Stuxnet, Flame, and Duqu - the OLYMPIC GAMES

Chris Morton[1]

Stuxnet emerged on the world stage in the summer of 2010 as the most sophisticated piece of malicious software ever found. Designed to permanently damage Iranian uranium enrichment gas centrifuges, Stuxnet represented a quantum leap in complexity and audacity in cyber conflict. Not only did the malware astonish researchers with its ability to penetrate and cripple a secretive regime's sensitive nuclear enrichment program, it also concerned security experts due to its brash destruction of part of a nation's critical infrastructure. With the emergence of the Duqu and Flame computer viruses, the revelation of a covert American cyber campaign (code-named OLYMPIC GAMES) against Iran, and the recognition of commonality between the three pieces of malware, Stuxnet became known as the centerpiece of a broader campaign, one that might hint at the future of warfare.

> *The appearance of Stuxnet was like the arrival of an F-35 into a World War I battlefield.*
>
> Ralph Langner, 2010

The target of the Stuxnet Worm was Iran's uranium enrichment program at the Natanz nuclear facility, or more specifically, Iran's uranium gas centrifuge tubes. Gas centrifuge tubes are used to enrich uranium, so that it may be used as a fuel for nuclear reactors. If refined highly enough, the uranium be can used in nuclear weapons. Stuxnet's payload only targets systems that meet very detailed specifications, those that perfectly match the gas centrifuges Iran uses at Natanz.

The malware operated for over a year at Natanz completely undetected, destroying gas centrifuge tubes, masking the damage it was causing, and sending data back to the plant operators and digital failsafe systems that the tubes were working perfectly. While sabotaging the enrichment process, Stuxnet was able to replicate itself throughout the system and evolve through updates pushed to it by servers located in two different countries.[2]

In November 2010, four months after the news of Stuxnet went public, the Iranian government acknowledged that a cyber attack damaged its uranium enrichment program at Natanz. In a press conference, Iranian President Mahmoud Ahmadinejad said that, "They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts."[3] The Iranian government seemed to downplay the impact Stuxnet had on their systems, but a public admission of interference was out of character for a government known for playing their nuclear program cards close to their chest.

Ultimately, Stuxnet rendered nearly 1,000 of the 9,000 IR-1 type gas centrifuges unusable at the Natanz uranium enrichment facility. While the computer virus did not cripple Iran's ability to enrich uranium, it is unclear how close Iran would be to producing a nuclear weapon without the Stuxnet infection.[4]

Geopolitical Context

On the international stage, Iran was perceived as a destabilizing force, accused of sponsoring terrorist organizations and developing nuclear weapons. Iranian President Mahmoud Ahmadinejad often stoked the fire of conflict, calling for the destruction of Israel, and even suggesting that eradication of the Jewish state was the solution to the Middle East Crisis.[5] Iran flaunted its nuclear technological advancements, claiming they were peaceful in nature, all the while shunning the International Atomic Energy Agency's (IAEA) attempts to inspect its facilities.[6]

As Iran sought to develop its nuclear technology, the United States and Israel were quite vocal in opposition to a nuclear Iran. In the face of this opposition, the United States was engaged in two counterinsurgency conflicts, draining resources and effort that might otherwise be used to curtail Iran's nuclear ambitions. Israel had strong motivation to oppose the development of the nuclear program in Iran, especially because Iran could use ballistic missile technology to strike Tel Aviv. But conventional military strikes, such as Israel's strike on Iraq's Osirak nuclear facility in 1981,[7] were not politically palatable to the United States. On a practical level, Israel would need approval from the United States to traverse Iraqi airspace, and they would require advanced weapons technology to damage the underground facilities.

Iran and Nuclear Weapons

Iran's pursuit of nuclear technology is not a recent development. In fact, it was the United States that gave Iran its first low-enriched uranium (LEU) for use as a research tool under the Atoms for Peace program during the Eisenhower administration. Through this program, the US Atomic Energy Commission leased Iran up to 13.2 pounds of uranium. In

[1] A 2011 graduate from Georgetown's Public Policy Institute, Chris Morton has spent the past twelve years in public service. His experience ranges from small group leadership to influencing policy at the strategic levels of government. He holds a Masters degree in Policy Management and a Bachelor of Science degree in Chemistry and Life Sciences from the United States Military Academy at West Point. Chris is originally from Muskogee, Oklahoma. The assertions, opinions, or assumptions expressed in this work are solely those of the author and do not reflect the position of any institutions or

[3] Clayton, "Stuxnet: Ahmadinejad Admits Cyberweapon Hit Iran Nuclear Program."

[4] Albright and Brannan, "IAEA Iran Safeguards."

exchange, Iran agreed to sign the Nuclear Non-Proliferation Treaty (NPT) and established the Tehran Nuclear Research Center.[8]

The United States felt that such a program would open Iranian doors to American commerce and entrepreneurs, while preventing Iran from undergoing its own domestic uranium enrichment research. By the 1970's, France and Germany joined the United States in partnership with the Iranian nuclear power program. Fears of impending energy shortages, combined with Iran's knowledge that their oil supply was limited, encouraged the Shah of Iran, Mohammed Reza Pahlavi, to seek nuclear power as an alternative to fossil fuels. Soon, Germany and France both signed agreements with Iran to assist in building nuclear power plants and to provide the enriched uranium that the plants required.[9] Iran was on its way to becoming a nuclear-powered state.

A 1974 Special National Intelligence Estimate on Nuclear Proliferation indicated that if Iran was able to create a fully sustainable nuclear power program, the Shah could easily decide to procure nuclear weapons. It stated in particular that, if India were to continue with weapons development, Iran would likely follow suit.[10] In May 1974, India detonated its first nuclear weapon.

Concerns about the future of nuclear weapons development led to Germany and France abandoning their plans to assist Iran in building its nuclear power plants. In March 1979, West Germany left the Bushehr nuclear reactor 85 percent complete. Following the Islamic Revolution and the severing of diplomatic ties between the United States and Iran, American leaders grew sour on the idea of supporting a nuclear program in Iran. Throughout the 1980's and 1990's, the United States continued their opposition to Iranian nuclear ambitions. Iran later contracted with Russia to assist in completing the Bushehr nuclear power plant, a project which the United States objected to until 2004. US diplomats changed the focus of their concerns from its nuclear power plants to its enrichment facilities, requesting that Iran answer to the United Nations Security Council.[11]

Please pay attention and understand that the people of Iran are brave enough that if it wants to build a bomb it will clearly announce it and build it and not be afraid of you.

Iranian President Ahmadinejad

In 2009, Iran developed the capability to obtain high-enriched uranium (HEU) through the gas centrifuge enrichment process at the Natanz facility. HEU is considered weapons-grade uranium, which is enriched to a point where it consists of 80 percent of the U-235 isotope. Commercial nuclear power reactors only require LEU, which is enriched to only 20 percent of U-235. While the IAEA attempted to conduct its inspections as authorized under the NPT, the Iranian government was less than transparent. Perhaps even more disturbing is that Iran developed a 40-megawatt research reactor capable of producing plutonium, a much more efficient fissionable material.[12] These developments have led many western nations, especially the United States and Israel, to condemn Iranian actions, push for sanctions through the United Nations, and make public statements rebuking Iranian nuclear ambitions.

The United States and Iran

The poor relationship between the United States and Iran grew from general discord after the overthrow of the Shah, Iran's monarch and pro-American dictator, into a rage during the hostage crisis of 1979. US President Jimmy Carter agreed to allow the Shah, who was hiding in Mexico following his ouster, to come to New York City for medical treatment of his lymphatic cancer. The Ayatullah Khomeini spurred on anti-American sentiment and called the embassy in Tehran a "nest of spies."[13] Soon thereafter, demonstrations turned into a hostage crisis, with the self-labeled "Students of Khomeini" holding 52 Americans captive, demanding that the United States return the Shah to Iran. The hostage crisis lasted over a year.[14]

Over the next two decades, tensions continued to mount. The United States backed Iraq during the eight-year Iran – Iraq war in the 1980's, when an Iraqi victory became doubtful. Iran responded with its support of radical Islamic terror organizations, such as Hamas and Hezbollah, further increasing tensions. Nation-state support of international terrorism took front stage following the terrorist attacks on the World Trade Center on 11 September 2011.

In his State of the Union Address in 2002, President George W. Bush declared Iran part of an "axis of evil," citing Iran's desires to pursue weapons of mass destruction and to export terror.[15] Part of the new, so-called Bush Doctrine was to not only go after terrorist organizations that posed a threat to the United States, but to also use force against the nations that harbored terror groups. The United States demonstrated its willingness to impose this doctrine through the invasion of Afghanistan and the deposition of its Taliban leadership. The subsequent 2003 invasion of Iraq left Iran with a sizable American military presence to its east and its west, leaving them isolated in the Middle East. In 2003, the Director of National Intelligence, Michael McConnell, said that there was "overwhelming evidence" that Iran was supporting insurgents in Iraq and "compelling" evidence that they

[8] Bruno, "Iran's Nuclear Program."

[12] Kessler, "Nuclear Nonproliferation – Does Iran Want a Nuclear Weapon?"

were doing the same in Afghanistan.[16]

Israel and Iran

As with the United States, outward Iranian dislike of Israel is in-part a byproduct of the overthrow of the Shah. In fact, Iran stayed out of the three Arab-Israeli wars that occurred during the time of the Shah. During the 1970's Arab oil embargo, Iran continued to supply Israel with oil. Iran enjoyed a partnership with Israel against the Sunni-Muslim Arab states. At the same time, Israel benefited from a partnership with Iran, along with the Christian portions of Lebanon and the more secular Turkey.[17] The past thirty years have seen a dramatic change in this relationship.

Current Iranian President Ahmadinejad has made hard-line comments toward the state of Israel, saying that Israel will soon "disappear off of the geographical scene" and should be "wiped off the map."[18] Coinciding with his statements, Iran developed advanced ballistic missile technology capable of reaching Israel. In September 2009, President Obama cited these new capabilities in reference to a European protective missile shield.[19] These new Iranian missiles, combined with their overtly aggressive statements against Israel, seem to position the two nations for a potential head-to-head conflict.

Israeli concerns about the Iranian nuclear program seemed to reach a crescendo in 2008. At the beginning of the year, Israel requested high-tech bunker-busting bombs from the United States, the sort that might destroy underground nuclear facilities. In addition, they sought refueling equipment that would allow their aircraft to reach the Iranian nuclear facilities. They then requested permission to traverse Iraqi airspace. A Pentagon analysis of an Israeli Air Force operation over the Mediterranean Sea in June of 2008 noted that the mission range matched the distance between Israel and the Natanz uranium enrichment facility.[20] Washington rebuffed all of the Israeli requests, while covert operations that the United States were pursuing seemed to satisfy the Jewish state.

Contextually, the Iranian pursuit of nuclear weapons, combined with their involvement in a proxy war against the United States in Afghanistan and Iraq, prepped the grounds for action. Iran's sharp anti-Semitic sentiment stoked Israeli fears that the Persian nation might move from simple financial support of groups like Hamas and Hezbollah to an outright nuclear attack. It seemed to be in the best interest of both the United States and Israel to slow or stop Iran's nuclear weapons ambitions. Conventional attack seemed politically risky, even though the IAEA and the United Nations condemned Iran's efforts

[16] McConnell, "McConnell Cites 'Overwhelming Evidence' of Iran's Support for Iraqi Insurgents."

[17] Weiss, "Israel and Iran: The Bonds that Tie Persians and Jews."

to keep their nuclear ambitions under wraps. The best answer might have rested in the dark recesses of cyber sabotage.

The Incident

Stuxnet was designed to destroy Iran's IR-1 centrifuges, rendering them useless for enriching uranium by speeding them up and slowing them down quickly, causing permanent vibrational damage. Damaging these tubes would not just delay the enrichment of uranium; it would also sew internal doubt as to the competence of the Iranian scientists. To accomplish its goal, Stuxnet employed the most sophisticated cyber attack methods seen at the time. It attacked several points of entry to the Natanz nuclear enrichment facility, employed a "dual-warhead" design to deliver its malicious software, and updated itself through peer-to-peer updates to evolve in changing conditions.

Stuxnet behaved like a lab rat that didn't like our cheese. It sniffed, but didn't want to eat. After we experimented with different flavors of cheese, I realized that this was a directed attack.

Ralph Langner

The Timeline

A Belarusian information technology company called VirusBlokAda discovered Stuxnet on 17 June 2010.[21] While troubleshooting a client's computer, employees discovered not just an encrypted virus using a zero-day vulnerability, but one which boasted a legitimate digital certificate. VirusBlokAda could not ignore the sophistication of the malware. The use of a zero-day vulnerability would permit the virus to gain access to the computer, and a digital certificate would convince the computer that the malware was a trusted piece of software. Therefore, during the first two weeks in July, the small IT company made public what it found.[22]

By 19 July 2010, the computer company Symantec reported that they were investigating malware that infected Siemens SCADA systems. It named the malware W32.Stuxnet, "Stuxnet" being an anagram created from the code of the software.[23] Over the next two months, Symantec conducted an extensive evaluation of the worm, attempting to understand its origin, methodology, and remaining threats. Not until 30 September did Symantec release a comprehensive analysis of the virus.[24]

During the year prior to the release of the Symantec report, problems with gas centrifuge tubes at the Natanz fuel enrichment facility were giving Iranian scientists fits. Until

[21] Gross, "Stuxnet Worm. A Declaration of Cyber-War."

November 2009, things were going smoothly. Then, the facility began having problems. While the detailed actions taken by Iranian scientists at the facility are unknown, by February 2010, Iran removed nearly 1,000 centrifuge tubes from its facility.[25] The number was 984, to be exact—a number frequently found in Stuxnet code.[26] This marked the end of the first version of Stuxnet, and of the first wave of the attack.

On 1 March 2010, the command and control domains pushed an updated version of its code to Stuxnet, creating the second wave of the attack. Only a month and a half later, on 14 April, a third wave was launched. Iran has revealed little evidence of the effects of the second and third waves of attacks.[27] Ostensibly, they were designed to overcome patches and defensive measures that Iranian scientists were able to employ to defeat the virus. They could also be modifications to change the direction of the attack.

One known late change in Stuxnet was its digital signature, that it used to mask its presence. When Symantec found that the malware was using a Realtek digital signature, it notified Realtek, who then revoked the signature. The command and control servers simply pushed a new authentic digital signature, this time held by JMicron, to the virus. This allowed the virus to avoid detection for a time, but by 14 July, when the new digital signature was issued, industry insiders became widely aware of the new threat. Symantec was able to identify this digital signature fairly quickly, and JMicron revoked its signature. A third signature was never sent. On 15 July, a distributed denial of service (DDoS) attack was launched against the websites that contained the mailing lists for two of the top newsletters for industrial control systems security. One of the sites was able to overcome the attack, but the other was shut down, preventing it from responding to requests for information on the new threat.[28]

In August 2010, the Iranians blocked all outbound traffic from infected sites to the command and control servers.[29] By November, the Iranians temporarily halted all enrichment activities at Natanz, perhaps to purge Stuxnet from all of its computer systems.[30] This is the same month that Ahmadinejad admitted that a computer virus infected Iranian nuclear fuel enrichment facilities.[31]

While Stuxnet seems to have only had disabling effects on gas centrifuge tubes at Natanz, it spread worldwide. As of September 2010, it infected over 100,000 hosts in 155 countries.[32] While this infection seemed to spread worldwide, its impact remained isolated in Iran. Iran eventually claimed to have purged its system of the computer virus. By September 2012, two years later, Stuxnet ceased to operate, either by its automatic encoded kill switch, or due to identification and removal tools provided by Symantec.[33] After the shroud was pulled back on Stuxnet in the fall of 2010, little was heard about the complex cyber weapon. Then, two seemingly related pieces of malware emerged–Duqu and Flame. These viruses, combined with the revelations of Stuxnet and of the US OLYMPIC GAMES cyber operation, suggested a multi-phased cyber campaign.

In June 2012, the *New York Times* reported that President Obama ordered the continuation of a complex Bush administration cyber operation against Iran, collectively known as OLYMPIC GAMES.[34] The *Times* citied as its sources current and former American, European, and Israeli officials involved with the program, as well as a number of subject matter experts.[35] OLYMPIC GAMES was a multi-pronged effort to sabotage Iran's nuclear enrichment program at Natanz. Reportedly, it was conceived collaboratively by a team established by then Vice Chairman of the Joint Chiefs of Staff General James Cartwright and the National Security Agency (NSA). According to the *Times*, an initial virus was dropped into the facility to provide a detailed schematic of the Natanz facilities. It then beamed that information back to the NSA, providing the needed intelligence to damage the facility.[36] The initial virus was likely the Flame or Duqu infection, or some combination of the two. Like a blind man describing an elephant, as more parts of the operation are found, Stuxnet's purpose in the context of that operation becomes more clear.

Discovered in October 2011, Duqu is a Remote Access Trojan (RAT), specifically designed to gather intelligence on industrial infrastructure and to acquire design documents, which might enable a future cyber attack against the systems. The RAT gleans its intelligence through executable files that gather system information and by recording computer keystrokes. Once Duqu steals data, it packages it into small files and exfiltrates the data out of the system. In addition, it seems that Duqu has the ability to hide small computer files from the system and disable a computer's security tools, such as antivirus software.[37] Duqu does not propagate as widely as Stuxnet, and it destroys itself after thirty days of functioning.[38] Despite the apparently different functions of Duqu and Stuxnet, two major attributes associate them: they share much of the same computer language in their programming, and they seem to target the Iranian nuclear program.

[25] Markhoff, "Malware Aimed at Iran Hit Five Sites, Report Says."

[26] Langner, "Ralph Langner: Cracking Stuxnet, a 21st-Century Cyber Weapon."

[27] Falliere, et al., "The Stuxnet Worm."

[28] Gross, "Stuxnet Worm. A Declaration of Cyber-War."

[29] Falliere, et al., "The Stuxnet Worm."

[33] "Siemens Industry Online Support"; and Jackson, "Stuxnet Shut Down by its Own Kill Switch."

[34] Sanger, "Obama Order Sped Up."

[35] *Ibid.*

Flame, announced to the world by Kaspersky Lab in May 2012, also serves to gather intelligence, but on a much grander scale. Twenty times larger than Stuxnet and more diverse than Duqu, Flame steals documents, takes screen shots from computers, records audio, and even accesses remote Bluetooth devices connected to computers to send and receive information.[39] Recording keystrokes as Duqu did is one thing, but turning on and off microphones, computer cameras, and even extracting a geolocation from an image was off the charts at the time in terms of sophistication. Furthermore, Flame operated undiscovered for more than two years before it was found and revealed in the spring of 2012.[40] It too shared lines of code with Stuxnet, making them brothers, or at least first cousins. Duqu and Flame could gather intelligence and disable security settings, enabling Stuxnet to do its damage.

The Anatomy of the Attack

Stuxnet's attack was simply a quantum leap in terms of the sophistication of its design and effects. Until 2010, most malware focused on other computers—either by overloading networks with DDOS attacks, such as occurred in Estonia during 2007, or by stealing data, such as the operation revealed in 2010 against the Defense Department, which began at the United States Central Command.[41] Stuxnet was different—it damaged infrastructure not directly connected to the Internet. In an interview in 2011, an official from the Department of Homeland Security lauded Stuxnet's elegance. He highlighted the malware's complexity and its ability to perform multiple phases of an attack—infiltration, assumption of control, surveillance, and finally the extraction or destruction of information, all without independent human control or commands.[42]

Upon analysis, researchers found that Stuxnet targets industrial control systems, rewriting the computer code on programmable logic controllers (PLCs), or more specifically, Siemens Supervisory and Control and Data Acquisitions (SCADA) systems. After changing the PLC software to direct industrial systems to operate in a manner that Stuxnet desires, it hides these changes from the operators of the industrial systems.[43] Stuxnet employed an unprecedented four Microsoft Windows vulnerabilities to gain control of the PLCs that dictate the speed at which IR-1 gas centrifuges spin. Once it gained authority over the tubes, Stuxnet sped them up and slowed them down, causing irreversible vibration damage. It also opened and closed valves between groups of centrifuge tubes, called cascades, either to confuse operators or to cause further damage. Once the centrifuges are damaged,

[39] Kaspersky Lab, "Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat."
[40] Nakashima, et al., "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say."

they become unusable and must be replaced in order for them to enrich uranium.[44] Simultaneously, the malware overrode automated system health indicator monitoring, giving operators indications of normal functioning tubes.[45]

Stuxnet employed a sophisticated dropper software package to deploy its payload. After the initial infection of a computer, Stuxnet went in search of Field Peripheral Gateways (PG). Field PGs are specialized computers that are generally used to control and configure PLCs. The virus would find the Field PGs through one of four methods: a. through a LAN, b. by way of a Windows zero-day vulnerability or a two-year-old unpatched vulnerability, c. through Step 7 projects, or d. through removable drives. Step 7 is the Siemens software that is used to program and configure that company's industrial control systems hardware.[46] Using Step 7 as a vector was especially important for Stuxnet, as the PLCs at Natanz used Siemens software. In addition, because Stuxnet inserted itself into Step 7 projects, cleaned computers would be reinfected with the malware through the hidden software in these project folders.[47]

Stuxnet employed two methods to control the targeted computers and to hide its presence. First, it used a rootkit dropper, which essentially lets the virus act as if it is the administrator of the system—giving Stuxnet persistent, unfettered access to its host.[48] Second, it employed an authentic digital signature to hide its heavily encrypted software, once it found its way to a host. Hackers have used fake digital signatures for some time, but Stuxnet used an actual signature stolen from Realtek, adding to its veracity.[49]

Infection through removable drives likely served as both the initial infection method and as a last hop to the Field PG computer. Normally, Field PGs are not connected to untrusted networks due to security concerns. Propagation through LANs served as intermediate steps, either from a computer that connected to a LAN containing systems with Step 7 projects, or to the Field PGs if they were ever connected to a network that Stuxnet managed to find.[50] Regardless of the method, the malware was constructed with multiple vectors in mind, all of which allowed it to find its way to computers that are normally not part of a network.

Once Stuxnet found its way to a Field PG computer, it then examined the PLCs that the Field PG controlled. It sought a PLC that controlled IR-1 type gas centrifuges, which were spinning at a specific rate. If Stuxnet was unable to find PLCs connected to the

[44] Barnes, "Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions."
[45] Falliere, et al., "The Stuxnet Worm."
[46] Keizer, "Stuxnet worm can re-infect scrubbed PCs."
[47] Falliere, et al., "The Stuxnet Worm."

Field PG that were running centrifuges with the appropriate configuration, it did nothing, laying dormant as a useless and harmless piece of hidden software.[51] If it found what it was looking for, it contacted home-base.

Stuxnet did not operate completely independently. It communicated with two command and control servers located in Malaysia and Denmark.[52] Stuxnet sent certain bits of information regarding the PLC configuration back to these command and control servers. These servers could then direct the virus to upload whatever code the server controllers wished. It also allowed for updates to Stuxnet, if configurations were changed to combat the infection. More uniquely, Stuxnet could update itself through peer-to-peer updates. If one version of Stuxnet came in contact with another, older version of the virus on another system, it would simply update the older version.[53] Stuxnet's ability to update remotely is the likely cause of its propagation beyond Natanz. US administration officials claimed that an overzealous Israeli update to the virus placed an error in the code, allowing Stuxnet to sneak onto an engineer's laptop when it was connected to the centrifuges. When that laptop was later connected to the Internet, Stuxnet broke free, spilling into an open, unsecure environment.[54] While posing little threat outside of Natanz, its veil of secrecy was gone.

PLCs do not use Windows as an operating system like the Field PGs, so the virus must use the configuring powers of the Field PGs to alter the software residing in the PLCs. The software that it uses to alter the PLCs is the payload of the malware. Ralph Langner, in a presentation at the Technology, Entertainment, and Design (TED) Conference in March of 2011 commented, "If you have heard that the dropper in Stuxnet is complex and high-tech, let me tell you this, the payload is rocket science."[55] The payload would write itself into the software of the PLCs that were controlling the gas centrifuges.

The payload itself consisted of a dual-warhead design. The first, smaller warhead was specifically designed to speed up and slow down individual gas centrifuges within a cascade. A cascade is a grouping of tubes, in the case of Iran's IR-1 tubes, 164 in number. The number 164 appears frequently in the code of the first warhead. The second warhead served to open and close valves connecting Natanz's six centrifuge cascades. Six cascades of 164 tubes totals 984 tubes, a number also frequently found within the code of Stuxnet.[56]

While the malware is speeding up and slowing down centrifuge tubes, it creates reality-blocking software for the operators of the fuel enrichment plant. Much like in Hollywood

[51] Gross, "Stuxnet Worm. A Declaration of Cyber-War."

[52] *Ibid.*

[53] Jackson, "Stuxnet Shut Down"; and Falliere, et al., "The Stuxnet Worm."

movies, it pre-records normal operating signals, then replays those signals while it is conducting its attack. This gives the operators no indication of any malfunction within the system. Furthermore, it overcomes the digital safety systems employed by the plant. Normally, when anomalies are detected, these automated systems react to prevent damage resulting from system malfunctions. Stuxnet feeds these systems false data, triggering no automatic response.[57]

Adversaries

The Stuxnet attack bears the marks of state involvement. First, the target of the assault seems to have been limited to the uranium enrichment facilities of Iran. While there are groups with motivation to undermine the proliferation of nuclear weapons, simply targeting Iranian gas centrifuge tubes would be a dramatic technological jump for activists, and it would not generate the same sort of publicity that other attacks or methods would bring. As activists rely on graphic images or acts that make a splash in the media, and do not favor subtle, complicated incursions, these attack methods seem not to be the work of activist perpetrators.

In addition, the Stuxnet Worm was specifically designed to attack Siemens-run PLCs, the sort that Iran uses in its enrichment facility. Knowledge of the industrial software that Siemens uses to control its logic controllers is something that would be difficult for the average non-state actor to obtain. Either industrial or nation-state sponsored espionage combined with highly technical engineering would be required to exploit this type of system. Not only is the worm huge, suggesting that it required several man-months of work, it is also highly sophisticated. Only governments wield the resources to produce such malware.[58]

Iran

As of 29 September 2010, Stuxnet infected approximately 100,000 hosts worldwide; of that number, nearly 60 percent were identified to be in Iran.[59] In response, Iran pointed the blame for the attack on the West, and more specifically, at Israel.[60]

Whatever precautions Iran had in place did little to stop the spread of the malware. Stuxnet primarily targeted facilities that would give it the best access to get at its final target. Security firms indicated that there were initially up to five different strains of the virus. These specifically looked for ways to infect systems that were not connected to the

[57] *Ibid.*

Internet. The virus did this through USB keys.[61] The scenario would be that contractors working at one of a number of infected facilities would transfer the malware from their computers to their USB sticks. Stuxnet would then wait for one of the contractors to plug a removable drive into a computer that is a part of the detached system which Stuxnet targeted. While Iran certainly had basic computer cyber defenses at the Natanz facility, its detachment from the Internet was its best defense. Stuxnet specifically targeted this attribute and had little trouble finding its target, despite Iranian cyber defenses.

In the end, Iran's weak information technology practices at its nuclear facilities and its lack of a stringent cyber defensive structure within its nuclear facility computer network contributed to the attack's success. Iran blamed the attack on Israel and the United States, mostly due to its political mistrust of the two countries rather than because of hard evidence. The private company Symantec conducted the most comprehensive study on the malware.[62] It has avoided outright attribution, but German security expert Ralph Langner revealed at the Long Beach Technology, Entertainment, and Design (TED) Conference that he believes that the Israeli Intelligence Agency Mossad and the United States together are behind the worm.[63] *The New York Times* later specifically attributed the malware to the US and Israel, and claimed this was a part of the OLYMPIC GAMES cyber operation.[64]

> *Iran's stance has always been clear on this ugly phenomenon [Israel]. We have repeatedly said that this cancerous tumor of a state should be removed from the region.*
>
> Ayatollah Ali Khamenei

Israel and the United States of America

Israel and the United States not only had the motivation to prevent Iran from obtaining highly enriched uranium; they also articulated their intent to prevent Iran from obtaining nuclear weapons. In January 2007, Nicholas Burns, the American Under-Secretary of State, indicated that, "Iran is seeking a nuclear weapon. There's no doubt about it." He further said that, "the policy of the United States is that we cannot allow Iran to become a nuclear state." Burns later commented that, "We are committed to our alliance with Israel. We are committed to being Israel's strongest security partner. I can't remember a time when the relationship between our two countries was stronger than it is today."[65] Mr. Burns made it clear that the United States sought to deny Iran nuclear weapons and that its partnership with Israel was of the utmost importance.

[61] Fildes, "Stuxnet virus targets and spread revealed."

[62] Falliere, et al, "The Stuxnet Worm."

In June 2009, the *New York Times* revealed that the United States had hung its hope of preventing the further development of a nuclear Iran on a covert program. After concluding that the sanctions had failed to prevent Iran from enriching uranium, the Bush administration struggled to find another method to intervene. Overt military action, such as the plan that Israel suggested, might ignite a regional conflict, and this was something that Washington desperately wanted to avoid, especially while fighting two wars in the Middle East. The covert operation was an experimental effort to undermine Iran's computers and networks, on which Iran relies to enrich uranium. Some dismissed the efforts as "science experiments," but others said that the covert operations were needed to dissuade Israel from bombing the facility. Secretary of Defense Robert Gates criticized the National Intelligence Estimate (NIE) released in 2007 for under-emphasizing the importance of Iranian enrichment activities.[66] This article reads like a blueprint for the decision to release a covert cyber attack against the Natanz nuclear facility. It was released in January 2009, a full eighteen months before the public or the media knew about Stuxnet.

While both the United States and Israel had the motivation to prevent nuclear advances in Iran, neither nation could accomplish such a feat alone. They would need each other. Richard Clarke, in his book *Cyber War*, asserts that Israeli cyber capabilities were placed on display during a September 2007 attack on secret Syrian nuclear facilities. The Israeli Air Force was able to strike the facility, despite Syria's significant investment of billions of dollars on a new air defense system. Instead of Syrian radar screens lighting up when sorties of F-16 Falcons and F-15 Eagles streaked across the night sky, they remained completely dark. Syrian air defenders were completely blind to the incident.[67]

Although Israel brought cyber expertise to the table, their most valuable asset was more likely their intelligence agency, Mossad. The US and Israel probably needed such an asset, not just to gather intelligence on Iranian facilities and officials, but to plant the virus into a closed computer system not connected to the Internet. Some evidence points to Mossad involvement. In early 2011, retiring Mossad Chief Meir Dagan told the Israeli Knesset that Iran had run into technical difficulties that would delay their construction of a bomb until 2015.[68] Dagan cited "measures that have been deployed against them" when discussing their technical difficulties.[69] Previous estimates of Iranian bomb construction time-frames estimated a date closer to March 2011. Finally, during the retirement of Israeli Defense Forces (IDF) Chief Lieutenant General Gabi Ashkenazi, a commemorative video seemed to allude to the Stuxnet attack while applauding his leadership.[70]

[66] Sanger, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site."

[67] Clarke and Knake, Cyber War, 5

Israel and the United States both had the ability to test a destructive tool like Stuxnet. In the 1970's, a Pakistani metallurgist, A.Q. Khan, stole the design for the P-1 uranium gas enrichment centrifuge tube from the Dutch (IR-1 centrifuges are the name given to the Iranian version of the same tube). After giving the plans to the Pakistani government, allowing them to go nuclear, he sold the designs on the black market to Libya, North Korea, and Iran. Many nuclear experts believe the secretive Israeli nuclear facility at Dimona houses P-1 gas centrifuges.[71]

I think on the offensive side, the U.S. government invented it [cyber war]. They are probably the best in the world.

Richard Clarke

While it is assumed that Israel possesses P-1 centrifuges, it is known that the United States does. In 2003, Libya abandoned its nuclear program, giving its nuclear enrichment equipment, including P-1 centrifuges, to the United States. They were sent to the Oak Ridge National Laboratory in Tennessee.[72]

In 2008, Siemens teamed up with the Idaho National Laboratory to study the Step-7 software on its programmable logic controllers. The goal of the study was to identify cyber security flaws that might be exploited in a future attack on systems in the United States.[73] The software is the same that Iran uses to control its nuclear enrichment gas centrifuge tubes – Siemens Step-7 software.

There are other pieces of circumstantial evidence pointing to US and Israeli involvement. One string of code in Stuxnet refers to 24 September 2007, the date that Iranian President Ahmadinejad questioned whether the holocaust actually happened.[74] There is also the presence of the file code Myrtus. Myrtus is sometimes an allusion to the biblical book of Esther, in which the Jews preempted a Persian plot to destroy them.[75]

Failsafe mechanisms in the virus, such as its customization to only target software designed to control centrifuge tubes and a "kill switch" that deactivates the virus in June 2012, seem to indicate a Western nation's involvement. Regarding the first of these mechanisms, the virus limits its own ability to spread. Each infected device may only spread Stuxnet to three other systems. This mechanism allows a moderate rate of infection, but does not permit the sort of uncontrolled propagation indicative of other worms. Stuxnet's spillage outside of Iranian systems seems to have been accidental, and due to an error in the code created during an update to the virus.[76] In addition, Stuxnet did not infect computers at

random. It only affected Siemens SCADA PLC software that matched a complex set of parameters. It would also only infect Windows computers that it believed were connected to these specific PLCs. If these parameters were not found, Stuxnet simply became an inert piece of software.[77] Finally, on 24 June 2012, all copies of the virus ceased to function, due to a command embedded deep in Stuxnet's code. Such efforts to minimize collateral damage and rates of infection indicated a more Western approach to the attack, because of the bureaucratic process that might be involved for approving the assault. In reference to Stuxnet, Richard Clarke commented that, "It just says lawyers all over it."[78] Few places have as many lawyers as the United States government.

In June 2012, the *New York Times* revealed that President Obama had issued an order for OLYMPIC GAMES to be sped up, in an attempt to thwart Iranian nuclear ambitions.[79] Another assertion in the *New York Times*, apparently leaked to them by a high ranking administration official, was that Israel and the National Security Agency (NSA) co-developed the complex virus, which required the expertise of both nations, as well as the sensitive intelligence gathered by Israel's Mossad. Ostensibly, OLYMPIC GAMES would delay Iran's enrichment of uranium, thereby precluding Israel's desire to conduct a conventional strike. The operation was seemingly successful, but the *New York Times* claimed that an Israeli update to the malware caused it to spill outside of Natanz, and thus reveal itself to the world.

Considering their adversarial stance against Iran, and their motives and capabilities to launch such a sophisticated attack, the United States and Israel are likely candidates as participants in the Stuxnet incident. In an interview in 2011, William Marshall, the Managing Director of the Chertoff Group, which is a global security consulting company, noted that non-state actors would not have the ability to bring together all of the elements required to produce Stuxnet—access to Microsoft source code, access to Siemens technology, nuclear engineering expertise, and critical intelligence about the Natanz enrichment facility.[80]

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.

Update of ISIS December 2010 Report

[71] Broad, et al., "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[72] *Ibid.*

[73] *Ibid.*

[77] Falliere, et al., "The Stuxnet Worm."

Finally, the lack of significant cyber defenses in the Iranian nuclear facility and the overwhelming strength of American and Israeli cyber offensive tools made Iran a fairly easy target for cyber sabotage. If this imbalance did not exist, the attack might not have been a suitable alternative to an overt kinetic strike.

Response

The government response from Iran occurred both in the technical and political arenas. The immediate response of attempting to identify, control, and eradicate Stuxnet occupied Iranian scientists for some time. Due to the secretive nature of the country, little is known about its inner workings. Politically, Iran has reacted toward the suspected authors of Stuxnet with the usual zeal that emanates from the isolated nation.

Through late summer and early fall, operations at Natanz seemed to be going as planned. The enrichment of uranium fuel and the installation of IR-1 centrifuges had constantly been increasing since the start of the program in 2007. In fact, by September of 2009, nearly 9,000 centrifuge tubes had been installed, and 4,000 of those had been fed with uranium hexafluoride gas. Then something happened. The number of tubes that Iran was installing leveled off, and by February 2010, they had removed nearly 1,000 centrifuge tubes. The number of tubes enriching uranium also stopped rising and leveled off. While Iran managed to install enough tubes to replace the damaged ones, significant growth in capacity did not occur.[81]

Based on these timelines, it seems that between the infections of the Iranian computers in the late summer of 2009 and November 2009, the Iranians were oblivious to what was happening to them and were not reacting. Sometime between November and February 2010, when it was confirmed that Iran removed the 1000 tubes, the country realized that something was causing these gas centrifuge tubes to break. It is unclear whether Iranian scientists thought this was due to the naturally high rate of failure of these types of tubes, or whether something else was causing the problems. At a minimum, Stuxnet was causing the Iranians to question their own competence.

With a rampant computer worm destroying their tubes, and their limited ability to acquire more due to the embargo, replacing these tubes with new ones would have been inadvisable. Between February 2010 and July 2010, when Symantec discovered the virus, it is unknown whether Iranian computer experts understood the problem. That they apparently did not is suggested by the fact that new centrifuge installation as well as utilization remained constant.[82] Likely, they were unwilling to move too quickly until they understood the full nature of their problem. Actual uranium enrichment did still seem to increase, probably because of increased production in their active tubes.

It is also unknown whether the Iranian government understood Stuxnet before the private sector. More likely than not, they spent the bulk of 2010 trying to eliminate Stuxnet from their system. It was not until August 2010 that they finally cut their outbound connections to the command and control servers.[83] While Iran may have eventually stifled the damaging effects of Stuxnet on their nuclear enrichment program, the Flame and Duqu viruses gave the Iranians plenty more to deal with, at least though the summer and fall of 2012.

Iran emphatically blamed Israel and the United States for Stuxnet. President Ahmadinejad's remarks failed to mention any particular country by name, but his anti-Israeli/US rhetoric pointed to those two countries. Ahmadinejad also seemed to downplay the effect of the cyber attack, noting that Iran had the situation under control.[84] With the revelation of Flame, Iran continued to point to Israel, highlighting Flame's similarities to other computer attacks that come from the Jewish State.[85]

Iran also publicly announced the expansion of its militia to include new cyber warriors. The group would be part of Basij, a volunteer military group that is organized within the Iranian Revolutionary Guards. Iranian news specifically mentioned that the unit was being set up to counter-attack those that launched cyber attacks at Iran.[86]

In March 2011, Iranian national news reported that their new cyber warriors in Basij had started operations. General Ali Fazli was quoted as saying, "[a]s there are cyber attacks on us, so is our cyber army of the Basij, which includes university instructors and students as well as clerics, attacking websites of the enemy."[87] Clearly, Iran wanted to flaunt its new capabilities, which are assuredly more complex and capable than what was revealed in public.

Eleven days after this announcement, Comodo, an Internet security group, accused Iran of launching attacks against Google, Microsoft, Yahoo, Mozilla, and Skype.[88] Comodo claimed that they had sold nine digital authentication certificates to fake websites. Their incident report indicated that the Iranian government might have used the certificates to redirect legitimate users of services such as Gmail to a fake site. This would allow the Iranian government to steal usernames and passwords, or install malware to monitor online activities.[89] This sort of activity might have also come from Iran's new cyber police, the creation of which Iran had announced in January 2011. That cyber police force was tasked

[83] Falliere, et al., "The Stuxnet Worm."
[84] Toor, "Ahmadinejad Says Iran's Nuclear Facilities Were Hit by Stuxnet Worm."
[85] Erdbrink, "Iran Confirms Attack by Virus That Collects Information."
[86] Fogarty, "Iran Responds to Stuxnet by Cyberwar Militia."

with monitoring so-called "foreign-inspired political dissent."[90]

Secretary of State Hillary Clinton and the Israeli Ministry of Defense have noted that Iran's ability to procure nuclear weapons was delayed. Israel indicated that Iran might not become a nuclear-armed state before 2015.[91] Other studies suggest that Stuxnet's effect on Iran's ability to enrich uranium, while problematic, was not catastrophic. The Institute for Science and International Security reported that, although the Iranians were rattled by this attack, their actions in removing the damaged tubes and slowing production likely mitigated further damage. The report also says that since Iran possesses 9000 tubes, the removal of 1000 of them, while damaging, was not ruinous. A larger issue for Iran is that it has a finite amount of material to make more centrifuges, which will eventually limit is ability to expand its program much beyond its 2011 capacity.[92]

Implications[93]

Stuxnet had short-term political effects on both the Iranian government and the potential authors of the malware, which has led to a new state-of-affairs in nation-state conflicts. Stuxnet could prove to be a great equalizer between world powers. If a country can deploy a few lines of computer code and have kinetic effect, countries might choose to stop maintaining their resource-heavy armed forces. BS

Iranian confidence was certainly shaken. Stuxnet revealed that they were terribly vulnerable to offensive cyber weapons, and that their secrets were not so secret. Some of the techniques employed by the virus required detailed understanding and knowledge of the inner workings of Natanz. This understanding was apparently obtained both through traditional spycraft by Mossad and the CIA, and by modern intelligence operations such as those exemplified by the Flame and Duqu computer viruses. One can imagine the initial paranoia that Iranian government officials experienced when they discovered that their enrichment program was not working properly for unknown reasons. The Iranians most certainly questioned their own ability to maintain an independent nuclear program.

If the destruction of the fuel enrichment plant had been complete, Iran would look different today. Instead, the country took steps that at least limited the damage. Now that Iran has been inoculated with one of the most innovative and capable pieces of malware of our time, they will be on the lookout for the next attack. In this sense, Stuxnet might not have been worth the cost for Israel and the United States. While fuel enrichment was set back, it still continued. Iran publicly acknowledged that it needed stronger cyber defenses, created a militia to conduct cyber operations, and obviously became sensitive to the possibility of further attacks.

Although it is not known with complete certainty that the United States and Israel were behind the attack, it matters not, as most experts agree it was them. The leak by unnamed US administration officials to the *New York Times* about the OLYMPIC GAMES cyber operation was not terribly helpful for an administration trying to maintain at least a shred of attribution ambiguity with respect to Stuxnet. The US and Israel have both revealed what a nation-state created cyber weapon looks like. In addition, they have signaled to the rest of the world what the norms can now be expected to be in this arena, by causing physical damage to another nation's critical infrastructure with a computer attack when faced with a perceived security threat. The toothpaste is out of the tube. William Marshall believes that this might be a blueprint of what is to come—malware intended to influence politics and advance agendas by controlling the cornerstone elements of an industrial civilization. These elements would include critical infrastructure, such as electricity and water distribution systems, financial markets, and transportation networks.[94] Despite Stuxnet's quiet death by self-eradication in June 2012, a message has been sent.

That message might not be all that bad. At the end of World War II, when the United States dropped two atomic weapons on Japan, it sought to end the war and prevent hundreds of thousands of casualties which a land invasion would certainly have caused. The decimation of Hiroshima and Nagasaki also gave the world an in-color, 3D view of American military might. Stuxnet, especially when viewed in the context of the OLYMPIC GAMES cyber operation, could have the same effect. Many in the press have touted the lack of cyber defensive capability and accompanying vulnerability of US critical infrastructure to attack. The message to potential adversaries seeking to exploit this capability could be, "Think twice before you attack us. This is a sample of what we can do. We will do it again." Deterrence

The most wide reaching implication of the Stuxnet attack stems not from the display of its dazzling engineering, but rather from the potential for reverse engineering. Ralph Langner warned at the TED Conference in 2011 that the problem with the malware is that it is generic.[95] It can be modified to attack any industrial control system. Stuxnet serves as a draft to create a cyber weapon with the capability to attack electrical power grids, oil refineries, nuclear power plants, or hazardous chemical plants. One can only imagine the widespread damages that might be caused by this tool if it fell into the hands of those not so concerned with collateral damage or targeted warfare. Ralph Langer called Stuxnet the first cyber weapon of mass destruction. If Stuxnet is only the beginning of what Albert Einstein predicted concerning World War III, we should start to gather those sticks and stones.

[90] Dunn, "Iran's Orwellian Cyber-Police Target Dissent."