Stuxnet Virus
A feature of future wars

DHRUV C KATOCH

In June 2009, the Stuxnet worm made its appearance around the world. As per Symantec Corporation, the worm hit primarily inside Iran, but also appeared in India, Indonesia and other countries. The worm went undetected for months because unlike most malware, it seemed to be doing little harm. It did not slow computer networks or wreak general havoc. Post detection, it was found that the worm only became operational when it detected the presence of a specific configuration of controllers, running a set of processes that appear to exist only in a centrifuge plant. Thus it appears that the attackers took great care to make sure that only their designated targets were hit. In military terms, 'It was a marksman's job'.

Stuxnet was first reported in mid-June 2010 by VirusBlokAda, a little-known security firm based in Belarus. A month later, Microsoft confirmed that the worm was actively targeting Windows PCs that managed large scale industrial control systems in manufacturing and utility firms. Those control systems are often referred to using the acronym SCADA, for "supervisory control and data acquisition" and run everything from power plants and factory machinery to oil pipelines and military installations. At the time it was first publicly identified in June 2010, researchers believed that Stuxnet exploited just one unpatched, or "zero-day," vulnerability in Windows and spread through infected USB flash drives. Later it was found that Stuxnet could actually use four zero-day vulnerabilities to gain access to corporate networks. Once it had access to a network, it would seek out and infect the specific machines that managed SCADA systems controlled by software from Siemens.

One of the widely used controllers is the Siemens controller known as P.C.S.-7 (Process Control System 7). Its complex software, called Step 7, can run whole symphonies of industrial instruments, sensors and machines. These controllers were critical to the operations at Natanz, Iran's major enrichment centre. The

Stuxnet worm appears to have been designed to attack the vulnerabilities in the controller.

How the Stuxnet worm originated is a matter of speculation. Some believe that it was designed as an American-Israeli project to sabotage the Iranian nuclear program and was tested prior to launch at Israel's nuclear facility in the Dimona complex in the Negev desert. The Iranian centrifuge which was targeted has a history which goes back to Pakistan's nuclear scientist, AQ Khan. In the early seventies, the Dutch had designed a Uranium enrichment machine. Khan, who was working with the Dutch as a metallurgist stole the design in 1976 and fled to Pakistan. The resulting machine, known as the P-1, for Pakistan's first-generation centrifuge, helped the country get the bomb. When Khan later founded an atomic black market, he illegally sold P-1's to Iran, Libya, and North Korea. It is believed that the Israelis used machines of the P-1 style to test the effectiveness of Stuxnet. It is also speculated that Israel worked in collaboration with the United States in targeting Iran, but that Washington was eager for "plausible deniability." After successful trials at Dimona, it was used against Iran's centrifuge facility at Natanz and is believed to have destroyed roughly a fifth of Iran's nuclear centrifuges. Stuxnet then may be considered as the most sophisticated cyber weapon ever deployed.

The worm itself now appears to have included two major components. One part of the program is designed to lie dormant for long periods, and then speed up the machines so that the spinning rotors in the centrifuges wobble and then destroy themselves. Another part, called a "man in the middle" in the computer world, sends out those false sensor signals to make the system believe everything is running smoothly – otherwise the plant would shut down before it could self-destruct. Stuxnet thus was not the work of hackers but a deliberate attempt to destroy a specific target with military precision. The attacker would have had to have an intimate knowledge of the specific vulnerabilities of the Siemens controllers as well as an intimate understanding of exactly how the Iranians had designed their enrichment operations. For example, one small section of the code appears designed to send commands to 984 machines linked together. A report issued by the Institute for Science and International Security, a private group in Washington said Iran's P-1 machines at Natanz suffered a series of failures in mid- to late 2009 that culminated in technicians taking 984 machines out of action. The report called the failures "a major problem" and identified Stuxnet as the likely culprit. This was also admitted by the Iranian president, Mahmoud Ahmadinejad, who said that a cyber attack had caused "minor problems with some of our centrifuges." Fortunately, he added, "our experts discovered it."

The attacks then could be said to be partially successful. Some parts of Iran's operations ground to a halt, while others survived. But it is still not clear if the attacks are over. Some experts who have examined the code believe it contains the seeds for yet more versions and assaults. Viewed from the military angle, the attack has legitimised a new form of industrial warfare, one to which all countries including India would be highly vulnerable to.

What then are the implications for India? In an article in The Telegraph, dated 14 Oct 2010, Ben Coughlin sketched out an imaginary scenario of a cyber attack in 2025. An aircraft carrier dispatched to the Pacific to settle a trade dispute is suddenly hit by a massive power failure. The engines and the computer systems shut down, and the fleet's powerful array of weaponry is rendered inoperable. At a stroke, the British battle group had been neutralised by teams of highly skilled computer hackers who had placed a computer worm in the fleet's operating systems. Simultaneously, the country's power stations, water firms, air traffic control and all government and financial systems are attacked and forced to shut down. In the space of a few minutes, the entire nation is paralysed.

The scenario could be considered as far-fetched by some but the reality of cyber warfare is something which we can ignore only at our peril. The lesson of the Stuxnet worm is a pointer to the shape of things to come. Future threats are more likely to take place in cyber space than on the battlefield and the prospect of cyber attacks by terrorists, hostile states and criminal gangs is a reality for which we need to prepare. The time has come to consider cyber warfare as a primary threat, especially as hostile countries can carry out attacks with plausible deniability. Failure to prepare will render our spending on conventional armaments as an exercise in futility and will jeopardise the very well being and security of the nation.

Maj Gen **Dhruv C Katoch**, SM, VSM (Retd) is Additional Director, CLAWS