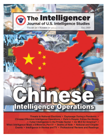

From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
Volume 26 • Number 1 • Fall 2020
$15 single copy price

Association of Former Intelligence Officers
7700 Leesburg Pike, Suite 324
Falls Church, Virginia 22043
Web: www.afio.com * E-mail: afio@afio.com

When Intelligence Made A Difference

— Post Cold War Era —

# Stuxnet

by Al Lewis

## Introduction

The revelations of the technical capabilities of Stuxnet were stunning and received much attention. But they pale in comparison to the significance it had on changing the landscape of modern nation-state engagement within the confines of cyberspace.

## Stuxnet

Iran's response, in 2006 to unsuccessful negotiations with the United States and European leaders was to resume its uranium enrichment program at the Natanz facility.[1,2] By 2008, engineers at the Natanz facility were experiencing a variety of malfunctions and breakages in their centrifuges.[3,4] The engineers experienced "low morale" as the seemingly inexplicable malfunctions, combined with political pressure to make an inherently complex process work, appeared beyond their reasoning.[5] The possibility of being the victim of a cyberattack was never considered, for two excellent reasons. First, the systems in the Natanz facility were air-gapped, therefore thought to be impenetrable to cyberattack. Second, no cyberattack had ever been capable of physical damage, and the centrifuges were experiencing physical damage.[6]

Discovered in 2010, Stuxnet is the name given to the most advanced computer worm written to date. A computer worm is a self-replicating software program designed to traverse from computer to computer across a network. In the case of Stuxnet, the worm contained four zero-day exploits. A zero-day is an unknown software vulnerability, making them both rare and valuable to an attacker. Furthermore, the worm was highly specific in its targeting, targeting only "a specific type of program used in Siemen's WinCC/PCS 7 SCADA control software."[7] "SCADA is an acronym for Supervisory Control And Data Acquisition, a category of computer programs used to display and analyze process conditions."[8] Additionally, the industrial controllers targeted were only those that were configured as a "cascade of centrifuges of a certain size and number (984) linked together…the exact setup at the Natanz nuclear facility."[9]

In 2010, the Congressional Research Service noted: "To date, no country or group has claimed responsibility for developing what has been termed by some as 'the world's first precision guided cybermunition.'"[10] However, the resources and skills needed to create and successfully infiltrate Stuxnet into its intended target indicate nation-state sponsorship. Initial analysis indicated that "countries thought to have the expertise and motivation of developing the Stuxnet worm include the United States, Israel, United Kingdom, Russia, China, and France."[11] Later, it was leaked to "have been a collaborative effort between US and Israeli intelligence agencies, known as 'Olympic Games'."[12]

The mission of Stuxnet was to penetrate the Natanz uranium enrichment facility in Iran and create the conditions to cause the centrifuges to fail.[13,14,15] The ability to infect air-gapped systems is

[1] DeIviscio, Jeffery, Parker, Diantha, Furst, David, Roth, Jeff, Huang, Jon, and Afkhami, Artin. 2017. "Iran, the United States and a Political Seesaw." *The New York Times. Archive.nytimes.com*. Accessed October 16, 2019. *https://archive.nytimes.com/www.nytimes.com/interactive/2012/04/07/world/middleeast/iran-timeline.html#/%23time5_206#time5_210.*

[2] Langer, Ralph. 2013. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," 7-8. The Langer Group. *Langer.com*. Accessed September 12, 2019. *https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.*

[3] DeIviscio, et. al. 2017.

[4] Gates, Guilbert. 2012. "How a Secret Cyberwar Program Worked." *The New York Times*. archive.nytimes.com. Accessed October 15, 2019. *https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?ref=middleeast.*

[5] Singer, P.W., and Friedman, Allen. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, New York, NY, p. 117.

[6] Singer and Friedman 2014, p. 117. In March 2007, the Idaho National Laboratory conducted a test of a simulated cyber attack on a large electrical generator. The "Aurora Generator Test" showed that a cyberattack could result in the physical destruction of hardware.

[7] Singer and Friedman 2014, p. 116.

[8] Langer, Ralph. 2013, p. 9.

[9] Singer and Friedman 2014.

[10] Kerr, Paul K., Rollins, John, Theohary, Catherine A. 2010. "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," p. 2. Congressional Research Service. CRS Report for Congress. R41524. *Crs.gov*. Accessed September 18, 2019. *https://assets.documentcloud.org/documents/2700120/Document-40.pdf.*

[11] Kerr, Rollins, and Theohary 2010, p. 2.

[12] Singer and Friedman 2014, pp. 117-8.

[13] Gates, Guilbert. 2012.

[14] Kerr, Rollins, and Theohary 2010, p. 4.

[15] Zetter, Kim. 2014. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*. Accessed October 15, 2019. *https://www*

so problematic that designing air-gapped systems remains a cybersecurity best practice. Nevertheless, the creators of Stuxnet were able to penetrate the air-gapped systems within the Natanz facility, thus introducing the worm into a controller computer.[16,17,18]

Purportedly, the Olympic Games operation set the Iranian nuclear capabilities back by "a year and a half or two years."[19,20] The first known instance of a cyberattack to cause physical damage in the real world, Stuxnet, has been referred to as "history's first field experiment in cyber-physical weapon technology."[21] Nevertheless, there was no cry of war, no suitable counterstrike, only a feeble attempt to downplay its effectiveness by the Iranian regime.[22] Stuxnet remains an enigma as it broke all convention crossing the cyber and physical barrier while seeming warlike and peacekeeping at the same time.

## Background

The impact of technology on warfare is comparable to the evolution of intelligence collection. In the book, *The Sling and the Stone: On War in the 21st Century*, author Thomas Hammes chronicles the generations of warfare. In doing so, Hammes lays out the role of technology in the advancement of military tactics. For example, maneuverability is the defining characteristic of the third generation of warfare.[23] The technological advances of "reliable tanks, mobile artillery, motorized infantry, effective close air support, and radio communications" surpassed the trench warfare of World War I, thus creating the conditions for a highly maneuverable fighting force.[24] Similarly, the creation of Information Communications Technologies (ICTs) has created the modern ecosystem referred to as cyberspace. These technologies have fundamentally changed the tactics of intelligence collection and the strategies that guide them.

As stated in the National Cyber Strategy: "America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace. Critical infrastructure, national defense, and the daily lives of Americans rely on computer-driven and interconnected information technologies. As all facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed, and new threats continue to emerge."[25] Similarly, the U.S. military recognizes five military battlespaces – land, sea, air, space, and cyberspace. As the world has grown in complexity and connectivity, traditional concepts that have defined military objectives, such as terrain and borders, have become increasingly blurred and ambiguous. "There are no longer battlespaces that operate independently, or more to the point, independent of cyberspace; as cyberspace is the battlefield from which all battlefields are amplified."[26] The Department of Defense (DoD) considers cyberspace to be "a part of the so-called information environment, defined as the 'aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[27]

The duality of cyberspace has enabled the ability to merge the disciplines of intelligence and operations.[28] Further, the underlying tradecraft of the respective disciplines now assumes a commonality when conducted through cyberspace. In other words, not only can they co-exist, they are two sides of the same coin. Inherent advantages of operating in cyberspace include the continuity of command and control across the lifecycle of an operation and the lack of definitive attribution to a specific threat actor. The first enables operational efficiency; the second provides plausible deniability. In the case of Stuxnet, the most significant intelligence victory of cyberspace remains behind a thin veil of deniability.

This article highlights how intelligence, leveraging an advanced technical asymmetric advantage, not only delayed Iran's nuclear proliferation ambitions but in doing so, created a new weapon for peace – Stuxnet. Importantly, Stuxnet not only ushered in a new

*.wired.com/2014/11/countdown-to-zero-day-stuxnet/.*

[16] Fidler, D. P. 2011. "Was Stuxnet an Act of War? Decoding a Cyberattack," 57. IEEE Security & Privacy 9, no. 4 (July 2011): pp. 56–9.

[17] Foltz, Andrew. 2012. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate," 44. *Joint Force Quarterly*: JFQ, no. 67 (October 1, 2012): pp. 40–8. *http://search.proquest.com/docview/1271860607/*.

[18] Kushner, David. 2013. "The Real Story of Stuxnet," 50. IEEE Spectrum. *Spectrum.ieee.org*. Accessed October 15, 2019. *https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.*

[19] Delviscio, et. al. 2017.

[20] "In 2019, various news reports indicated that the Stuxnet worm was implanted in 2007 by a human source recruited by Dutch intelligence. " 'Dutch Mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Israel," *The Times of Israel*, 3 September 2019."

[21] Langer, Ralph. 2013, 3.

[22] Fidler, D. P. 2011, p. 59.

[23] Hammes, Thomas X. 2004. *The Sling and the Stone: On War in the 21st Century*. Zenith Press, MBI Publishing Company, St. Paul, MN, p. 13.

[24] Hammes, Thomas X. 2004, p. 13.

[25] The White House. *National Cyber Strategy of the United States of America*, p. 1. Accessed September 29, 2018. *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf*

[26] Lewis, Al. 2019. "Houston, We Have a Problem: A Space Force Must First be a Cyber Force." *Modern Diplomacy*. May 10, 2019. *https://moderndiplomacy.eu/2019/05/10/houston-we-have-a-problem-a-space-force-must-first-be-a-cyber-force/.*

[27] Porche III, Isaac R., Sollinger, Jerry M., and McKay, Shawn. 2011. "A Cyberworm that Knows no Boundaries," 19. RAND. National Defense Research Institute. *Rand.org*. Accessed September 18, 2019. *https://assets.documentcloud.org/documents/2700122/Document-42.pdf.*

[28] This may be the reason why the director of NSA and the commander of CyberCom have remained the same person.

era of cyber weaponization but ushered in a new era for how nation-states are to conduct political warfare[29] through punctuated deterrence.

Punctuated deterrence is "an approach that accepts the possibly insurmountable limitations of denial while rejecting the policymakers' pervasive obsession with absolute prevention. Instead, it calls for more flexible logic of punishment that addresses not single actions and particular effects, but series of actions and cumulative effects".[30] No defense is impenetrable. In cyberspace, the advantage favors offensive operations. By accepting a level of adversarial success, the defense becomes free to allocate limited resources to the most critical areas, rather than the strategy of attempting to protect everything, all the time, from everyone. Punctuated deterrence changes the economics for the attacker.

Stuxnet serves as a modern example of cyber diplomacy. As negotiations surrounding Iran's nuclear program faltered, Iran countered with a renewed emphasis on its uranium enrichment program. In the context of punctuated deterrence, the creators of Stuxnet recognized the inevitability of Iran continuing its nuclear program; therefore, they sought to change the economics by not only inhibiting its acceleration but through the demonstration of a capability far beyond that of the rest of the world's cyber-powers, let alone, Iran. The message was clear, the continuation of the program, without negotiations, will be countered, possibly with previously unknown capabilities.

## Conclusion

The ability for one nation to impose its will on another, absent a war, is political nirvana. Cyberspace offers nations a low-risk and high-reward ability to impose their will on others, which means that cyber conflict has become the de facto method of engagement for nation-states to wage political warfare. Stuxnet was not only a first in cyber weaponization, but it was also a harbinger of how nation-states will conduct political warfare going forward. In this regard, Stuxnet symbolizes an intelligence and covert action victory of the highest order, offering the ability to engage nation-states behind a cloak of secrecy to further a national agenda.

Al Lewis is a doctoral candidate in Strategic Intelligence in the School of Security and Global Studies at the American Military University. He oversees the Cybersecurity Operations Center of Boeing. Before that he served as a Special Agent in the Secret Service.

[29] Blank, Stephen. 2017. "Cyber War and Information War a' la Russe." *Understanding Cyber Conflict*: 14 Analogies." Washington, D.C.: Georgetown University Press. Ch. 5, 81 – 98.

[30] Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven Yale University Press, p. 196.