SPENCER STUCKY is a third year political science major with a concentration in global politics. Spencer is heavily involved in extracurricular activities at Cal Poly, including being a member of Delta Sigma Phi and a volunteer in Panama in 2016. After graduating, Spencer plans to volunteer in Latin America and pursue a master's degree in international relations or public policy.

A WAR IN THE SHADOWS

Spencer Stucky

Introduction

On April 24, 2016, David Sanger of The New York Times reported that the United States military had recently launched cyber-attacks against the Islamic State of Iraq and Syria (ISIS) in an effort to broaden the methods of warfare aimed at toppling the regime.[1] The article outlines how until recently, U.S. Cyber Command, the military's cyber operations command, has yet to aim the technological weapons that have been traditionally used against nations such as Iran, North Korea, and Russia at ISIS.[2] Cyber Command plans to initiate this "new line of combat against" the terrorist organization alongside traditional military efforts that are being executed.[3] Specifically, the cyber-attacks will aim to "disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions,

[1] David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times,* April 24, 2016, https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0.

[2] *Ibid.*

[3] *Ibid.*

like paying its fighters."[4] Furthermore, through the acknowledgement of these tactics the U.S. military hopes to inflict psychological paranoia within ISIS as its leaders notice their plans, operations, and organization succumbing to technological sabotage.[5] The article notes that launching cyber weapons must be done with caution, but the time to open up a new front in the war against ISIS has begun to override those initial concerns.

The United States' decision to announce the use of such tactics against a foreign enemy represents a changing tide in warfare doctrine. Previously, all U.S. cyber operations were classified and the nation had never publicly announced the use of such weapons.[6] Thus, Sanger's article represents a shift in transparency regarding new domains of warfare. Perhaps more importantly, the article highlights that the U.S. does, in fact, use cyber weapons for offensive purposes. There have been suspicions in the past regarding cyber operations that could have potentially been carried out by the U.S. government. However strong the evidence may be, the U.S. has never admitted to such a tactic; until now. To put the scope of the U.S. cyber platform into perspective, the American populace generally believes that most agencies and programs operate on a purely defensive level. [7] Nonetheless, because the cyber security infrastructure in the U.S. is so expansive, many think otherwise: that operations go beyond simple defensive measures. The Sanger article chronicles a shift in United States cyber warfare as its use slowly begins to emerge from the shadows and into the light.

The layman's view sees cyber operations as purely defensive and in the interest of the protection of the country. In a recent poll by Gallup, 73 percent of Americans saw the presence of cyber activities as a critical threat to U.S. national security.[8] This highlights that a majority of Americans believe the nation is vulnerable to attack by cyber operations from other nations and organizations. Furthermore, this lends to the idea that the U.S. assumes a defensive position

[4] *Ibid.*

[5] *Ibid.*

[6] *Ibid.*

[7] U.S. Government. The Comprehensive National Cybersecurity Initiative. 2009. *Defense Technical Information Center.*

[8] "Americans Cite Cyberterrorism Among Top Three Threats to U.S.," *Gallup*, February 10, 2016, *http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx.*

in the field of cyber warfare and only acts in response to an aggressor's attack. In another poll taken by the Pew Research Center, 61 percent of respondents believed that a serious cyber-attack would cripple the society and infrastructure of a nation in the near future.[9] This poll serves to underline the consensus of alarm amongst the population that cyber warfare is an imminent threat and the U.S., among other nations, must take the necessary steps in order to protect itself. In general, both polls characterize the conventional wisdom behind cyber warfare: that the possibility of an attack is likely and the U.S. must pursue precautionary, defensive measures in order to ensure the security of the country.

Although the United States has developed a defensive cyber arsenal since the events of 9/11, this perspective is incomplete. There are, indeed, cyber programs that have been developed in the interest of national security and defense. However, this viewpoint does not capture the entire story. The United States has eclipsed defensive cyber strategies and developed and implemented offensive cyber operations aimed at sabotaging the infrastructure of groups and nations across the globe. The U.S. fleet of cyber programs has drastically expanded since the terrorist acts on September 11, 2001.[10] The U.S. has embarked down a path of aggressive cyber warfare that has slipped beneath the public's perception and been misunderstood for national security purposes.

The United States military's decision to pursue a path of offensive cyber warfare in the conflict against ISIS raises numerous questions and concerns. The implications of such an action range from ethical issues associated with privacy rights and technological sabotage to the further concentration of global political power in the U.S.'s hands. The act of launching an offensive cyber weapon opens the floodgates to an entirely new form of warfare. While still in its infancy, the potential strength of cyber operations is just beginning to be discovered and the U.S.'s decision to meddle in the structural and logistical arms of an enemy opens the door to unknown side effects. Not only does this decision alter the methods and direction of combat, but it also creates

[9] "Cyber Attacks Likely to Increase," *Pew Research Center,* October 29, 2014, *http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/.*

[10] Barton Gellman and Greg Miller, "Black Budget Summary Details U.S. Spy Network's Successes, Failures and Objectives," *The Washington Post*, August 29, 2013, *https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?utm_term=.31dd5c03d15e.*

potentially dangerous situations if this malicious data gets in the hands of the wrong people. For example, once a malicious code is created it remains in the domain of the World Wide Web and can be reused by whoever finds it to commit sabotage or espionage.[11]

The decision by the U.S. to conduct such operations highlights the military and technological strength of the country. The power of offensive cyber operations must not be overlooked and the potential for them to fall in the hands of the wrong people raises considerable alarm. No longer can these methods of warfare solely be considered defensive mechanisms for security. To better understand the scope and extent of the U.S.'s cyber warfare program, the following research question will be asked: How have United States cyber operations abroad evolved in the years following September 11, 2001?

Operation Olympic Games

Operation Olympic Games was an operation initiated by President George W. Bush and later carried out by President Obama aimed towards crippling Iran's nuclear capabilities.[12] The primary component within the program was a malicious virus, later named Stuxnet, which successfully infiltrated the Iranian nuclear facility at Natanz in 2010.[13] Alongside Stuxnet were malicious programs, Flame and Duqu, that are thought to have contributed to the overall operation.[14] The combination of Stuxnet, Flame, and Duqu made up the overall cyber strategy of Operation Olympic Games.

Between January and June of 2010, Iranian officials at the Natanz nuclear facility reported an unprecedented amount of failures among their centrifuges.[15] United States intelligence officials had discovered that scientists were

[11] Rachel King, "Stuxnet Infected Chevron's IT Network," *The Wall Street Journal*, November 8, 2012, *http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/.*

[12] Cyber Conflict Studies Association, "The History of Stuxnet: Key Takeaways for Cyber Decision Makers," *AFCEA*, June 4, 2012.

[13] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* June 1, 2012, *http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.*

[14] Ellen Nakashima, "Iran acknowledges that Flame virus has infected computers nationwide," *The Washington Post*, May 29, 2012, *https://www.washingtonpost.com/world/national-security/iran-acknowledges-that-flame-virus-has-infected-computers-nationwide/2012/05/29/gJQAzlEF0U_story.html?utm_term=.918c047822e0.*

[15] Ari Shapiro, "Documentary Explores The Cyber-War Secrets of Stuxnet," *NPR: All Things Considered*, July 4, 2016, *http://www.npr.org/2016/07/04/484713086/documentary-explores-the-cyber-war-secrets-of-stuxnet.*

being fired at the nuclear facility due to industrial miscalculations.[16] On June 17, 2010, Iranian officials contacted an outside cyber security firm to investigate a series of peculiar crashes their computers were experiencing.[17] The security firm, VirusBlokAda, based in Belarus, analyzed the computer malfunctions and identified the culprit as a large sequence of malicious code.[18] The company then contacted Microsoft – the creator of the interface by which the malware operated. Microsoft security experts began to file through the unusually large 1 megabyte of binary code, finding trailblazing complexities within the software. Soon thereafter, the connection between the malware identified on the servers and the industrial failures at the Natanz nuclear facility was made. Stuxnet, the world's most dangerous and sophisticated cyber weapon, had been discovered. The virus that had caused the malfunctions of the centrifuges was found within the computer network at Natanz.[19] The first ever cyber weapon had been successfully utilized to physically sabotage a target.

The original version of Stuxnet, which operated prior to 2010, was designed to block the release of pressure within the centrifuges.[20] Subsequently, this alteration in pressure would sabotage the nuclear enrichment process. This initial design of Stuxnet was intended to spread manually via USB stick and lacked the later qualities of self-replication.[21] However, after some time, officials at the nuclear facility "did change several important configuration details such as the number of centrifuges and enrichment stages per cascade."[22] These alterations in the enrichment process subsequently rendered the overpressure attack void. Additionally, the tactic of over pressurizing centrifuges led to some concern that the result could be catastrophic. Hence, the creators of the code abandoned the pressure attack and went to work on a new and improved code.

[16] *Ibid.*

[17] *Op. Cit.*, fn. 13.

[18] 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/.*

[19] *Op. Cit.*, fn. 18

[20] Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," *The Langner Group*, November 2013

[21] Paul K. Kerr, John Rollins and Catherine A. Theohary, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," *Congressional Research Service*, December 9, 2010.

[22] *Op. Cit.*, fn. 20.

The new version of Stuxnet was designed to attack the Centrifuge Drive System (CDS), targeting the rotor velocities of the centrifuges.[23] This version of the malware was slightly simpler in its objective: targeting the speed of the centrifuges instead of pressure. The new Stuxnet had the ability to not only spread via the manual use of USB sticks, but could also self-replicate. As noted by Ralph Langner in his technical analysis of Stuxnet, the malware now had the power to duplicate itself on machines "within trusted networks and via USB sticks even on computers that did not host the engineering software application."[24] Suddenly, the malicious code had been updated with an incredibly new powerful arsenal. It was now equipped with the, "latest and greatest MS Windows exploits and stolen digital certificates."[25] These zero-day exploits are undisclosed software vulnerabilities that hackers can utilize to adversely affect computer systems.[26] Specifically, the exploits allowed the virus to be more versatile and lethal, but came at a cost. It was this expansion in hacking vulnerabilities and self-replication that made the virus less secure and ultimately led to its discovery when Iranian officials noticed random shut downs and reboots on their computers.[27] Along with these multiple zero-day exploits, the malware had many diverse functions that included modifying system libraries, attacking Siemens' SCADA control software, and using rootkits.[28] Rootkits are, "clandestine computer programs" that allow an unauthorized user to access computer systems while going undetected.[29] By using rootkits, Stuxnet was able to collect information from the SCADA control software, which was responsible for visually displaying the physical and functional layout of the Natanz nuclear facility on computer screens.[30] Accessing the information on these SCADA screens was vital to understanding the layout of the facility and the industrial processes of the plant. It was this combination of functionalities that rendered Stuxnet so unique, effective, and complex.

[23] *Op. Cit.*, fn. 20.

[24] *Op. Cit.*, fn. 20.

[25] *Op. Cit.*, fn. 20.

[26] Kaspersky Lab, "What is a zero day exploit?" *USA Kaspersky,* 2016, *https://usa.kaspersky.com/internet-security-center/definitions/zero-day-exploit#.WMNLC2QrLR0.*

[27] *Op. Cit.*, fn. 21.

[28] Paul Mueller and Babak Yadegari, "The Stuxnet Worm," *Arizona Computer Science,* 2012.

[29] Neil DuPaul, "Rootkit: What is a Rootkit?" *Veracode*, https://www.veracode.com/security/rootkit.

[30] *Op. Cit.*, fn. 20.

The virus was purposefully and specifically designed to infiltrate the Step7 installations within the Siemens' SCADA control software.[31] These Step7 installations control the programmable logic controllers (PLCs) that are necessary to control the industrial processes. The Iranian nuclear facility at Natanz used this specific software for its industrial operations. Additionally, in order for the virus to be successful, it needed to understand the layout and structure of the building. Stuxnet's programming was catered to the layout of the Natanz nuclear facility, which was carefully pieced together over the years from insider information and the unintentional release of a photograph of former President Ahmadinejad during his tour of the facility in 2008.[32]

The enhanced form of Stuxnet operated periodically, about once a month, to avoid detection. The new directive of the cyber weapon was to speed up the rotors of the centrifuges which, by function, increases rotor-wall pressure. At Natanz, normal centrifuge rotor speeds hovered around 63,000 rpm, but the introduction of Stuxnet increased speeds to 84,600 rpm for approximately fifteen minutes. Other methods such as deceleration were thought to have been used if the initial high velocity speeds did not successfully sabotage all the uranium in the centrifuge. The operation is thought to have destroyed approximately 1,000 of Iran's 5,000 centrifuges in use and set back the nation's nuclear program by a couple of years.[33] This number might have been larger if computer analysts had not discovered the code so early on. Regardless, the operation was aimed at the long-term. The creators of such a code had the intention of a prolonged, slow process of manipulation, rather than a quick, violent destruction of Iran's nuclear capabilities.

As previously mentioned, Stuxnet had some assistance from other software. Both Flame and Duqu share striking similarities with Stuxent in their technical aspects and design.[34] Flame is perhaps the largest piece of malware ever discovered at six megabytes.[35] The intent of this malware was aimed more specifically at the collection of data through espionage. Spying activities such as activating webcams and microphones and colleting geo-locational data are

[31] *Op. Cit.*, fn. 20.

[32] *Op. Cit.*, fn. 20.

[33] *Op. Cit.*, fn. 20.

[34] Boldizsár Bencsáth, "Duqu, Flame, Gauss: Followers of Stuxnet," *BME CrySyS Lab*, 2012.

[35] *Ibid.*

just a few of its primary functions.[36] Quite similar but with a slight difference was the Duqu malware whose function was to collect information regarding industrial processes. More specifically, Duqu was a, “reconnaissance tool that researchers say was used to copy blueprints of Iran’s nuclear program.”[37] Given the functions of Flame and Duqu and the overall similarities in structure, these programs are thought to have supplemented Stuxnet and assisted in its overall operation.

The Culprits

Much ink has been spilled over who created such a project. While neither the United States nor Israel have claimed responsibility for the attack, there is sufficient evidence that points toward these two countries. The United States has pursued a route of nuclear non-proliferation and containment toward Iran for decades.[38] The U.S. wishes to deter nuclear powers, especially within the volatile Middle East, whilst supporting Israel’s defense and power within the region. Furthermore, the complexity and sheer size of Stuxnet led many professional software analysts to conclude that only a powerful nation-state could have created and conducted such an operation.[39] By process of elimination, the political motivations and grandeur of the malware point directly toward the United States. In Ralph Langner’s “To Kill a Centrifuge,” he argues that the operation against Iran was as much a nuclear non-proliferation tactic as much as it was a cyber-attack.[40] He goes on to say, “it is not even difficult to identify potential suspects for such an operation; nuclear non-proliferation is the responsibility of the US Department of Energy and since 1994 also of the Central Intelligence Agency.”[41] His remarks highlight the rational motive behind the United States undertaking such an operation.

In David E. Sanger’s article entitled, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” he chronicles a meeting in the White House Situation Room following the leak of the virus in which President Obama,

[36] *Ibid.*

[37] Nicole Perlroth, “Researchers Find Clues in Malware,” *The New York Times*, May 30, 2012, *http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.*

[38] Department of Defense and Department of Energy. September 2008. *National Security and Nuclear Weapons in the 21st Century.*

[39] *Op. Cit.*, fn. 21.

[40] *Op. Cit.*, fn. 20.

[41] *Op. Cit.*, fn. 20.

Vice President Joe Biden, and former CIA Director Leon E. Panetta discuss shutting down the operation.[42] Furthermore, Sanger goes on to note that his account of the US-Israeli operation to sabotage the Iranian nuclear program is, "based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program."[43] Sanger, a reputable journalist specializing in covert American programs, chronicles detailed information and interviews that exposes the US-Israeli joint effort in Operation Olympic Games. The facts and assumptions clearly point toward the United States and Israel as the primary culprits behind the masterful cyber weapon.

Conclusion

As presented above, it is quite clear United States' covert cyber operations have not only drastically expanded since 9/11, but have done so in an offensive manner. The complexity, sophistication, and grandeur of Stuxnet are a testament to the vast expansion and utilization of the United States' cyber arsenal. Furthermore, this repudiates the view that the U.S. is the victim in most cyber affairs, simply playing a defensive role in the interest of national security. Operation Olympic Games serves as a prime example of the proliferation and secrecy of U.S. cyber operations abroad in the wake of September 11, 2001.

The research presented throughout this paper serves to highlight the overall growth of the United States cyber arsenal. The offensive cyber-attack against Iran's nuclear facility merely scratches the surface of a larger agenda looming deep within the U.S. government. The U.S. has capabilities that stretch far beyond defensive measures; so far that in most cases the U.S. is the aggressor, instigating the cyber conflict. Since the terrorist attacks on 9/11, the United States has pursued a path that has resulted in the massive expansion of covert cyber operations and the subsequent growth of its industry.

On a broader scale, the use of such cyber operations has profound implications in the geopolitical realm. The U.S. deployed the first-ever digital weapon on Iran, forever altering warfare. The introduction of such a covert, powerful weapon has begun to change the methods of warfare and has spawned the emergence of the fifth warfighting domain: cyber space. Furthermore, the

[42] *Op. Cit.*, fn. 13.

[43] *Op. Cit.*, fn. 13.

extensive cyber platform currently utilized by the U.S. further concentrates hegemonic power within its hands. The scale of the global distribution of power continues to shift toward America as the nation demonstrates its strength on the global stage. Internationally, U.S. dominance in the cyber realm affects the decisions, policies, and security of nations around the globe. The power the U.S. exerts in the field of cyberspace has caused nations to implement cyber programs of their own. The attack has thus opened the floodgates to a digital age of warfare that has no bounds and few restrictions. Finally, the capabilities of cyber operations have instigated an ethical war between privacy rights and national security that has further contributed to the onslaught of unintended consequences. As the realm of cyber warfare expands, so too will the danger it poses to society.