-propagates on Windows and then adds to or modifies the computer programs on programmable logic controllers. The PLC code does not have the capability to self-replicate or spread the computer code. What makes 417 code inactive is that the Windows code does not inject it properly, e.g. no modification of OB1 and the missing DB8061.

¹⁴ This data would be in DB8061, which Stuxnet does not create, private communication from Symantec.

¹⁵ Symantec, private communication.

Because the code has correctly characterized the cascade by stage (cluster number) and the number of centrifuges per stage, the target is likely the centrifuges and not the cascade itself. In that case, one obvious target is the valves of the centrifuges. Other possibilities exist, such as changing the temperature of a centrifuge or affecting the pressure sensors in a cascade. But such attacks would be unlikely to have a significant impact on the centrifuges, particularly since after the attack is over, the operator would resume control of the cascades.

The valves play an essential role in the safety system of a cascade, stopping gas flow to a malfunctioning centrifuge and isolating it before their damage can spread to neighbors.¹⁶ They are also a key part of the system to evacuate uranium hexafluoride from the cascade in an emergency. But by closing these valves unexpectedly, the 417 code could damage the centrifuges.

Closing all the Fast-Acting Valves. Each centrifuge has three fast acting valves, one each on the feed, product, and waste tubes attached to the top of the centrifuge. If all three fast-acting valves were the target, closing all the valves on 110 centrifuges would cause the feed gas to bypass each of these centrifuges.

If the feed gas is blocked from going into the affected centrifuges, it will redistribute itself into other centrifuges. The rate of feed in the other centrifuges in the cascade would increase, building up the gas pressure at the wall of the rotor. Above a certain pressure, the feed gas would solidify, which could imbalance the rotor, causing it to fail. This could result in destruction of up to 54 out of 164 centrifuges in each affected cascade.

In this scenario, the attacker would want to delay any safety systems that could automatically cut off the flow of the feed gas into the cascades. That could explain why the centrifuges in the feed stage are not affected. In addition, the feed stage may have additional sensors not connected to the S7-417 PLC, which could, in the event of a malfunction, quickly stop the feed flowing to the cascade, undermining the attack.

The 417 code sends false data to the operator during the attack that would effectively blind them to changes mandated by Stuxnet's attack sequences. Plant personnel in the cascade area may hear centrifuges breaking, but the attack is so short that the operator is unlikely to have time to enact countermeasures.

During this attack, the enrichment product would be affected but only briefly. There would be reduced production of LEU since two-thirds of the centrifuges would be isolated from the cascade. The enrichment level of the LEU would be significantly reduced. The centrifuges in the upper two stages raise the enrichment level significantly but they would all be isolated. However, this effect would be temporary and minimal, since the attack lasts only seven minutes. The primary effect would be damaged centrifuges. Afterwards, the operators would resume control of the centrifuge cascades and learn of the closed valves.¹⁷

¹⁶ Valves are also used to assist in a sudden loss of the power to a centrifuge motor. In this case, the centrifuge starts to run down, and the pressure in the center of the rotor will increase, causing instabilities that can crash the centrifuge. The safety system will shut off the feed to the cascade and quickly empty the cascade in order to reduce the pressure inside the rotor.

¹⁷ One anomaly in the FEP's operation is that the feed rate often suddenly decreases temporarily from an average of about 60-80 grams per hour of uranium hexafluoride per cascade. Iran has refused to discuss these effects. Perhaps, this effect is related to the frequent dumping of the uranium hexafluoride in the cascades and subsequent isolation of the cascade by cutting off the uranium hexafluoride feed, which in turn could reflect the routine breakage of centrifuges at a level of 10 percent a year. However, even if code 417 were active, it would be unlikely to have caused this phenomenon. It would more likely result from the myriad other problems affecting the IR-1 centrifuge cascades.

Closing a Subset of Valves. Another destructive procedure would be if code 417 shut off the valves to the product and waste tubes in centrifuges, but left open the feed valve, rapidly increasing the amount of gas inside the centrifuge. This would undoubtedly be catastrophic for the rotor. This attack could destroy as many as 104 centrifuges (no gas can pass to the top and bottom stages (see table 2)). Since a certain number of product and waste valves must remain unaffected to allow the gas to pass to the next stage, this approach could not destroy all the centrifuges in a cascade. However, it could destroy about double the number affected in the attack shutting all the fast-acting valves.

There are undoubtedly other options for the attack. Some have speculated that code 417 does not seek to destroy centrifuges but instead lowers and disrupts the output of enriched uranium on a sustained basis. It is unknown how this would be done. In any case, after the short attack sequence, the operator would regain control of the cascades and would detect any changes in the enrichment output at the product end of the cascade, leading to a search for the cause and remediation. It is far more likely that Stuxnet seeks to destroy centrifuges and disrupt operations in that matter.

Update on Nature of the 315 Code Attacks

The ISIS December 22 report left open the question of whether Stuxnet would successfully destroy most of the affected centrifuges in attack sequences A and B, which Symantec has identified as two distinct, but similar attack sequences that target Siemens S7-315 PLCs. They work by changing the speed of two types of frequency converters.¹⁸ These frequency converters in turn drive the motors of IR-1 centrifuges, which control the speed of the centrifuge rotor. Once in control, Stuxnet alternatively increases and decreases the speed of the centrifuge rotor. The attacks are short-lived, either 15 or 50 minutes, and recur about every month.

With additional analysis, ISIS has assessed that the first attack subsequence is sufficient to destroy most of the affected centrifuges simply by increasing rotor speed toward the burst frequency. Safety systems independent of Stuxnet are unlikely to be effective in preventing damage to the centrifuges. Thus, the limiting factor appears to be whether the control systems meet all the criteria to initiate an attack, including encountering the specific type of 315 PLC, the right communication module, and the requisite number of frequency converters of the correct manufacture.

The initial ISIS report focused on sequence A, which is an attack involving a preponderance of Finnish frequency converters and is far better understood than sequence B involving Iranian assembled frequency converters. In sequence A, there are two specific attacks that are separated by about a month. The first, called sequence one, would raise the speed of the centrifuge as high as a frequency of 1,410 hertz (Hz) during a 15 minute attack, before the malware returns the control system to normal operation. After waiting about 27 days, Stuxnet would launch attack sequence two. This attack would lower the frequency only a few hundred hertz during a 50-minute attack. Then it would raise the frequency back to the nominal IR-1 centrifuge frequency of 1,064 Hz. After another 27 days, the first attack sequence would start again; followed by the second sequence 27 days after that, and so on.

The code of attack sequence one, which raises the speed, does not give the starting frequency, but a reasonable assumption is that it is between 1,007 Hz and 1,064 Hz.¹⁹ After 15 minutes, the frequency would reach nearly 1,325-1,380 Hz, respectively. These frequencies imply a fast rotor speed, but they are below the maximum frequency of 1,410 Hz, which corresponds to the burst frequency for this aluminum rotor where the aluminum simply fails from rotational acceleration. Will the rotors nonetheless break? The answer is likely yes.

¹⁸ W32.Stuxnet Dossier, op. cit.

¹⁹ ISIS December 22 report.

The ISIS December 22 report conjectured that each of four high-strength rotor tubes in a rotor assembly would experience a flexural critical resonance before reaching the burst frequency of about 1,410 Hz. (A rotor assembly comprises four short aluminum tubes connected by three maraging steel bellows and a top and bottom aluminum end cap.) In practice, the rotor tubes would start to break well before reaching this critical frequency.²⁰ However, subsequent calculations show that the first flexural solid body resonance for each tube exceeds the burst frequency and is in fact greater than 2,000 Hz.²¹ As a result, resonances will not break the centrifuges in their run up to 1,410 Hz.

However, when rotor speeds approach the maximum frequency, the rotor assembly will experience forces that will likely cause most of them to fail in any case. For example, at those high speeds, the mid-point of the top and bottom rotor tubes in an assembly expand outward. However, one end of each of these two rotor tubes has an end cap welded to it. The end caps, which are aluminum discs, resist expansion more than the tube itself, causing the rotor tube to form into a bottle shape, something that would likely break many of the tubes. The bearings will also be subjected to enormous stresses that could cause the rotor to break.

An attack by Stuxnet turns off the converters' warnings and alarms, and sends false data to the operators' computer terminals. As a result, the operators are unlikely to discover what is happening until it is too late. They may receive reports of centrifuges breaking in the cascade areas, but during the attack itself, the operators have no obvious way to wrest control of the frequency converters from Stuxnet.²² It is doubtful that any of the plant's safety systems can intervene in time to stop the destruction wrought by this particular attack sequence.²³ Thus, Stuxnet should destroy most of the affected rotors.

But that being said, what is the purpose of the second attack? It lowers the frequency only a few hundred hertz at best. Few centrifuges would break as a result, and enrichment levels would be affected only during the attack, which lasts just 50 minutes. Was this attack merely to sow confusion?

About a month later, the first attack sequence would repeat itself. Perhaps, multiple attacks are needed because the first attack to raise the frequency may abort, requiring another attempt. Or, the next attack may seek to damage any centrifuges that survived the first attack and any centrifuges installed to replace the broken ones.

Despite Stuxnet's sophistication, Iran appears to have taken a simple step that may have reduced the impact of a subsequent attack, assuming Iran had not yet discovered the malware on its controllers. It stopped the centrifuges in eleven cascades in module A26, the module that was likely most affected by Stuxnet. It kept them disconnected until late May 2010, when it started up six of those cascades (see table 1). Given that Stuxnet was publicly discovered in June 2010, Iran should have discovered the infection then, perhaps even earlier. Because a cascade needs to operate for at least two weeks before an attack starts against S7-315 PLCs,

²⁰ Typically, designers would want to keep the frequency at no more than 80 percent of this flexural frequency, or below about 1,130 Hz to avoid breakage.

²¹ Calculations were performed based on information in J.P. Den Hartog, *Mechanical Vibrations* (New York: Dover Publications, 1984); and S. Timoshenko, *Vibration Problems in Engineering* (New York: D. Van Nostrand Company, 1937).

²² Private communication from Symantec.

²³ The Stuxnet code does not appear to stop other safety systems from operating. For example, each IR-1 centrifuge has a vibration sensor that alarms when the vibration levels exceed some pre-determined level. A speed up would likely set these sensors off before the rotors break. Within milliseconds after an alarm, the control system would order the dumping of the uranium hexafluoride in an affected cascade. In expected emergencies, this action can resolve the excessive vibration problem. This dumping is accomplished by the closing of the three fast-acting valves on each centrifuge, the maintenance of the feed pressure, and the opening of a valve to allow the gas to leave the cascade and enter the dump tank. However, in a Stuxnet attack, the speed up would likely continue until the attack sequence ends. The dumping may still produce a benefit. With the uranium hexafluoride dumped from the cascades, some centrifuges may survive the speed up.

Stuxnet may not have had enough time to attack again after the restart of several cascades in module A26 in late May.

Six cascades in A26 that were enriching uranium remained operational in 2010 (see table 1). Perhaps these centrifuges either continued to be damaged or A24's control system was unaffected by Stuxnet.

Another Set of Attacks in Spring 2010

Symantec dates the initial infections of four Iranian organizations to June and July 2009. Symantec has identified fresh infections in March, April, and May 2010 on Iranian organizations, including two organizations attacked earlier and a new one.

Stuxnet's operators had modified the malware's code by the spring of 2010, apparently trying to attack Iran's gas centrifuge program again. According to Symantec, as of March 2010, Stuxnet operators had updated the code, making it spread more aggressively.²⁴ Once modified, the code would rapidly update older versions via network connections and Stuxnet's two dedicated command and control web sites in Denmark and Malaysia.

The collateral infections can be traced to the infection of these five organizations. Most of these infections, 12,000 of which Symantec tracked, resulted from the updated Stuxnet versions. It was likely the spread of Stuxnet from the spring 2010 infections that inevitably led to its public discovery.

Conclusion

Assuming Iran exercises caution, Stuxnet is unlikely to destroy more centrifuges at the Natanz plant. Iran likely cleaned the malware from its control systems. To prevent re-infection, Iran will have to exercise special caution since so many computers in Iran contain Stuxnet.

Although Stuxnet appears to be designed to destroy centrifuges at the Natanz facility, destruction was by no means total. Moreover, Stuxnet did not lower the production of LEU during 2010. LEU quantities could have certainly been greater, and Stuxnet could be an important part of the reason why they did not increase significantly. Nonetheless, there remain important questions about why Stuxnet destroyed only 1,000 centrifuges. One observation is that it may be harder to destroy centrifuges by use of cyber attacks than often believed.

The authors of Stuxnet remain unknown. This is one of the attractions of cyber attacks. The perpetrator can easily hide. Rumors and common sense point to a country or team of countries, but proving that they engineered Stuxnet remains almost impossible.

Stuxnet's elaborate nature and its updating show a firm determination to sabotage Iran's nuclear program. It is certain that foreign intelligence agencies will continue in their efforts to sabotage Iran's centrifuge program.

²⁴ W32.Stuxnet Dossier, op. cit., pp. 47-49.

Table 1: Number of Centrifuge Cascades enriching, under vacuum, installed, or with centrifuges disconnected, January 31, 2010

	Fed with UF ₆	Under Vacuum	Installed, not Under vacuum	With Centrifuges Disconnected	Total
Module A24					
Aug. 12, 2009	18	0	0	0	18
Nov. 2, 2009	18	0	0	0	18
Jan. 31, 2010	17	1	0	0	18
May 24, 2010	18	0	0	0	18
Aug. 28, 2010	17	0	1?	0	18
Module A26					
Aug. 12, 2009	10	8	0	0	18
Nov. 2, 2009	6	12	0	0	18
Jan. 31, 2010	6	1	0	11	18
May 24, 2010	6	7	0	5	18
Aug. 28, 2010	6	6	6	?	18
Module A28					
Aug. 12, 2009	0	0	14-15	0	14-15
Nov. 2, 2009	0	0	17 (1 being installed)	0	18
Jan. 31, 2010	0	0	16	2*	18
May 24, 2010	0	0	16	2?	18
Aug. 28, 2010	0	0	18	0	18

* In these two cascades in module A28, Iran had removed all the centrifuges in one cascade and was removing the ones in the other one.

Source: David Albright, Paul Brannan, and Christina Walrond, [Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment](#), ISIS Report, December 22, 2010.

Table 2: Code 417 Data for an Array of 164 Objects

Cluster Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Objects in the Cluster	2	2	4	6	8	10	12	16	20	24	20	16	12	8	4
Object Number	0-1	2-3	4-7	8-13	14-21	22-31	32-43	44-59	60-79	80-103	104-123	124-139	140-151	152-159	160-163
Objects affected	2	2	2	4	6	8	10	13	14	0	14	13	10	8	4

Source: Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier version 1.4*, Symantec, February 2011.

Table 3: Sequence C Array and FEP IR-1 Centrifuge Cascade

Cluster	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Stage	10E	9E	8E	7E	6E	5E	4E	3E	2E	1E	5S	4S	3S	2S	1S
No. of Centrifuges	2 (1+1)	2	4	6	8	10	12	16	20	24	20	16	12	8	4
	Product Stage									Feed Stage					Tails Stage

Notes and Comments:

- 1) Stage 10E, which is where the highest enrichment level is achieved, involves two centrifuges but this stage acts to all intents as ‘one plus a spare.’
- 2) The cascade shape is far from ideal because of the limited number of centrifuges in this cascade.
- 3) The number of stages is set by the required enrichment and depletion factors. They would be similar for any centrifuge that has an enrichment factor equal to the depletion factor. Thus, this cascade design is not unique to an IR-1 design but it is the basis for what Iran showed the IAEA in the Pilot Plant at Natanz in August 2003 and what Iran has installed underground in the FEP.