After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities

Alexandra Van Dine[1]

The Stuxnet virus set off alarm bells all over the world when it was discovered in 2010. Many observers viewed this unprecedented cyber attack on a nuclear facility as the dawn of the age of cyber war—"the keystroke heard 'round the world."

Stuxnet also had significant implications for nuclear security. The attack revealed a troubling reality: in the future, cyber weapons could be used against nuclear facilities to achieve consequences far more serious than those observed at the Natanz uranium enrichment facility in Iran.

Terrorist groups have stated their desire to acquire weapons of mass destruction. Cyber weapons provide a new attack vector for groups determined to achieve this goal. Security and surveillance systems can be hacked to mask the theft of weapons-usable nuclear materials, or vital control systems can be compromised, potentially leading to a serious radiological release. Given repeated recent discoveries of malware—targeted or otherwise—at nuclear facilities, it is not impossible that malicious actors could gain access to these systems.

Stuxnet was an extremely precise weapon deployed against a highly secure facility for a very limited purpose. At no point were human lives or the environment in danger. However, this will not always be the case. With the code for Stuxnet now widely available online, it may only be a matter of time before a group intending to cause harm deploys a less discriminate weapon against a less secure, higher-consequence target like a nuclear power plant or nuclear materials storage facility.

The international community must learn from Stuxnet's lessons to prevent such an outcome.

---

1. Alexandra Van Dine is a program associate with the scientific and technical affairs team at the Nuclear Threat Initiative (NTI), where she works on cyber security-related projects and the NTI Nuclear Security Index. She is a graduate of Georgetown University's Edmund A. Walsh School of Foreign Service. The views presented in this paper are the author's alone and do not necessarily reflect those of the Nuclear Threat Initiative.

INTRODUCTION

Throughout late 2009 and 2010, centrifuges spinning in Iran's Natanz uranium enrichment facility started to break at unusually high rates. In time, it would become clear that these disruptions were not standard mechanical failures; they were the result of Stuxnet, a cyber weapon designed and deployed with the goal of slowing or halting Iranian uranium enrichment.

Stuxnet is a computer worm, that is, a virus with the ability to copy itself and travel quickly between computers. It was crafted to quietly take over industrial control systems and break the fragile, antiquated IR-1 centrifuges spinning at Natanz. Natanz's technology is widely viewed by the international community to be critical to Iran's pursuit of nuclear weapons.

Revelations about Stuxnet opened eyes in countries all over the globe. This was the first instance of a targeted cyber attack causing physical damage to highly sensitive infrastructure. Many observers viewed this discovery as "the keystroke heard 'round the world"—effectively, the dawn of the age of cyber warfare. Examining Stuxnet in a larger context, however, also reveals a troubling gap in the advancements made in nuclear security over the past decade. Nuclear facilities around the world remain too vulnerable to cyber attacks that could facilitate the theft of nuclear material or a radiological release.

Stuxnet, the code for which is now available to anyone with Internet access and sufficient funds, was able to penetrate a highly secure facility and cause physical damage intended to be limited in scope. But what if an adversary instead sought more destructive consequences?

Despite Stuxnet's warnings, the world is still playing catch-up when it comes to the cyber dimension of nuclear security. This paper will evaluate the current threat and approach to cyber security at nuclear facilities, discuss the Stuxnet case and its implications, and make recommendations based on the Stuxnet case for strengthening cyber-nuclear security.

THE THREAT

Leaders around the world have rightly expressed concern about the adequacy of physical security at nuclear facilities in the face of terrorist threats. As a result, countries have taken important steps to strengthen nuclear security domestically, and many international organizations—the International Atomic Energy Agency (IAEA), the World Institute for Nuclear Security (WINS), the United Nations, and Nuclear Security Summits, to name a few—have undertaken efforts to improve international preparation, prevention, and response.

The vast majority of this work has focused on key issues like the insider threat, physical security measures, and materials control and accounting technologies and procedures. Progress in these areas is a critical precursor to a more secure world and must benefit from continued investments of money, time, and attention. However, these efforts, important as they are, have been undertaken without sufficient attention to the cyber threat to nuclear security. In order to achieve the highest levels of global nuclear security, international efforts must also address the cyber threat and its implications for nuclear facilities.

Cyber attacks can have effects on par with a safety incident or physical security breach. For example, an adversary could hack into alarm or surveillance systems and disable them, masking the actions of malicious intruders. Materials control and accounting systems could be hacked in order to hide the theft of nuclear materials. In a worst-case scenario, an attacker could tamper with vital reactor control systems, potentially leading to radiological release with serious off-site consequences.

Recent decades have seen a proliferation of digital technologies across the nuclear enterprise. These technologies have real benefits in terms of safety and physical security; however, they do create cyber vulnerabilities that often go unanalyzed or even unnoticed. More digitization means more exploitable weaknesses, thus creating a dynamic and pervasive threat that strains national and international authorities alike.

Moreover, terrorist organizations like al Qaeda and the Islamic State of Iraq and the Levant (ISIL) are seeking radiological and nuclear capabilities and place a premium on attacks that maximize panic and destruction.[2] Cyber vulnerabilities could be leveraged in pursuit of these goals.

CURRENT STATUS

Government authorities, national regulators, nuclear industry, and international organizations have recognized the cyber threat to nuclear facilities and are taking some steps to develop and implement solutions. In the United States, for example, the Nuclear Regulatory Commission (NRC) and Department of Homeland Security (DHS) have defined roles in preventing and responding to a possible cyber attack at a nuclear facility. International organizations have also embraced their role, with the IAEA in particular working hard to provide training opportunities to regulators and facility staff around the world, develop and circulate guidance, and facilitate international dialogue on the topic. The nuclear industry has also been a leader in this area, with the Nuclear Industry Summit convening an international working group of industry representatives to consider the threat, develop solutions, and bring high-level attention to cyber security. The fact that this group will continue meeting, even in the absence of continued Nuclear Security Summits, demonstrates the industry's commitment to mitigating this threat.

Although all these efforts are useful and necessary to improving global cyber-nuclear security, the world remains underprepared to meet this dynamic threat. The current approach is unable to move as quickly and flexibly as the cyber threat and is unevenly applied geographically. Too many countries with nuclear materials or high-consequence nuclear facilities lack appropriate legal and regulatory frameworks in this area. What limited human capacity that exists at the nexus of cyber and nuclear security is heavily concentrated in North America, Europe, and Russia, meaning that many countries with new or expanding nuclear programs lack necessary technical expertise. Finally, cyber-security strategies tend to rely on technological measures like air gaps, firewalls, and

2. See Rolf Mowatt-Larssen, "Al Qaeda's Nuclear Ambitions," *Foreign Policy*, November 16, 2010, http://foreignpolicy.com/2010/11/16/al-qaedas-nuclear-ambitions/ and Kim Sengupta, "ISIS [Islamic State of Iraq and Syria] Nuclear Attack in Europe Is a Real Threat, Say Experts," *Independent*, June 7, 2016.

antivirus tools that have been proven fallible to the exclusion of other, perhaps more effective measures.

Lack of Legal Frameworks

Moreover, data exists that suggests a global lack of preparedness. The 2016 NTI Nuclear Security Index, a first-of-its-kind ranking of nuclear security conditions around the world, asked four basic questions about cyber security at nuclear facilities in countries with one kilogram or more of weapons-usable nuclear material or high-consequence nuclear facilities:[3]

1. Does the country require nuclear facilities to be protected from cyberattack?
2. Does the country require nuclear facilities to identify critical digital assets?
3. Does the country incorporate cyber threats into its design basis threat or other threat assessment?
4. Does the country require performance-based testing of its cyber security measures?

Scoring was based on publicly available laws and regulations, and did not measure implementation. Therefore, a high score does not necessarily guarantee security, although it does provide some idea of how seriously countries are taking the cyber threat. Key results included:

- Of 24 countries with weapons-usable nuclear materials, only 9 countries scored a maximum score on cyber security. Seven scored zero.
- Of 23 countries with high-consequence nuclear facilities, only 4 countries earned a maximum score. Thirteen scored zero, including some that are considering expanding their use of nuclear power or beginning new programs.
- In total, of 47 countries with weapons-usable nuclear materials or high-consequence facilities, 20—nearly half—scored a zero on cyber security.

These results suggest that the existence of key laws and regulations related to cyber security at nuclear facilities is disturbingly uneven. This threat is global—a cyber attack that causes damage at a nuclear facility could have consequences that reverberate around the world. Therefore, it is troubling that so many countries are not taking basic regulatory steps to protect nuclear infrastructure from attack.

Limited Human Capacity

Even where countries are working to improve their regulatory frameworks and operational processes and procedures, it is not always possible given the uneven distribution of limited human capacity in the cyber-nuclear space. Practitioners must possess a knowledge of digital control systems in nuclear environments, a skill set that is increasingly rare. There have been few of these experts; now, many have retired, and a limited number of candidates are entering the field. Those who remain tend to be concentrated in just a few countries. This leaves many countries developing or expanding nuclear energy programs grasping for solutions. As long as so few experts are concentrated in so few places, solutions will be difficult to devise and implement.

3. For more information about the NTI Nuclear Security Index, see www.ntiindex.org.

Overreliance on Technologies

The current operational approach to cyber security at nuclear facilities also tends to overestimate the effectiveness of certain technological measures. Defense strategies tend to be premised on the assumption that it is possible to completely prevent cyber attacks. Accordingly, they rely heavily on measures like air gaps, firewalls, and antivirus tools to deny access to attackers. Unfortunately, several cases in the past few years have demonstrated that these measures are not fully effective. These include discoveries of malware designed to provide remote access to adversaries and seek out login credentials at a German power plant; malware found in a Japanese nuclear power plant and a facility that handles plutonium and other nuclear materials; and a hack and subsequent data release affecting Korea Hydro and Nuclear Power, South Korea's nuclear operator.[4]

Although these tools can and do play an important role in cyber security, it is not reasonable to expect them to hold up to sustained attacks from determined adversaries. Such adversaries think creatively, move quickly and flexibly, leverage the full suite of system capabilities, and take advantage of enduring vulnerabilities that cannot be patched, such as inherent human imperfection. Therefore, a truly effective cyber-security strategy cannot be based upon prevention alone, and is ill-served by focusing on fallible technological measures to the exclusion of other security practices and solutions.

STUXNET: AN OVERVIEW

The cyber operation against Natanz leveraged two versions of the Stuxnet virus, the first more intensive and complicated than the second. The first part of the attack targeted the systems that protected the centrifuges spinning at the Natanz uranium enrichment plant. The malware tried to overpressurize the centrifuges by directly impacting the very system meant to prevent this from happening. At Natanz, this system was particularly elaborate due to the equipment it was protecting—outdated and unpredictable IR-1 centrifuges. Without such a system to compensate for the antiquated technology, the centrifuges would be too unpredictable to use.[5]

The IR-1 was selected for use at Natanz because Iran could produce the model at massive scale, which meant that frequent breakage was acceptable. IR-1 centrifuges only tend to work reliably if their parts are fabricated with incredible precision and they are operated in an environment with

4. For more on Germany, see Christoph Steitz and Eric Auchard, "German Nuclear Power Plant Infected with Computer Viruses, Operator Says," Reuters, April 26, 2016, http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS. For more on Japan, see "Monju Power Plant Facility PC Infected with Virus," *Japan Today*, January 7, 2014, http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus; and "Nuclear Center Waits Over a Year to Report Cyber-Attack," *Asahi Shimbun*, May 19, 2016, http://www.asahi.com/ajw/articles/AJ201605190028.html. For more on South Korea, see Meeyoung Cho and Jack Kim, "South Korea Nuclear Plant Operator Says Hacked, Raising Alarm," Reuters, December 22, 2014, http://www.reuters.com/article/us-southkorea-nuclear-idUSKBN0K008E20141222.

5. Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, November 19, 2013, https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

specific equipment. Iran could not create those conditions, and therefore had to lower the operating pressure of their centrifuges in order to decrease the stress on the sensitive rotors. This meant that fewer centrifuges would go offline as a result of damaged rotors, but that efficiency would decrease due to the lower operating pressure.[6] In order to compensate for this inefficiency and frequent centrifuge failure, Iranian scientists constructed a cascade protection system that ensured continuation of enrichment, even when one or more centrifuges broke.[7] At Natanz, a cascade was a grouping of 164 centrifuges connected together by pipes. Uranium gas would flow through those pipes and into the centrifuges in stages; each stage enriched the gas further, separating out isotopes needed for nuclear reaction and concentrating them in the gas.[8]

Using valves installed on each centrifuge, the system could isolate a troublesome centrifuge from the rest of the cascade long enough for an engineer to replace it while the process continued across the rest of the cascade. However, sometimes shut-offs occurred faster than engineers could fix them, leading to multiple isolated centrifuges within the same stage and a resultant rise in operating pressure, which is not good for the smooth operation of centrifuge cascades.[9]

To address this flaw, the Iranians installed exhaust valves at each stage to relieve this pressure. When pressure, as monitored by a sensor, exceeded a certain threshold, the exhaust valve would open and release extra pressure. These sensors and valves were operated by Siemens S7-417 industrial controllers that were tiny computer systems connected directly to the equipment.[10] Although this somewhat convoluted solution did keep the centrifuges up and running, it greatly increased the complexity of digital systems at Natanz. This provided fertile ground for Stuxnet's creators, who developed an attack that industrial control systems expert Ralph Langner described as "so far out, it leads one to wonder whether its creators might have been on drugs."[11]

One of the first steps of the Stuxnet attack was camouflage; that is, the malware was designed to mask its own activities when the attack executed, usually about once each month. Immediately before an attack, the malware would record exactly 21 seconds of the normal values displayed on the sensors protecting the cascades.[12] Then, Stuxnet would replay those 21 seconds in a constant loop as the attack took place, thus effectively projecting normalcy to facility operators while masking the weapon's activities from any network surveillance or monitoring capabilities.[13]

---

6. Ibid.

7. "Basic Attack Strategy of Stuxnet 0.5 Rev. 1," Institute for Science and International Security [ISIS], February 28, 2013, http://isis-online.org/isis-reports/detail/basic-attack-strategy-of-stuxnet-0.5/.

8. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

9. "Basic Attack Strategy of Stuxnet 0.5 Rev. 1."

10. Dan Goodin, "Revealed: Stuxnet 'Beta's' Devious Alternate Attack on Iran Nuke Program," *Ars Technica*, February 26, 2013, http://arstechnica.com/security/2013/02/new-version-of-stuxnet-sheds-light-on-iran-targeting-cyberweapon/2/.

11. Langner, "Stuxnet's Secret Twin."

12. Ibid.

13. Joby Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyber Attack," *Washington Post*, February 15, 2011, https://www.washingtonpost.com/world/irans-natanz-nuclear-facility-recovered-quickly-from-stuxnet-cyber-attack/2011/02/15/ABUIkoQ_story.html.

Safely hidden from view, the malware would close the valves that isolated centrifuges in such a way that pressure was raised on the rest of the centrifuges in a given cascade. This, in turn, placed greater stress on the rotor, ultimately breaking the centrifuge.[14] This would go on until the attacker decided that a sufficient number of centrifuges had been damaged, and conveyed the appropriate message to the virus via a complex command-and-control system.[15] Destroying too many centrifuges at once would have been easily detected by Iranian engineers and the true cause of the damages discovered much faster.[16]

At some point in 2009, the attacker changed course and deployed a second version of Stuxnet. This time, the malware targeted a different component: Siemens 315 programmable logic controllers (PLCs) that controlled centrifuge frequency converters, which are responsible for determining rotor speed. This was a much easier attack, and the methods by which the malware achieved it were far more direct than those of the first Stuxnet version.[17]

Unlike the first stage of the attack, this version was able to self-replicate within specified networks and transfer via removable stick drives to all kinds of computers. However, like the first version, it would only execute when it detected the specific Siemens PLC configuration it targeted. This version was also loaded with "zero day vulnerabilities" or undiscovered flaws in Microsoft Windows software. These are rare, and can go for hundreds of thousands of dollars each on the open market—indicating either a wealthy attacker, a technically sophisticated attacker, or both. Finally, this stage of the attack was accompanied by stolen digital certificates, which masked the malware as legitimate software and prevented its rejection by updated Windows operating systems.[18]

Once again, the new attack executed once per month, this time speeding up centrifuge rotor speeds, abruptly slowing them to almost a stop, and then speeding them back up again.[19] This occurred over a period of about 50 minutes. Because of the IR-1's supercritical design, the rotor had to pass through certain "critical speeds" before achieving a normal operating pace. Passing through these critical speeds, or "harmonics," could cause rotors to break. While the cascade protection system that Iran had devised could handle one cracked rotor, the problem once again occurred when multiple rotors crashed. This frustrated Iranian engineers immensely; while they had enough centrifuges to keep replacing those that broke, the engineers still had the maddening task of deciphering why the centrifuges were crashing in such volumes.[20]

---

14. "Basic Attack Strategy of Stuxnet 0.5 Rev. 1."

15. Geoff McDonald, Liam O'Murchu, Stephen Doherty, and Eric Chien, "Stuxnet 0.5: The Missing Link," Symantec Security Response, February 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf.

16. Langner, "Stuxnet's Secret Twin."

17. Goodin, "Revealed: Stuxnet 'Beta's' Devious Alternate Attack on Iran Nuke Program."

18. Langner, "Stuxnet's Secret Twin."

19. Ron Rosenbaum, "Richard Clarke on Who Was behind the Stuxnet Attack," *Smithsonian Magazine*, April 2012, http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/#obL1AHrdHV08K5A0.99.

20. Langner, "Stuxnet's Secret Twin."

Although this attack could only spread between computers attached to the same network or that exchanged files over USB sticks, computers could connect to these networks from hundreds of miles away using remote access or virtual private networks (VPNs). This change to how Stuxnet propagated spelled the beginning of the end as contractors carried Stuxnet-infected laptops to other client sites besides Natanz. Stuxnet would make the jump to that network and lay dormant, not detecting any of the specific technical specifications it was instructed to find.[21] The virus would then be transferred to other computers and USB sticks that would then be carried elsewhere and connected to still other networks. As people remotely accessed infected networks, the virus zoomed to their computer, sometimes actually traveling across continents. Soon, Stuxnet had traveled around the world solely on trusted Internet connections, making its ultimate discovery by a Belarusian security research firm inevitable.

Ultimately, Stuxnet destroyed roughly 1,000 out of a total of 9,000 IR-1 centrifuges at Natanz. This was certainly disruptive to Iranian enrichment efforts, forcing them to spend time and resources investigating the breakages, which in turn delayed nascent plans to expand the plant. Stuxnet also forced Iran to draw on its supply of centrifuges more quickly than it otherwise would have in order to replace those broken by the malware.[22] However, the attack was not an unmitigated success, as Iranian scientists responded to the breakages with actions that reduced further damage, mainly by shutting down centrifuge cascades for months on end. If the cascades were shut down, Stuxnet could not attack; and this decision created enough time and space for public discovery.[23]

BEYOND STUXNET: WHAT COMES NEXT?

The deployment of Stuxnet against the Natanz uranium enrichment facility was unprecedented and gave rise to many important questions about the nature of conflict in cyberspace; after all, never before had a cyber attack caused real, physical consequences at a nuclear facility. However, examining the case of Stuxnet in the nuclear security context demonstrates that Stuxnet was only the beginning. More malicious adversaries attacking less secure targets with less discriminate weapons can achieve far more serious consequences.

Target

A key component of the Stuxnet worm was the target it was intended to impact: a specific device within a well-defended facility that had already been the subject of significant international outcry. The Natanz uranium enrichment facility was part of what many believed to be a clandestine nuclear weapons program and was not supposed to exist. Although initially marketed to the international community as a desert-eradication project, evidence revealed by the National Council of Resistance of Iran (NCRI) in 2002 suggested that the site was actually meant for undeclared uranium

21. Ibid.

22. David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS [Institute for Science and International Security] December 22, 2010 Report," Institute for Science and International Security, February 15, 2011, http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf.

23. Ibid.

enrichment.[24] Satellite imagery and Iranian regime behavior later confirmed this assertion. Because this site was being constructed in secret to conduct illicit activities, security measures surrounding it were intense; in fact, plant employees were not even allowed to discuss their work with local officials. The Atomic Energy Organization of Iran would not even reveal the nature of the site with the local governor's office.[25]

Security was taken so seriously because Iranian authorities knew the site would be a target for foreign governments even before its existence was revealed. Satellite imagery analyzed by the Institute for Science and International Security provided evidence to this point. Photographs showed that the site was constructed entirely underground and that efforts were ongoing to camouflage it from view using earth and cement.[26] Circles visible around the perimeter of Natanz suggested plans to install antiaircraft guns. Underground buildings were built with concrete walls varying between six and eight feet thick—suggesting that they were heavily reinforced. Finally, even the tunnels leading to the underground facilities were constructed in such a way as to protect their contents from missiles fired on top of or directly into the tunnels.[27]

After the existence of Natanz was revealed and confirmed, the IAEA did gain some limited access. However, after Iran purported to suspend uranium enrichment activities in January 2006, the IAEA lost the ability to monitor key items like centrifuge components, assembled centrifuges, and associated equipment. Iran also revoked the IAEA's ability to conduct advanced inspections as permitted in the Additional Protocol. Taken together, this meant that the IAEA's understanding of activities at Natanz deteriorated over time.[28] It also suggested a tightening of security at the Natanz facility itself.

The fact that such a well-defended facility could still be compromised by a cyber weapon should concern the international community. Most nuclear facilities, including nuclear power plants, nuclear materials storage facilities, spent fuel pools, and even some large research reactors are more susceptible to cyber attack than Natanz and would result in more serious consequences should such an attack prove successful. Moreover, these facilities often employ standardized technologies. This means that many different facilities share the same system designs and configurations and rely upon the same technologies from the same small group of vendors. Therefore, if one facility can be hacked, it is likely that others could be too.[29]

---

24. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 34.

25. Ibid., 36.

26. Paul Brannan and David Albright, "ISIS [Institute for Science and International Security] Imagery Brief: New Activities at the Esfahan and Natanz Nuclear Sites in Iran," Institute of Science and International Security, April 14, 2006, http://isis-online.org/uploads/isis-reports/documents/newactivities.pdf.

27. David Albright and Corey Hinderstein, "The Iranian Gas Uranium Enrichment Plant at Natanz: Drawing from Commercial Satellite Images," Institute for Science and International Security, March 14, 2003, http://isis-online.org/isis-reports/detail/the-iranian-gas-centrifuge-uranium-enrichment-plant-at-natanz-drawing-from-/8#images.

28. Brannan and Albright, "ISIS Imagery Brief."

29. Langner, "Stuxnet's Secret Twin."

Additionally, because the malware was meant to attack only a specific device, the potential for the loss of life or environmental degradation was extremely low. By targeting the operations of the Siemens programmable logic controllers (PLCs), the potential for harm to humans or the environment was significantly lowered. While the Iranian uranium enrichment program certainly experienced a setback, the potential for the theft of nuclear materials or radiological release was extremely limited. This is not necessarily the case at most nuclear facilities.

Intent

Technical analysis of both stages of Stuxnet confirms that the attacker—likely a nation-state—sought to slow or halt Iran's uranium enrichment program and avoid catastrophic damage. For example, the first version of the attack, which attempted to break centrifuges by overpressurizing them, monitored the status of targeted centrifuges very closely. Ralph Langner, an industrial control systems expert who worked to initially decipher Stuxnet, described the code undergirding this stage of the attack as "so engineered that even the slightest oversight or any configuration change" would have rendered the attack useless.[30] This means that the attack would only execute in conditions for which it had been designed to operate.

Looking at the Stuxnet operation in its entirety, Langner also contends that "the attackers were in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead." This suggests that the intent was not to cause massive destruction; rather, it was to reduce the effectiveness of Iranian enrichment, force engineers to spend valuable time and resources on fixing or replacing centrifuges, and perhaps even push Iran to question its ability to develop and field a nuclear program.[31]

Unfortunately, not every deployment of a cyber weapon against a nuclear facility will have as narrow a mission. Terrorist groups have stated their desire to acquire weapons of mass destruction to achieve their aims. For example, Ayman al-Zawahiri, the current leader of al Qaeda, has written forcefully in favor of using nuclear weapons to retaliate against the West and has maintained this position for well over a decade.[32]

Furthermore, fears about the brutal organization Islamic State of Iraq and the Levant (ISIL) obtaining weapons of mass destruction have been growing as the group has ramped up its activities in the past two years. In fact, in March 2016, law enforcement discovered that the same ISIL cell that carried out the horrific Brussels attack that same month were actively surveilling a senior scientist who had access to sensitive areas of a Belgian nuclear research facility.[33] Additionally, ISIL was able to radicalize an employee at the Doel nuclear power plant in Belgium who ultimately left the country to fight for the terrorist organization.[34] Although he was

30. Ibid.

31. Ibid.

32. Mowatt-Larssen, "Al Qaeda's Nuclear Ambitions."

33. Sengupta, "ISIS Nuclear Attack in Europe Is a Real Threat, Say Experts."

34. Karl Vick, "ISIS [Islamic State of Iraq and Syria] Attackers May Have Targeted Nuclear Power Station," *Time*, March 25, 2016, http://time.com/4271854/belgium-isis-nuclear-power-station-brussels/.

killed in Syria, it is clear that this brutal terrorist group has a dangerous foothold in the nuclear space.

Groups like al Qaeda and ISIL would not use cyber weapons as Stuxnet's creators did: as a precise tool to achieve a specific and limited goal in a way that does not threaten human life or the environment. They would leverage the complete destructive power of cyber weapons to achieve their aims. This could include detonating a nuclear device built using materials stolen during a cyber-facilitated theft or achieving serious radiological release by sabotaging a nuclear facility.

Weapon

Stuxnet as a weapon has two important implications for the nexus of cyber and nuclear security. The first is its precision; Stuxnet was engineered to be a precise and discriminate weapon that did not cause physical destruction outside a narrow and specific set of conditions. The second is its availability; when it was first developed, a weapon like Stuxnet could not have been constructed without a nation-state's access to extensive technological, financial, and intelligence resources. As revelations of Stuxnet came to light, so too did its source code, which is now widely available to use in any number of more sinister attacks. When Stuxnet was originally deployed, it required a thorough understanding of nuclear engineering in order to be effective. This may continue to raise the "barrier to entry" for a potential attacker; however, this will depend on the target. Now that almost anyone with sufficient funds can make use of a weapon like Stuxnet, the initial, carefully calibrated deployment of the weapon can no longer be guaranteed—especially where non-state actors are concerned.

Precision

Stuxnet's technological precision was discussed in previous sections, but insight from Richard Clarke, counterterrorism expert and former special advisor to the president of the United States on cyber security, provides evidence that the weapon was also legally precise. He noted in a recent interview, "it very much had the feel to it of having been written by or governed by a team of Washington lawyers."[35] Based upon his knowledge of how government lawyers review proposals for covert action, he pointed to how Stuxnet's design limited its possible physical effects. "The lawyers want to make sure that they very much limit the effects of the action. So that there's no collateral damage," Clarke explained. The fact that Stuxnet may well have been designed with an eye toward laws and norms underlines the extent to which it was designed to have a narrow physical impact and not cause broader destruction.[36]

Ultimately, the weapon behaved as expected and did not cause damage beyond the centrifuges it was built to target. The weapon was painstakingly engineered, exhaustively tested, and only sought one victim: a Siemens PLC. Interrupting the operations of this particular device did not pose a threat to humans or the environment. Even when Stuxnet escaped Natanz, it caused no damage, instead simply shutting itself down in the absence of the specific conditions in which it

35. Rosenbaum, "Richard Clarke."

36. Ibid.

was designed to operate.[37] As a result, there were no serious physical consequences—just a rush in the security community to identify the virus.

Beyond the Nation-State

Cyber weapons are no longer the exclusive purview of nation-states. In the words of the renowned cryptographer Bruce Schneier, "Today's NSA secrets become tomorrow's PhD theses and the next day's hacker tools."[38] Today, determined adversaries can purchase Stuxnet for a fraction of what it cost to develop and use the source code as a template.[39]

Experts agree that this is perhaps the most troubling consequence of Stuxnet—the fact that its code can now be dissected and repurposed into new, possibly more dangerous weapons. Clarke himself has publicly stated that:

> if you're a computer whiz you can take it apart and you can say, "Oh, let's change this over here, let's change that over there." Now I've got a really sophisticated weapon. So thousands of people around the world have it and are playing with it. And if I'm right, the best cyberweapon the United States has ever developed, it then gave the world for free.[40]

Ralph Langner is more doubtful about the level of knowledge an adversary must possess to make use of Stuxnet's code. In an interview with the *Christian Science Monitor*, he stated, "you don't have to be a genius to create a program that works on a control system exactly the way Stuxnet does." Knowing how to copy elements of the code and understanding how to weaponize it for a desired target is now sufficient to make use of one of the most sophisticated cyber weapons ever developed.[41]

Importantly, many of the costs associated with Stuxnet came from the constraints faced by its creators. They hoped Stuxnet would never be discovered, and made every effort to design it appropriately. The largest investments of time and money likely came as a result of efforts to camouflage the attack and make its effects appear to be legitimate mechanical issues.

Furthermore, gathering the requisite intelligence on Natanz was likely not cheap, and required heavy investments from the intelligence community. Attackers seeking to cause destruction and not hide it are unlikely to make similar investments in disguising the effects of their operations, making a copycat attack all the easier.[42]

---

37. Jason Healey, "Stuxnet and the Dawn of Algorithmic Warfare," *Huffington Post*, March 16, 2013, http://www.huffingtonpost.com/jason-healey/stuxnet-cyberwarfare_b_3091274.html.

38. Bruce Schneier, "Cyberweapons Have No Allegiance," *Motherboard*, February 25, 2015, http://motherboard.vice.com/read/cyberweapons-have-no-allegiance.

39. Mark Clayton, "Stuxnet 'Virus' Could Be Altered to Attack U.S. Facilities, Report Warns," *Christian Science Monitor*, December 15, 2010, http://www.csmonitor.com/USA/2010/1215/Stuxnet-virus-could-be-altered-to-attack-US-facilities-report-warns.

40. Rosenbaum, "Richard Clarke."

41. Clayton, "Stuxnet 'Virus.'"

42. Langner, "Stuxnet's Secret Twin."

RECOMMENDATIONS FOR MOVING FORWARD

Armed with Stuxnet's lessons, leaders today can improve global preparedness and construct effective defenses. The following recommendations demand a sustained investment of resources, financial, intellectual, and otherwise; they also constitute much-needed advances toward the comprehensive nuclear security the world needs.

First, and most important, the current approach to cyber security at nuclear facilities must be fundamentally rethought. A new strategy, grounded in technically sound and forward-looking principles, must be developed to meet this dynamic threat. Despite ongoing efforts at the International Atomic Energy Agency, the World Institute for Nuclear Security, the United Nations, Nuclear Security Summits, and various national initiatives, recent years have seen example after example of successful infiltration of nuclear facilities by malware, targeted or otherwise. These cases alone demonstrate the insufficiency of the current approach. In order to defend against the well-resourced, targeted cyber attacks against nuclear facilities that could cause significant damage, a fresh look at what is necessary for defense is required.[43]

In the Stuxnet case, malware was able to infiltrate the facility for two key reasons. First, an organizational overreliance on air gaps to protect networks from infection created a false sense of security, and attackers were able to use this to their advantage. Second, the digital systems employed to keep Iran's IR-1 centrifuges up and running were highly complex and, therefore, highly vulnerable.

A new strategy for cyber security at nuclear facilities must address both of these factors. It could include a reassessment of the effectiveness of commonly relied-upon defense architectures and tools; these findings might lead to the creation of fundamentally new defense techniques and procedures at nuclear facilities. It could also focus on reducing the use of digital technologies at the most critical nodes of the facility, and reducing complexity in the most vital systems. Removing these known vulnerability multipliers from facilities would be an important step toward better security.

Second, nations must invest in response capabilities at home and abroad. Even if perfect policy could be written tomorrow, it would still take several years to implement. During this time, the possibility of a cyber attack with serious physical consequences would still exist. Therefore, every country needs to have a clearly articulated rapid response plan in place, with any provisions necessary to facilitate international cooperation.

Moreover, those countries that benefit from higher numbers of cyber-nuclear experts should work to develop ways to share this expertise with countries that need it in order to prevent or respond to cyber incidents. In terms of prevention, these experts could consult with facility operators on steps that could be taken immediately to improve protections against cyber attacks. If an incident is under way, these same people could make themselves available to help respond or, at the very

43. The Nuclear Threat Initiative has begun this work by developing a set of strategic priorities to guide such a strategy. Please see www.nti.org/about/cyber for more information.

least, to assist with post-incident analysis. The nuclear industry could play an important role in facilitating these connections.

Third, the international community must work to build global human capacity in this area. Achieving a sustainable strategy for mitigating this threat requires sufficient talent to develop and implement it. This aim can be achieved by strengthening the global cyber-nuclear community and facilitating connections across borders, seeking out opportunities to support or incentivize educational programs focusing on the cyber-nuclear nexus, and funding and supporting training programs at home and abroad to improve and build expertise in this area.

CONCLUSION

Although the Stuxnet worm will live in infamy as "the keystroke heard 'round the world," it only represents the beginning in terms of what can be achieved with a cyber attack at a nuclear facility. Stuxnet was an unprecedented weapon into which significant resources were invested. It was crafted to be precise in its destruction and deployed with the specific goal of slowing or halting Iran's nuclear program. It was launched against a highly secure facility and still managed to compromise its defenses.

The more pressing threat today is not that of a targeted action against a country undertaking an illegal nuclear weapons program. It is that determined adversaries with more sinister ambitions will use indiscriminate cyber attacks against less secure, higher-consequence nuclear facilities to facilitate the theft of nuclear materials or a serious act of sabotage. Stuxnet showed the world the art of the possible when it comes to cyber attacks at nuclear facilities; it serves as a valuable reminder that no matter how secure a facility appears, it can still be vulnerable. However, the international community has no shortage of targets and no shortage of potential adversaries seeking to cause destruction.

The international community must heed Stuxnet's wake-up call and start taking steps to better defend itself against this threat.