FUTURE
for Advanced Research & Studies

Artical Name : Stuxnet 2.0

Artical Subject : A hypothetical scenario for a cyber-attack on the Iranian nuclear program

Publish Date: 18/04/2021

Auther Name: Dr. Ehab Khalifa

Subject :

An Iranian official statement indicated that the uranium enrichment plant in Natanz was hit by a claimed “terrorist attack”, following the announcement of a power outage at the nuclear facility. On the other hand, Israeli intelligence sources reported that the Mossad was behind the attack. The incident at the Natanz facility occurred while Tehran and Washington are attempting to revive the 2015 nuclear deal, after former US President, Donald Trump, withdrew from it three years ago. However, under Biden's administration, Israeli Defense Minister Benny Gantz announced that Israel is seeking to put a military option on the negotiating table with Iran concerning its nuclear program, and that he is personally working on that. In this regard, it seems that the military option here was a cyber-attack.Targeting the Iranian nuclear program through a military cyber action came one day after Iran announced the launch of IR-9 systems, which are advanced centrifuges that enrich uranium more quickly. This quick and immediate response, once the new centrifuges were in place, is a clear message to Iran that Israel can penetrate the facility.On the evening of announcing the attacks on Natanz, the Israeli Prime Minister, Benjamin Netanyahu, responded that the current setting/ context of negotiations with Iran may not necessarily be available in the future, without any explicit reference to the cyber-attack on the Iranian nuclear facility. This may reflect an Israeli assessment of the huge losses that the facility has suffered.This analysis attempts to present a hypothetical scenario that demonstrates targeting the cyber-attacks on the Natanz facility, which may have relied on the second generation of the Stuxnet worm that hit the same facility in 2009, in addition to comparing the limits of both the Israeli and the Iranian cyber capabilities.A hypothetical scenario .. The second targeting of the Natanz facility:The magnitude of the losses resulting from the cyber-attacks targeting the Natanz facility are not clear yet. The Iranian Foreign Minister stated that there were no human casualties, no radiation leakage was detected. Yet, he declared that the electric power supplies feeding the new centrifuges were targeted, which resulted in the dysfunction of some of these devices. However, there are several indications that the losses are greater than what the Iranian Foreign Minister stated, which can be explained as per the following:The speed with which the new centrifuges were targeted as soon as they were set indicates that the Iranian nuclear program was already exposed to the Israelis, through one of two scenarios:1- First Scenario - Stuxnet: Targeting the control systems sets a hypothesis that the second generation of Stuxnet software, which may be connected to the Internet, has already been activated, and if it is not connected to the Internet, then at least there is a spy within the facility who gave orders for the activation of the program.2- Scenario Two - Zero day vulnerabilities: If not Stuxnet or one of the more sophisticated software, then at least there are zero-day vulnerabilities known to the Israelis within the industrial control systems of the nuclear facility, which were previously detected, identified and exploited in the recent attack.- Targeting electricity supply systems may lead to the dysfunction of a large number of centrifuges, and not a limited number as stated by the Iranian Foreign Minister.- A US intelligence source indicated that the attack on the Natanz facility may regress the Iranian nuclear program by 9 months.In all cases, the Iranian nuclear program is quite exposed to Israel, considering the speed of response and the magnitude of the losses incurred, which raises questions about the facility's cyber security capabilities.Israeli cyber capabilitiesIsrael has advanced capabilities in the field of cyber warfare, as it hosts major research centers for: Apple, Google, Microsoft, Amazon and Facebook, and gets 20% of global investments in cybersecurity. Furthermore, the Israel Defense Forces has Unit 8200, which is responsible for military operations in cyberspace.Unit 8200 of the Israeli Intelligence Corps, “Aman”, was established in 1952. It became responsible for leading the cyber warfare in the Israeli army, forming an alliance with the US National Security Agency (NSA) and the US Cyber Command. It is considered to be the largest Israeli electronic spy base in the Negev for bugging broadcast radio, phone calls, fax and e-mails in Asia, Africa and Europe. It was later upgraded to include war missions on cyberspace.This unit played a major role in attacking the Iranian nuclear program through the design of the Stuxnet virus. Amir Rapaport, the Israeli military commentator, confirmed that the role played by Unit 8200 has made Israel the second largest country globally in the field of bugging after the US. Rapoport indicated that the advanced computers of this unit are capable of monitoring messages of intelligence value by processing millions of communications and billions of words.Israel does not distinguish between cyber warfare and physical warfare. This means that hinting to a military use of force include the possibility of using cyber military force. For instance, Israel announced that it had launched a military attack on a building which it claimed was being used by a group of hackers who belong to Hamas, to launch cyber-attacks against Israeli targets, which have not been identified. Thus, this Israeli attack is considered to be the first military response to a cyber-attack in history.In the Iranian case, this was not the first incident targeting the Natanz facility. Iranian centrifuges were previously targeted by the Stuxnet worm, which caused the dysfunction of about a thousand centrifuges. Therefore, Stuxnet is the first model of using a cyber weapon to target the Iranian nuclear program. This was then considered one of the most dangerous types of cyber weapons developed, and was considered a paradigm shift in cyber wars. Through Stuxnet, war shifted from destroying and stealing data to destroying actual physical components and operating systems.Stuxnet was discovered in 2009, when it hit Iranian centrifuges at the Natanz facility. It caused the dysfunction of a large number of centrifuges, by targeting the operating systems that work through the SCADA control program, manufactured by Siemens. It recorded parameters related to the process of uranium enrichment, and then tampered with

and damaged the mechanism of operating the centrifuges. Stuxnet has the ability to reprogram the programmable logic controllers, to hide the changes that have been implemented and to display the old information on the screens so that things would appear to observers and technicians as proceeding normally, until the completion of the mission.Stuxnet generally attacks industrial control systems widely used in critical facilities, such as: Oil transmission lines, power plants, nuclear reactors and other critical and strategic facilities. It switches between devices via USB devices, exploiting one of the vulnerabilities in the Windows operating system.Furthermore, CNN quoted what Sean McGurk, head of the Internet Security Department at the US Department of Homeland Security, told the Senate Homeland Security Committee: “This code can automatically enter a system, steal the formula for the product you are manufacturing, alter the ingredients being mixed in your product, and indicate to the operator and your anti-virus software that everything is functioning as expected".Iranian cyber capabilitiesIran has paid great attention to enhancing its cyber capabilities. The financial resources allocated to enhancing its capabilities in this field have doubled. Iranian annual budget to develop its cyber capabilities was initially about USD 76 million. However, as of 2011, Iranian's expenditure has surpassed USD 1 billion, with the aim of acquiring cyber technology, infrastructure, and capacity building. In 2012, the IRGC claimed to have recruited about 120,000 people over the previous three years to work in this realm/ field.Regarding the assessment of Iran's cyber capabilities, there are conflicting estimates, as some overestimate Iran's cyber capabilities, and estimate that its power comes next to China, which is quite an exaggerated estimate. Other estimates classify it as a third-class cyber power, since it lacks advanced cyber capabilities owned by main actors in this field, such as the US, Russia, China and Israel.The conflicting assessments can be due to attributing some advanced cyber-attacks to Iran, while after a while, it has become clear that other countries stand behind that. One example is holding Iran responsible for employing malware that was found in Saudi petrochemical facilities, which targeted industrial control systems, which could have caused explosions in the facility. However, later, it became clear that this malware was linked to the Russian government. Thus, one can argue that Iran's cyber capabilities are not as advanced as the major powers, which is evident through some of the following indicators:1- The weakness of Iran's cyber defense capabilities: Iran's defensive cyber capabilities are suffering from major vulnerabilities, which is evident in its reliance on the use of its offensive capabilities in order to respond to the attacks it is subjected to. This was seen in the cyber-attacks on Saudi Aramco in 2012 and 2016, as well as the Qatari Ras Gas Company, in the same month, as a response to the cyber-attacks levelled against Tehran.2- The limited development of successive cyber-attacks: Iran's offensive cyber capabilities do not evolve greatly from one attack to another. Similar cyber tools have been used to attack Las Vegas Sands in 2014 and Saudi Arabia, two years later.3- The backwardness of Iran's cyber capabilities compared to the developed countries: Tracing Iranian cyber activities clearly reveals its lack of organization and the expected professionalism, which limits its capabilities to launch more complex cyber-attacks. It has not yet been able to penetrate any electric generator or control tools in the electricity networks, which reveals the lack of progress in its cyber capabilities in this respect.4- Iran's capabilities in espionage, disabling websites and services, and erasing data: It can be argued that Iran's strength in cyber capabilities revolves around 3 main points, which are:Espionage and Information Gathering: Particularly in the field of energy, as it mainly targets the US and attempts to steal American technologies to develop the Iranian nuclear and missile program. However, Iranian capabilities are still too weak to penetrate the US military defenses.Disruption of websites and services: By targeting government, service and military websites and attempting to disable them through attacks of denial of service to temporarily take the site out of work, change the interface of the website or the electronic account, and put slogans and statements in support of Iran.Sabotage and data erasure: Through this method, Iran targets the economic, industrial and energy sector in Saudi Arabia. This is the most dangerous aspect in the current Iranian capabilities, as it targets and sabotages vital sectors by erasing data, and not through the physical destruction so far.