Stuxnet—The First Cyber Guided Missle

In July 2010, a computer security firm Belarus announced that it had discovered the signature of a new piece of malware—malicious computer software. This announcement was not unusual or surprising. After all, the cybersecurity firm Symantec discovered more than 400million new pieces of malware in 2011, ost or which were easily identified and rendered harmless. But this new virus—Stuxnet—was different; it was the harbinger of a changed world. Up until this software was developed, many experts believed that the effects of cyber conflicts would be restricted to the cyber domain. Stuxnet showed the world that cyber war could potentially kill real people.

A Two-Phase Attack

- Stuxnet caused a malfunction in the centrifuges used in uranium purification facility in Natanz, Iran.

- What's frightening in that statement is that there is nothing that limits a cyber assault to this type of facility or process. The type of system invaded in Iran also controls the heat of nuclear reactors. It would be no harder to cause the centrifuges to break down than to pull out the graphite control rods, causing a nuclear meltdown.

- Stuxnet used a two-phase attack. In the delivery phase of the program, the **malware** infected a Windows-based operating system. The purpose of this delivery phase was to put the attack program in a system that might someday be attatched to the target's control system.

- From this delivery platform, the malware was designed to "jump" to infect what is known as the **SCADA** system—a supervisory control and data acquisition system—

manufactured by the German firm Siemens. This jump from the Microsoft operating system to the SCADA system was the attack phase of the program.

- The program required two phases for its attack because so many SCADA systems that run sensitive or secret machinery are not directly connected to the Internet. A direct connection makes a system more vulnerable to intrusion; thus, the operators add an additional layer of security by creating an "air grap," a measure designed to ensure that there are not connections between the system and the Internet.

- The Iranian nuclear enrichment program was almost certainly air gapped from the broader Internet. Stuxnet must have entered the SCADA system through some interaction with an external, Windows-based program. No one knows for sure how that happened.

- The second phase of the attack demonstrated a high degree of sophistication. It was designed to target only a particular type of operating program. In identifying its target within the Iranian nuclear enrichment facility, Stuxnet's developers exhibited a significant degree of inside knowledge.

- Stuxnet manipulated the speed of centrifuge rotors used in the process of purifying uranium, causing variations that were designed to slowly ware down, and ultimately, crack the rotors. Because the centrifuges fan at a variable rate, the uranium produced by the facility was impure and unsuitable for use. Stuxnet also disabled and bypassed several digitally operated safety systems designed to ensure that the centrifuges ran at a fixed speed.

- Ultimately, Stuxnet was a piece of computer malware that had a real-world effect. Any physical system that is operated by a computer system was now at least theoretically vulnerable to attack and possible destruction.

- Not only did Stuxnet have physical effects, but it also hid them! Buried within the program was a prerecorded series of false data reports, leading operators to believe that the centrifuges were running normally.

- Though Stuxnet was targeted at an Iranian facility, according to Symantec, by September 2010, there were 100,000 computer servers infected with the virus around the world, including the United States.

- Responsibility for the Stuxnet malware has not been decisively demonstrated, although some people believe that hints buried in the malicious code point to Israeli authorship. *The New York Times* reported that Israel and the United States cooperated to produce Stuxnet, and according to the *Washington Post*, Stuxnet was the last phase of a U.S.-Israeli cyber sabotage program known as Flame.

A Decisive Change

- In July 1945, when the first experimental atomic bomb was exploded, J. Robert Oppenheimer, the scientist who led the Los Alamos development effort, immediately recognized the destructive power of the bomb and the tranformative effect it would have of war-making. But neither Oppenheimer nor anyone else could, at the dawn of the nuclear age, anticipate the long-term social,

psychological, and geopolitical effects of the development.

Of course, we now know that the first atomic bomb brought us nuclear power and cheaper electricity, but it also brought us new ways of thinking about war, such as the concept of mutually assured destruction.

In the broader field of world geopolitics, nuclear weapons also wrought unexpected changes. The existence of atomic weapons mandated a policy of containment rather than confrontation because nuclear war was to grave to risk. From this policy flowed the Cold War, the Marshall Plan, NATO, and ultimately limited wars of Korea and Vietnam.

At the beginning of the nuclear era, all these developments were unanticipated by anyone who witnessed the first atomic explosion.

- The dawn of the cyber age is no different. We have had an easy time exploiting the benefits of the Internet, but now it seems as though vulnerabilities threaten to outweigh those benefits. The Internet is a wild and dangerous place, where our secrets and even our identities are increasingly as risk.
- Stuxnet was a proof of concept that cyber war can be real. And as the Department of Homeland Security recently noted, now that information about Stuxnet is publicly available, it's much easier for other bad actors

to develop variants that target other SCADA systems around the world. Because SCADA systems are pervasive and generic, the Stuxnet **worm** is, essentially, a blueprint for a host of infrastructure attacks.

- The American demonstration that nuclear weapons were capable of manufacture assured the Soviets that their efforts would eventually succeed. Similarly, the proof, though Stuxnet, that cyber attacks can have kinetic effects has opened a world of possibilities for malware designers, many of which are potentially catastrophic.
- It's also possible that the damage to Iran's nuclear program caused by Stuxnet was just a useful collateral benefit to a larger purpose: that os sending a message to the Iranians that even their most sensitive programs were vulnerable. This is sometimes called a "info hack," in which the purpose is more to let opponents know that hey are vulnerable rather than to achieve any particular result.

- The most profound similarities between the atomic weapons and cyber threats, however, lie in the disruptive nature of the Stuxnet event.

- Imagine what it must have been like the day after the first atomic bomb was exploded. Around the globe, settled assumptions about war, policy, foreign affairs, an law had, in an instant, all come unglued. Even 17 years after the atomic bomb was first exploded, the uncertainty about the use of these weapons and the threat they posed was so great that the Cuban missile crisis nearly engulfed the world in nuclear war.

- We are on the verge of experiencing that same sort of tumultuous time, and almost nobody in America—expect a few senior policymakers—knows it.

- Perhaps more ominously, even at the dawn of the nuclear age, we were confident that we could identify anyone who used atomic weapons, and they would all be peer nation—state actors. In the cyber realm, we have much greater difficulty identifying who "fires' the weapon, and the culprit may well be a non-state actor—perhaps terrorists or a small group of hackers.

- In short, we stand on the threshold of a new world, much as we did in 1945. From this vantage point, nobody can say where the future might lead. But we do know that the changes that lie ahead will affect everyone on the planet.

Taken from: ***Thinking about Cyber security Cyber Crime to Cyber Warfare***, The Teaching Company 2013