SMALL WARS JOURNAL

smallwarsjournal.com

Stuxnet: Cyberwar Revolution in Military Affairs

by Paulo Shakarian

On June 17th, 2010, security researchers at a small Belarusian firm known as VirusBlockAda identified malicious software (malware) that infected USB memory sticks.[1] In the months that followed, there was a flurry of activity in the computer security community – revealing that this discovery identified only one component of a new computer worm[2] known as Stuxnet. This software was designed to specifically target industrial equipment. Once it was revealed that the majority of infections were discovered in Iran,[3] along with an unexplained decommissioning of centrifuges at the Iranian fuel enrichment plant (FEP) at Natanz,[4] many in the media speculated that the ultimate goal of Stuxnet was to target Iranian nuclear facilities. In November of 2010, some of these suspicions were validated when Iranian President Mahmoud Ahmadinejad publically acknowledged that a computer worm created problems for a "limited number of our [nuclear] centrifuges." [5] Reputable experts in the computer security community have already labeled Stuxnet as "unprecedented,"[6] an "evolutionary leap,"[7] and "the type of threat we hope to never see again."[8]

In this paper, I argue that this malicious software represents a revolution in military affairs (RMA)[9] in the virtual realm – that is Stuxnet fundamentally changes the nature of cyber warfare. There are four reasons to this claim: (1) Stuxnet represents the first case in which industrial equipment was targeted with a cyber-weapon, (2) there is evidence that the worm was successful in its targeting of such equipment, (3) it represents a significant advance in the development of malicious software, and (4) Stuxnet has shown that several common assumptions about cyber-security are not always valid. In this paper I examine these four points as well as explore the future implications of the Stuxnet RMA.

[1] Kupreev Oleg and Ulasen Sergey, *Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review,* VirusBlockAda, July 2010.

[2] A worm is defined as a self-propagating piece of malicious software.

[3] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier Version 1.4.* Symantec Corporation, February 2011, 7.

[4] David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Institute for Science and International Security (ISIS), December, 1.

[5] Thomas Erdbrink, "Ahmadinejad: Iran's nuclear program hit by sabotage," *Washington Post,* 29 November, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html (accessed 16 February, 2011).

[6] Quote from Roel Schouwenberg, Senior Anti-Virus Researcher at Kaspersky Labs in an interview at the *Virus Buletin* conference, October 2010, http://www.youtube.com/watch?v=C9H3MrtLgUc (accessed 16 February, 2011).

[7] Martin Brunner, Hans Hofinger, Christoph Krauss, Christopher Roblee, Peter Schoo, and Sascha Todt, *Infiltrating Critical Infrastructures with Next-Generation Attacks W32.Stuxnet as a Showcase Threat,* Fraunhofer SIT, December, 2010, 23.

[8] Falliere, et. al., 55.

[9] Williamson Murray, *Thinking about Revolutions in Military Affairs*, Joint Forces Quarterly, Summer 1997.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **15 APR 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE **Stuxnet: Cyberwar Revolution in Military Affairs**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Military Academy,West Point,NY,10996**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

Stuxnet Targets Industrial Equipment

Several major computer security firms have thoroughly examined Stuxnet[10] and all conclude that the primary goal of this piece of software was to cause subtle failures to industrial equipment. Although the possibility of attacking such equipment by cyber means has long been hypothesized, this new worm actually attempted the feat. Further, this type of attack was most likely the sole goal of the software. For instance, other malware include standard code for a variety of criminal activities – including identity and password theft, launching denial-of-service attacks, and sending spam emails.[11] Despite its high degree of technical sophistication, Stuxnet was not designed to perform any of these activities.[12] Rather, the software attempts to propagate itself with the goal of infecting a Microsoft Windows-based computer which communicates with the industrial equipment. This is in stark contrast to the myriad of malicious software on the Internet that is used for a variety of criminal purposes. Stuxnet was designed for sabotage, not crime.

The type of industrial equipment Stuxnet infects is known as SCADA (Supervisory Control and Data Acquisition) systems. These systems are designed for real-time data collection, control, and monitoring of critical infrastructure, including power plants, oil/gas pipelines, refineries, water systems, or other applications requiring computer-controlled equipment.[13] SCADA systems often use PLCs (Programmable Logic Controllers) – computer hardware to control a physical component. To program the PLC, the administrator connects it to a standard Windows computer. The PLC is then normally unplugged from the computer when it is ready for use. So, for example, if he wants to run centrifuges at a faster rate, he attaches the PLC to the Windows machine, runs a piece of software that communicates with the PLC, and uploads the new instructions. Assume *Stuxnet* has infected the computer attached to the PLC. The malware essentially runs a "man-in-the-middle" attack against the system. The administrator attempts to send commands to the PLC. Stuxnet intercepts them, and instead sends its own instructions. However, the software then falsely reports back to the Windows computer that the original instructions were uploaded. By rendering the false report, Stuxnet hides itself, making it more difficult to detect.

Stuxnet was designed to attack PLC‟s controlled by the Siemens‟ *Step 7* software.[14] Further, it only infects two models of PLC‟s – the Siemens S7-315 and S7-417. The S7-315 is a general purpose controller which operates a single array of devices. Such an array or group of devices controlled by the S7-315 may, for example, operate different phases of a manufacturing process. The S7-417 is a top-of the line model, operating multiple arrays – thereby able to control a more equipment than the S7-315.[15] Security experts have determined that Stuxnet only launches attacks if the PLC is attached to devices configured in a very specific manner. For example, when the worm detects the S7-315, it only attacks if the PLC is attached to 33 or more

[10] These include Symantec, Kaspersky Labs, ESET, and Langner Communications GmbH.

[11] Paul Barford and Vinod Yegneswaran, "An Inside Look at Botnets," in *Malware Detection,* ed. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang, Springer, 2007.

[12] Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, *Stuxnet Under the Microscope Revision 1.2,* ESET, November, 2010, 5.

[13] John D. Fernandez and Andres E. Fernandez , "SCADA systems: vulnerabilities and remediation," *Journal of Computing Sciences in Colleges*, Vol. 20, No. 4, April 2005, 160-168.

[14] Thomas Brandstetter, "Stuxnet Malware," *CIP Seminar,* Siemens, November, 2010.

[15] Ralph Langner, "How to Hijack a Controller - Why Stuxnet Isn‟t Just About Siemens PLCs," Control Magazine, 13 January, 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101 html (accessed 16 February, 2011).

frequency converter drives – devices used to control the speed of certain equipment (i.e. the rpm‟s of a motor).[16] Likewise, when attacking the S7-417 PLC, it expects to find 6 cascades of 164 frequency converter drives.[17] The malware also ensured that the frequency converter drives were manufactured by either the Iranian company *Fararo Paya* or the Finish company *Vacon*. [18]

Once Stuxnet has determined it has infected the targeted configuration of frequency converters, it launches the attack. Based on analysis of the software, experts have found that it expects the drives to be running between 807 and 1,210 Hz. It then periodically alters this setting to values between 2 and 1,410 Hz.[19] In this way, the device being controlled by the frequency converter is operating in an unexpected manner. As Stuxnet reports that the PLC was programmed correctly, the operator would assume that the devices are functioning in the normal range. The fact that Stuxnet adjusts these settings illustrates an important point – the worm was intended to actually damage the industrial equipment. If Stuxnet were simply a proof-of-concept, or a stunt, the adjustment of the frequencies would probably be unnecessary.[20]

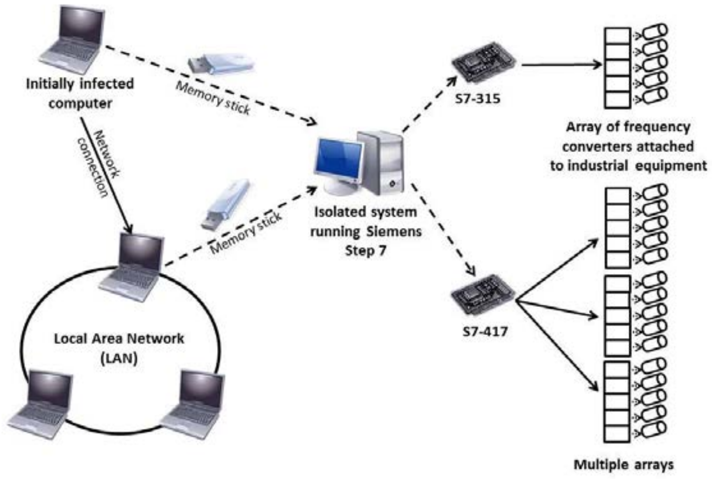
Initially infected computer
Memory stick
Network connection
Memory stick
Isolated system running Siemens Step 7
S7-315
Array of frequency converters attached to industrial equipment
S7-417
Local Area Network (LAN)
Multiple arrays

Figure One: The Propagation of the Stuxnet worm

Stuxnet Was Most Likely Successful

Not only was Stuxnet designed to target industrial equipment, there is also evidence that it was successful in doing so. The indicators for success arise from the following line of reasoning. First, it appears that the initial infections of the worm occurred in Iran. Second, the data structures in the Stuxnet code resemble the configuration of centrifuges at the Iranian FEP at Natanz. Third, Iranian government officials admitted that their centrifuge operations were affected by the worm.

[16] Falliere, et. al., 39.
[17] Ralph Langner, “417 Data Structures = Cascade Structure = Reported Damage,” *Langner Communications GmbH Blog*, 29 December 2010, http://www.langner.com/en/2010/12/29/417-data-structures-cascade-structure-reported-damage/ (accessed 16 February, 2011).
[18] Falliere, et. al., 39.
[19] Ibid., 41.
[20] Langner, *Control Magazine.*

It appears that Iran was the epicenter of the attacks. This is indicated by the volume of infections as well as analysis of malware samples. The security firm Symantec tracked 100,000 infected machines as of 29 September 2010 – approximately 60,000 of which were located in Iran. Indonesia followed with about 15,000 infections.[21] Symantec, in cooperation with other security firms, gathered 3,280 unique samples of the Stuxnet software and its variants.[22] These samples represented 12,000 total infections. Stuxnet maintains a list of previous systems it infected. Hence, for a given sample, researchers were able to determine the path the worm propagated in order to arrive at that computer. In reviewing these samples, Symantec could trace the infection history to one of five different organizations - all of which have a presence in Iran.[23]

From what is known of the Natanz FEP, there seems to be a striking resemblance between their centrifuge configuration and the Stuxnet code. According to the IAEA, the IR-1 centrifuges at the Natanz FEP operate in cascades of 164.[24] This precisely aligns with the configuration Stuxnet searches for when attacking the S7-417 controller. Another potential indicator is the maximum speed of an IR1 centrifuge: 1,400-1,432 Hz.[25] This frequency range is very close to the maximum speed the malware sets during the attack – 1,410 Hz.[26] An IR-1 centrifuge set to such a high frequency would likely incur damage.

The process of Uranium enrichment can be optimized if it is divided into a series of phases with multiple centrifuges operating at each phase.[27] It was revealed in a 2006 interview that the Iranians were conducting their Uranium enrichment with such a method using fifteen phases.[28] At each phase, a certain number of centrifuges are allocated for optimal production. Alexander Glaser, a professor at Princeton‟s Nuclear Futures lab, studied the optimal arrangement of centrifuges in a 164-sized centrifuge cascade. Ralph Langner, founder of Langner Communications GmbH, which specializes in SCADA systems, compared this analysis to the data structures in the Stuxnet. He found that the malware possibly operates in a manner that significantly interferes with the optimal distribution of centrifuges at each phase. The resulting allocation is appears to be the opposite of the optimum as determined by Glaser.[29] If Stuxnet targeted the Natanz centrifuges, it would have resulted in sub-optimal output of enriched Uranium – hence the amount produced would likely be much below capacity.

In addition to the aforementioned technical analysis, there is also some evidence of the software‟s potential effectiveness in the statements of Iranian leaders. President Ahmadinejad confirmed the presence of malicious software affecting their centrifuges in November 2010 – although he did not explicitly describe the presence of Stuxnet.[30] In an interview with SPIEGEL ONLINE the general secretary of Iran's Supreme National Security Council, Saeed Jalili, was asked specifically about Stuxnet being used to attack Natanz. Although Jalili did not go into

[21] Falliere, et. al., 5.
[22] The designers of Stuxnet launched attacks in three phases, each phase using an updated version of the software. The technical details can be found in Falliere, et. al.
[23] Ibid., 7.
[24] Albright, et. al., 2.
[25] Ibid., 4.
[26] Falliere, et. al., 41.
[27] Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)," *Science and Global Security*, June, 2008, 14.
[28] Ibid.
[29] Ralph Langner, "Applying Aqazadeh‟s revelations to Stuxnet forensic analysis," *Langner Communications GmbH Blog, 30 January 2011*, http://www.langner.com/en/2011/01/30/applying-aqazadeh%E2%80%99s-revelations-to-stuxnet-forensic-analysis/ (accessed 16 February, 2011).
[30] Erdbrink.

details on the damage done by the worm (again downplaying the effect it had), he did admit that an incident had occurred by stating that "our experts already warded off this attack a long time ago."[31]

It is also interesting to note that there is a possibility that Stuxnet was installed at Natanz by a saboteur using a memory stick.[32] In such an event, the designers of the worm would greatly increase their probability of success, as opposed to passively waiting for the software to propagate to the facility. In October 2010, Iran‟s intelligence minister, Heydar Moslehi announced that an unspecified number of "nuclear spies" were arrested in connection with Stuxnet.[33] While the details and nature of the arrests are unknown, this (at the very least) illustrates that Iran recognizes the various methods by which the worm could have spread – as well as the seriousness of its impact on their operations.

It is worth noting that in late 2009 or early 2010, Iran decommissioned and replaced about 1,000 IR-1 centrifuges at the Natanz FEP (6 cascades of 164 centrifuges each).[34] The timing of the decommissioning, along with the number of centrifuges taken offline is consistent with the timing and data structures of Stuxnet. The obvious alternative explanation for the failure is a manufacturing defect but it is unclear why such a defect would take so long to manifest itself.[35] From the previously mentioned analysis, it seems that Stuxnet does not attempt to immediately destroy centrifuges. Rather, it adjusts the frequencies in a more subtle manner over time – which makes it difficult to determine if a problem was caused by the worm or some other part of the enrichment process. This behavior of the malware makes it a more consistent explanation to the decommissioning of the centrifuges. In addition to pulling the IR-1‟s offline, the Natanz FEP also experienced sub-optimal levels of Uranium production during 2009-2010. IAEA reports show that the amount of enriched Uranium produced at Natanz remained relatively stable at this time despite a substantial increase in the number of centrifuges.[36] This indicates that the system was producing Uranium below an optimal level.

Despite the Iranian claims in late 2010 that the Stuxnet worm had minimal impact on their nuclear operations, security expert Ralph Langner asserts that the malware set Iran‟s nuclear program back two years.[37] The reasons for this are twofold. First, as stated earlier, damage caused by Stuxnet is more subtle – although most likely effective. Hence, equipment failure caused by the software is difficult to attribute. Second, due to the prolific nature of Stuxnet, it is very difficult to clean the malware of all computing devices involved in the enrichment process. These concerns may explain why Iran temporarily halted all enrichment operations at Natanz in November 2010 (for unknown reasons).[38]

[31] Dieter Bednarz and Erich Follath, "Iran's Chief Nuclear Negotiator: 'We Have to Be Constantly on Guard,'" *SPIEGEL ONLINE,* 18 January, 2011, http://www.spiegel.de/international/world/0,1518,739945-2,00 html (accessed 16 February, 2011).

[32] Falliere, et. al., 3.

[33] John Leyden, "Iran boasts of Stuxnet 'nuclear spies' arrests," *The Register,* 4 October, 2010, http://www.theregister.co.uk/2010/10/04/stuxnet_conspiracy_theories/ (accessed 16 February, 2011).

[34] Albright, et. al., 2.

[35] Ibid., 3.

[36] Ibid., 9.

[37] From an interview with Ralph Langner by Yaakov Katz in "Stuxnet Virus Set Back Iran‟s Nuclear Program by 2 Years," *Jerusalem Post,* 15 December 2010, http://www.studentnewsdaily.com/daily-news-article/stuxnet-virus-set-back-irans-nuclear-program-by-2-years/ (accessed 16 February, 2011).

[38] Albright, et. al., 6.

A natural question to ask is “what other countries were affected by Stuxnet?” Although there were reports of the worm on SCADA equipment in Germany,[39] Finland,[40] and China,[41] none of these infections resulted in damage to the industrial systems. This could be due to the specific configuration of the PLC, as Stuxnet only launches the attacks on certain setups. Siemens states that users of only fifteen systems running their software reported infections. Of these fifteen systems, none of them incurred any damage.[42] Iran most likely did not report infections to Siemens. Although they acquired S7-315 and S7-417 controller cards in 2002-2003, the IAEA established that Iran most likely diverted such hardware to its nuclear program – which resulted in Siemens halting sales.[43] However, it is known that S7-417 was installed at Bushehr, which may also have been a Stuxnet target.[44] At Bushehr, the S7-417 was not obtained directly from Siemens, but from a Russian firm known as Power Machines Corp., who then under Iranian contract installed it as part of their Teleperm system.

Stuxnet Is a Significant Advancement in Malware

As with other pieces of malicious software, Stuxnet takes advantage of previously unidentified security holes in system software known as “zero-day” vulnerabilities. As this type of exploit has been previously undetected, they are unidentified by anti-virus software. As a point of reference, the “Arora” malware, responsible for attacks on Google in late 2009 (which were generally attributed to China)[45] relies on one zero-day vulnerability. The use of two zero-day vulnerabilities would be unprecedented.[46] Stuxnet contains four zero-day vulnerabilities for the Microsoft Windows operating system and an additional one for the Siemens software. Two of the Windows vulnerabilities used in Stuxnet deal with privilege-escalation. These allow the worm illegitimate root or administrator-level access to the infected system. The other two deal with the propagation of the worm either through a memory stick or through a local network. At the time of this writing, self-propagation is less common in malware as it is often difficult to control. For example, consider a “botnet” – a large number of computers infected with malware and controlled by a “command and control” server which is not legitimately affiliated with the infected machines.[47] This is a very common platform for conducting cyber-crime. With a botnet, propagation occurs primarily through spam emails and malicious websites – self-propagation methods is very limited.[48]

Stuxnet Invalidates Several Security Assumptions

Our final aspect of the Stuxnet RMA is that it invalidates several security assumptions. The first such assumption is that isolated systems are more secure. As SCADA systems, by

[39] “Stuxnet also found at industrial plants in Germany,” *The H Security,* 17 September 2010, http://www h-online.com/security/news/item/Stuxnet-also-found-at-industrial-plants-in-Germany-1081469.html (accessed 16 February, 2011).

[40] “Stuxnet Spreads to Finland,” *The New Internet,* October, 2010, http://www.thenewnewinternet.com/2010/10/14/stuxnet-spreads-to-scandinavia/ (accessed 16 February, 2011).

[41] John Leyden “Stuxnet worm slithers into China,” *The Register,* 1 October, 2010, http://www.theregister.co.uk/2010/10/01/stuxnet china analysis/ (accessed 16 February, 2011).

[42] Brandstetter.

[43] Albright, et. al., 5.

[44] Ralph Langner, “417 Installed in Bushehr NPP,” *Langner Communications GmbH Blog, 14 December 2010*, http://www.langner.com/en/2010/12/14/417-installed-in-bushehr-npp/ (accessed 16 February, 2011).

[45] Timothy L. Thomas, “Google Confronts China‟‟s „„Three Warfares,‟‟”*Parameters,* Summer 2010, 101.

[46] Interview with Roel Schouwenberg at *Virus Buletin* (see note 2).

[47] Barford and Yegneswaran, 2.

[48] Ibid., 3.

definition, control mission critical machinery, many administrators do not connect these computers to a network – attempting to achieve security by isolation. As a result, file transfer to such machines is conducted by removable media. The designers of Stuxnet exploited this assumption by enabling the worm to spread through the memory sticks. Once the stick is infected, the Stuxnet software runs itself on the computers that subsequently use the infected drive. The infection commences when the user simply clicks on the associated icon in Windows. This is a direct application of one of the zero-day vulnerabilities that Stuxnet leverages.

Another key security assumption Stuxnet invalidates is the trust relationship set in place by digitally-signed certificates. In order to provide more stability, modern operating systems, including Microsoft Windows, limit a computer program‟s access to system components. A normal program requests systems calls to hardware via driver software. As such is the case, the driver software has more access to lower-level system components than other programs. To avoid the easy creation of malicious driver software, Microsoft Windows relies on digitally signed certificates. In order to prevent detection by anti-virus software, Stuxnet uses legitimate digitally-signed certificates. This is another aspect of the malware that has not been previously observed. Early versions of Stuxnet used certificates by Realtek Semiconductor systems – later versions used certificates from JMicron Technology Corp. The use of these certificates gives the worm the appearance of legitimate software to Microsoft Windows. Security experts at ESET notes that both companies were based out of Taiwan and suspect that the certificates were stolen. Further, they believe it was most likely physical theft (perhaps even an inside job) as digital certificates for driver software are not commonly found on black-markets on the Internet.[49]

Implications for The Future

Stuxnet is highly significant – it is a next-generation piece of malware that poked flaws in existing security assumptions and was able to inflict damage on industrial systems that were outside the Internet. Let us consider two other attacks as a comparison. First, the Russian cyber-attacks against Georgia in 2008 relied primarily on botnets and activist hackers to conduct denial-of-service attacks against the Georgian Internet infrastructure[50]. These attacks resulted in Georgia temporarily losing its connection to the Internet, primarily during Russian conventional operations. While the methods of attack were well-known in the security community at the time, they were still significant due to its scale and that it occurred in tandem with conventional operations. However, the attacks against Georgia were targeting computer infrastructure – not SCADA. In many ways those attacks were a classic example of CNA (computer network attack) – the aim of the cyber activity was to degrade a computer network.

In a more recent cyber-operation known as Arora, Chinese hackers managed to penetrate the corporate networks of Google in December 2009 to steal information, including email accounts and possibly computer source code. Arora used a zero-day vulnerability in Microsoft Internet Explorer – taking advantage of a common application individuals use on a daily basis.[51] This particular cyber-attack is a good example of CNE – computer network exploitation as the attackers sought to steal information from the target.

[49] Matrosov, et. al., 13. Also see the related ESET technical blog post at http://blog.eset.com/2010/07/22/why-steal-digital-certificates (accessed 16 February, 2011).

[50] For more details on the Russian cyber-attacks on Georgia in 2008, see Stephen Korns and Joshua Eastenberg, "Georgia‟s Cyber Left Hook," *Parameters, Winter 2008-09, 60-76* and Paulo Shakarian, "Analysis of the 2008 Russian Cyber-Campaign Against Georgia," *Military Review,* to appear.

[51] Matrosov, et. al., 5.

Stuxnet differs from these two cases in several ways. Both the attacks on Georgia and Google were targeting computer networks directly or indirectly attached to the Internet. In either of those instances, a system disconnected from the network would have been unharmed. Not so with Stuxnet. This advanced worm had the capability to bridge the "air-gap." Network administrators charged with the security of such isolated systems face an interesting dilemma. In order to ensure that such systems are protected from the latest malware, they must periodically perform updates. However, in doing so, they run the risk of spreading an infection (i.e. by memory stick or through a local area network – both of which Stuxnet can propagate through).

Another key difference is that the targets in both Arora and the Georgian attacks were other computers. Stuxnet, on the other hand, inflicts minimal damage to information systems. Rather, its goal is to damage a piece of equipment in the physical world. The admission of the Iranians tells us that Stuxnet successfully affected a non-virtual entity. This is a significant advance in weaponry – a piece of software that only exists when a computer is turned on was able to successfully conduct sabotage in the real world. Stuxnet clearly demonstrates that cyber-weapons can play a significant role in operations – as opposed to the previous idea that such software can only amount to "weapons of mass annoyance."[52]

What are the implications of malicious software that can affect real-world equipment? There are numerous questions that must now be addressed. Recent Senate hearings in the wake of Stuxnet explore how the US can better protect its critical infrastructure from such attacks.[53] However, that is only part of the puzzle. There are many policy questions – some associated with cyber-warfare in general – that now take on increased importance.[54] How do we attribute such an attack? How do we respond to cyber-attacks on SCADA infrastructure by extra-governmental groups? How does the law of land warfare apply to cyber-weapons that cause real-world damage?

There are several operational and technical questions that must be answered as well. In the realm of cyber-warfare, technical and operational concerns often blend together. For example, how do we best identify zero-day vulnerabilities (which by definition are unknown)? How can we locate malicious software, such as Stuxnet, which was designed to go undetected? What security assumptions are we making that can be invalidated? How do we template an unknown cyber threat?

Will cyber weapons such as Stuxnet proliferate? Several security experts have predicted Stuxnet-like variants to become more common in 2011.[55] There have already been reports of non-Stuxnet cyber-attacks on industrial equipment in China.[56] It is noteworthy that the freely

[52] Noah Shachtman, "Terrorists on the Net? Who cares?" *Wired,* 20 December 2002, http://www.wired.com/techbiz/it/news/2002/12/56935 (accessed 16 February, 2011).

[53] For details on the November 2010 U.S. Senate hearing in the aftermath of Stuxnet, see http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=954c3149-042e-4028-ae23-754868902c44 (accessed 16 February, 2011).

[54] See Jeffrey Carr, *Inside Cyber Warfare* for a detailed analysis of these issues.

[55] Stuxnet-like attacks have been predicted by several computer security professionals, including Symantec Corporation (see MessageLabs Intelligence: 2010 Annual Security Report). Several experts also make such predictions in eWeek (http://www.eweek.com/c/a/Security/Stuxnet-Variants-Will-Wreak-Havoc-on-More-Information-Systems-in-2011-373179/) ComputerWeekly (http://www.computerweekly.com/Articles/2010/12/22/244626/StuxNet-prepare-for-worse-in-2011.htm).

[56] Fahmida Rashid, "Stuxnet-Like Trojans Can Exploit Critical Flaw in Chinese Industrial Software," *eWeek,* 12 January 2011, http://www.eweek.com/c/a/Security/StuxnetLike-Trojans-Can-Exploit-Critical-Flaw-in-Chinese-Industrial-Software-296674/ (accessed 16 February, 2011).

available analysis by Symantec, Kaspersky Labs, ESET, and Langner Communications GmbH, while useful from a defensive standpoint, can also be turned on its head and used as inspiration for Stuxnet-like worms.

By its nature, cyber-warfare changes quickly. Motivated individuals and teams from government, corporate, academic, and black-hat (hacker) communities are constantly scrutinizing systems for the latest vulnerabilities. However, Stuxnet represents a clear advance in state-of-the art both as a piece of software and in what it accomplishes. It has revealed flawed assumptions of security that need to be re-visited on multiple levels, but perhaps most important, it showed that software can also be used as a decisive weapon system.

References

Kupreev Oleg and Ulasen Sergey, *Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review,* VirusBlockAda, July 2010.

Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier Version 1.4.* Symantec Corporation, February 2011, 7.

David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Institute for Science and International Security (ISIS), December, 1.

Martin Brunner, Hans Hofinger, Christoph Krauss, Christopher Roblee, Peter Schoo, and Sascha Todt, *Infiltrating Critical Infrastructures with Next-Generation Attacks W32.Stuxnet as a Showcase Threat,* Fraunhofer SIT, December, 2010, 23.

Williamson Murray, *Thinking about Revolutions in Military Affairs*, Joint Forces Quarterly, Summer 1997.

Paul Barford and Vinod Yegneswaran, “An Inside Look at Botnets,” in *Malware Detection,* ed. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang, Springer, 2007.

Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, *Stuxnet Under the Microscope Revision 1.2,* ESET, November, 2010, 5.

John D. Fernandez and Andres E. Fernandez , “SCADA systems: vulnerabilities and remediation,” *Journal of Computing Sciences in Colleges*, Vol. 20, No. 4, April 2005, 160-168.

Thomas Brandstetter, “Stuxnet Malware,” *CIP Seminar,* Siemens, November, 2010.

Ralph Langner, “How to Hijack a Controller - Why Stuxnet Isn‟t Just About Siemens PLCs,” Control Magazine, 13 January, 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html (accessed 16 February, 2011).

Alexander Glaser, “Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected),” *Science and Global Security*, June, 2008, 14.

Timothy L. Thomas, “Google Confronts China‟s „Three Warfares,‟”*Parameters,* Summer 2010, 101.

Paulo Shakarian is a Captain in the U.S. Army and a Ph.D. candidate in computer science at the University of Maryland (College Park) and will soon take up a position teaching computer science at the U.S. Military Academy. He holds a BS from the U.S. Military Academy and an MS from the University of Maryland (College Park), both in computer science.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, United States Cyber Command, the Department of the Army, the Department of Defense, or the United States Government.