CONTRIBUTOR BIO

SHAFALI RAJ is a fourth-year Political Science major concentrating in Global Politics and is pursuing a minor in Comparative Ethnic Studies. She is involved with the Liberal Arts college as a CLA Ambassador and is involved with the Political Science Department through the POLS Student Advisory Committee. Recently, Shafali joined AmeriCorps VIP and also completed an internship as a research and program development assistant for WITH US, where she is now serving as the organization's Education Coordinator and will begin full-time service next quarter. After graduating in Spring 2019, Shafali is eager to apply to graduate school and gain further experience in the NGO and non-profit sectors.
By Maure Gildea

Cyber: The Ultimate Political Weapon

Shafali Raj

Abstract

Cyber is one of the newest frontiers we face as a modern society. There are many unknowns when it comes to this intangible platform that has become shared globally. Political Science takes an interest in cyber because today it is used as a battle ground for attackers on the international scale. Our understanding of cyber warfare is still emerging, and much scholarship fails to discuss the usage of the United States' use of such weapons. This paper goes beyond a discussion of coders and hackers leaking into government data and instead focuses on the evidence of cyber as a weapon in world politics. Through three qualitative case studies, I will reveal the use of cyber for informational, psychological, and physical endeavors globally.

Introduction

On March 16th, 2018 Samantha Raphelson with *NPR* reported on accusations from the Department of Homeland Security on Russian involvement in various cyber-attacks on US power grids. The report released by DHS emphasized the imminent cyber threats and described them as attacks on energy, nuclear, water, aviation, manufacturing, and commercial facilities within the United States, perpetrated by actors from around the world.[1] One investigation detailed in the DHS report referred to the findings of American cybersecurity firm, Symantec, regarding a group named Dragonfly that broke into core operations of energy companies in the US and Europe.[2] Additionally, DHS official, Amit Yoran, describes other

1 Raphelson Samantha, "Report Russian Hackers Had the Ability to Shut Down U.S. Power Plants." National Public Radio (March 16, 2018)
2 Ibid

foreign attacks such as Russian meddling in public infrastructure and the 2016 election as "unprecedented and extraordinary" in the report.[3] Officials from the DHS as well as heads of cybersecurity companies stress the ability of Russians to interfere with critical US infrastructure, stating they have already employed attacks as far back as last March. Such findings prove the existence of cyber as a weapon.

The release of the DHS report represents change because it is the first time the United States government has openly held foreign actors accountable for a cyber-attack. The DHS report also discusses an imminent or impending threat using cyber weapons, which represents a shift in warfare to methods outside traditional means. This article specifically focuses on the open accusations and warning from the DHS on Russian attacks in various industries such as those on power grids in Texas.[4] Raphelson's story makes it apparent that security officials fear Russian attacks like those made on Ukrainian industries just two years earlier that were also mentioned in her article. However, it is important to contextualize these events. the United States continues to be a world power, leveraging its influence and capabilities to achieve certain goals. With this background in mind, the released DHS report become questionable, leading us to contemplate the real capabilities of the United States.

Yet this DHS report is important for world politics because the new strategies and intelligence stipulated by the United States will influence the actions of states all around the world. In addition, it poses the United States at the receiving end of a threat, which suggests cybersecurity is a top concern for the US and future policy decisions. This is the first time the United States has accused foreign actors such as Russia for outright interference in industry and political happenings and is momentous in the formation of future policy.[5] In addition, the DHS report does not address the fact the United States has been involved in and contemplated cyber-attacks such as those on the Iranian power grid.[6] The open discussion on cyber as a domain of war will change world politics forever as new weapons and methods enters the forefront of warfare. The report also does not consider accepted norms such as US military strength and its increased presence abroad, which leads me to ask the following research question, how does the United States utilize cyber as an

3 Ibid
4 Ibid
5 Ibid
6 Ibid

offensive weapon in world politics? I will answer this question by analyzing effects on environment, human rights, and labor standards.

Conventional Wisdom

The contemporary perceptions surrounding cyber threats is that most Americans are not confident in the United States' security capabilities. According to a *Pew Research Center* public opinion poll, seventy percent of Americans believe the United States will experience a major cyber-attack on public infrastructure within the next five years.[7] The same study found that only thirteen percent of participants feel that the United States government is "very" prepared for a cyber-attack. In addition, a poll performed by *Gallup* found that seventy-three percent of American adults ranked cyber-terrorism as a top three critical threat to US interests.[8] These two public opinion polls reflect the common feeling of insecurity amongst US citizens when it comes to matters of cyber. These findings present the conventional wisdom that the United States is not prepared for a cyber-attack or that the military has yet developed the tools to combat such threats.

However, the current conventional wisdom surrounding US cyber threats is extremely misleading. Most Americans are unaware of the capabilities the United States has developed and has already utilized. My research challenges the conventional wisdom regarding cybersecurity by exposing the uses of cyber as a weapon by the United States itself. Although common rhetoric puts the United States at the hands of foreign cyber threats, it is vital to understand that the United States remains a global power and is willing to utilize cyber in international politics. The released DHS report mentioned earlier might fuel paranoia amongst US citizens, but my research challenges the idea that the United States will be the victim of a crippling cyber-attack.

Case Study: Informational Cyber Tactics

Information warfare has been a legitimate strategy of the United States' military for decades and continues to be applied to new domains of warfare such as cyber. Unlike armed warfare, information warfare might take on more discrete forms and will always hold a political target. For instance, a Congressional Research Service Report defines information warfare through

7 "Americans and Cybersecurity," Pew Research Center (January 26, 2017)
8 "Americans Cite Cyberterrorism Among Top Three Threats to U.S." Gallup (February 10, 2016)

defensive and offensive operations such as "propaganda, misinformation, and disinformation."[9] Today, most information warfare is through cyber in the form of "botnets" or computers that are infected with a malicious software that can be used without the owner's knowledge. Social media has also become a contemporary platform through which information can be amplified to send a specific message and generate attitudes or confusion.[10] Social media is a perfect channel for information warfare because this strategy seeks to intensify the "fog and friction" or uncertainties each side experiences during times of war and peace by achieving political goals and controlling information.[11] Cyber has become the easiest means through which the United States can exercise information warfare, as new strategies of attack have been developed to include this domain. The Department of Defense has revealed and defined cyber operations to include activities such as "Cyber Network Attacks" which seek to "disrupt, deny, degrade or destroy information resident in computers and computer networks."[12] CNAs became an official part of cyber strategy when the Secretary of Defense, William Cohen, gave the NSA the authority to develop CNA techniques in 1997. Additionally, DOD policy outlines that the United States will employ a physical or non-physical attack "to provide support for full spectrum dominance."[13] Secretive documents such as DOD directives imply that the United States military and government *do* have the capability for offensive cyberwar. Moreover, the United States is ready and extremely willing to utilize cyber as a means for informational gain or stealing.

Through my research, I have found several pieces of evidence that demonstrate the bridge between cyber and information warfare the United States military has attempted to build. In 1997, William Black Jr. was appointed as the Special Assistant for Information Warfare and wrote the piece, "Thinking Out Loud about Cyberspace" for the National Security Agency.[14] Black emphasizes the recurring need for cyber technology in the NSA and the Informational Warfare unit itself at the time. This once-

9 Name redacted, Information Warfare: Issues for Congress, CRS Report No. R45142 (Washington DC: Congressional Research Service, 2018)
10 Ibid
11 Von Clausewitz, Carl, On War, Princeton University Press, June 1, 1989.
12 William B. Black, National Security Agency, "Thinking Out Loud About Cyberspace," *Cryptolog*, XXIII,1 (Spring 1997). Secret.
13 Ibid
14 Ibid

classified piece is an early indication of the integration of information warfare into the cyber domain. The National Security Agency in conjunction with other defensive units concluded that the primary method of conducting war in cyberspace is through Informational War tactics. In 1997, the NSA predicted the exploitation of computers and networks, which are troves of information, and set the agenda to include cyber a means of information dominance by exploring the term "cyber weapons." Offensive weapons for information war outlined by the NSA include "viruses, worms, logic bombs, Trojan horses, spoofing, masquerading, and 'trap' doors."[15] Although these are types of software and not a physical weapon, they have the power to destroy any nation's information infrastructure completely if utilized properly.[16]

In this case study, I will detail various instances of the use and development of cyber weapons for informational gains by the United States. In his book, *Dark Territory,* Fred Kaplan tracks the emergence of cyber units within the United States government such as the Department of Defense and the National Security Agency as well as their functions and strategies. These agencies work together to achieve goals that include acquiring information from interest nations or areas to promote an outcome ideal to the United States interests. A little-known US target to cyber-attacks was the Serbian military. In 1977, the US along with other NATO forces created the Stabilization Force (SFOR) to enforce the end of the Bosnia-Herzegovina war after the replacement of the president, Slobodan Milosevic.[17] This special force was enlisted to hunt war criminals and work in conjunction with US based agencies such as the NSA and J-39, a secret unit within the Pentagon's Joint Staff.[18] On March 24, 1999 NATO forces began a bombing campaign against the Federation of Yugoslavia which sought to ethnically cleanse the Balkan region. During the attack, US forces relied on spoofing techniques to intercept and stop military communications from the enemy. The specialized J-39 unit commanded hacks on the Serbian air defense system, sending false directions to aircrafts and relaying wrong informational updates. The changes were slight so that the Serbs could not detect their computer systems were interrupted by US commanded B-2 Spirit stealth bombers. "Spoofing" is when a person or program successfully imitates another by

15 Ibid
16 Fred Kaplan, Dark Territory(New York: Simon Schuster, 2016)
17 Ibid
18 Ibid

sending false data to the recipient and this is a basic example of how cyber is utilized as a tool by the US to gain a political/military advantage. This military operation ended in the bombing of Yugoslavia and allowed for US/NATO peacekeeping forces to enter the region. Since its inception in 1977, the SFOR and joint agencies have developed such offensive capabilities for informational gain in both military and civilian operations.

David Sanger with *The New York Times* reported in 2012 of another virus, Flame, in his article, "Obama Ordered Wave of Cyberattacks against Iran."[19] Flame illustrates a contemporary example of the US ability to steal, copy, and share information. This code was a continuation of the original US-created code named Duqu, which was a reconnaissance tool that could copy blueprints of Iran's nuclear program. The newer Flame virus sent a visible code onto Iranian officials' computer to essentially steal information on Iran's development of nuclear weapons.[20] No single state has claimed Duqu or Flame, but later findings suggest it was the work of the United States and Israel. The nature of these events insinuates a physical attack since a USB was manually inserted into these individuals' personal computers.[21] However, physical damage was just a secondary objective for these two cyber operations. Flame and Duqu were utilized as a covert method to steal information from Iran. It had the sole purpose of achieving a political goal just as any informational warfare operation. These instances prove to be unique, however. Cyber was the domain of warfare for this operation and in an effort to remain secretive; the code could not be traced to an original creator. This attack was successful, in that the computers affected were useless or had their information copied and shared.[22] Such events prove the efficiency and emergence of cyber offensive tools to fulfill tasks such as information gathering to achieve political gains.

Case Study: Psychological Cyber Tactics

Psychological warfare and its methods fall under the "umbrella" of information warfare. The psychological war strategy conducts covert missions or attacks to gain information. PSYOPS, or psychological

19 David Sanger, "Obama Ordered Wave of Cyberattacks against Iran," The New York Times(June 1, 2012)
20 Ibid
21 Nicole Perlroth, "Researchers Find Clues in Malware," The New York Times (May 30TH, 2012).
22 Ibid

operations, has become an integral part of military defensive and offensive plans. The Department of Defense directives define PSYOPS as operations "meant to induce foreign attitudes favorable to the originators cause."[23] Psychological warfare is not a new phenomenon and was a powerful tool throughout United States history. For example, during the Cold War, President Eisenhower deployed pamphlets and boosted programs such as Voice of America in Europe to change attitudes toward the Soviet Union through such offensive psychological warfare tactics.[24] Eisenhower's success reflects the possibilities and effectiveness psychological warfare can achieve if aided with new technology such as cyber.

PSYOPS came to the forefront of operations such as those during the Iraq War under the Bush Administration, which pushed for informational gains and the use of psychological war to attain new material and altern negative perceptions of the West.[25] A small number of cyber uses were stipulated by the military and US government but were not employed. These included possible plans in which an individual can have access to a weapon or tool that would target a specific computer or system and modify its functions/ information it receives and spreads. Other plans detailed how a PSYOP team could develop a website for an audience in Iraq so that behaviors can change indirectly.[26]

My research indicates that psychological tactics have played a large role in United States military operations in the past and will continue to do so in the future. The United States Army Field Manual explicitly states that PSYOPS "are meant to change the behavior of a foreign target audience to support U.S. national objectives."[27] In 2005, the tasks of PSYOPS soldiers were written to be to develop, design, produce, distribute, disseminate, and evaluate psychological war materials and tools.[28] Cyber can be used in the

23 Name redacted, Information Warfare: Issues for Congress, CRS Report No. R45142 (Washington DC: Congressional Research Service, 2018)
24 Kenneth A. Osgood, Form Before Substance Eisenhower Commitment to Psychological Warfare and Negotiations with the Enemy, Diplomatic History
25 Christopher J. Lamb, "Review of Psychological Operations Lessons Learned from Recent Operational Experience," (Washington DC: National Defense University Press, September 2005).
26 Ibid
27 Department of the Army. "Tactical Psychological Operations: Tactics, Techniques, and Procedures," (Manual, Department of the Army, Washington DC, October 28, 2005)
28 Ibid

form of social media and the Internet, for example, by interfering with the interactions and information an individual receives. The Internet has become increasingly utilized as a means of achieving psychological war through cyber. The United States has ownership of the Internet and has utilized it as a tool for democracy in nations all over the world. For example, after bombing Yugoslavia with NATO forces, the US decided to allow Serbians to maintain access to the internet to allow the people to see the atrocities committed in Kosovo by the Milosevic regime.[29] Additionally, the Serbian government attempted to stop the independent radio station, B92, from organizing protests. When this occurred, B92's transmission was broadcasted to the Internet and relayed back to Serbia by the British Broadcasting Channel and Voice of America radio stations.[30] This case demonstrates the US's attempt to bolster Serbian support after an exploitative and violent US venture and displayed the ease of utilizing cyber for a political gain through an everyday institution such as the Internet.

Similarly, a contemporary use of psychological warfare through means of cyber can be seen through Operation Iraqi Freedom during the Iraq war. During Operation Iraqi Freedom, the United States employed various methods to gain US support in Iraq against troubling political figures such as Saddam Hussein.[31] During this operation, broadcast messages were sent from Air Force plane, EC-130E and from Navy ships operating on the Persian Gulf. These messages were accompanied by a barrage of emails, faxes, and cell phone calls to numerous Iraqi leaders.[32] The message being sent by US forces was to abandon Saddam Hussein. In hopes of changing public opinion, the US military led Operation Iraqi Freedom utilizing cyber and psychological warfare. Military Deception or "MILDEC" is a strategy used by the United States army that relies on sending false signals to the enemy. Deception is a primary part of psychological warfare in that it keeps

29 Briscoe; Jon Swartz, "Administration Drops Idea of Blocking Serb Net Sites," The San Francisco Chronicle, 15 May 1999: in Eden-Webster Passports/Lexis-Nexis [database online], World News library.
30 David J. Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age," Journal of International Affairs 51 (Spring 1998): in Columbia, International Affairs Online [database online], (9 January 2001).
31 Catherine Dale, Operation Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress, CRS Report No. RL 34387, (Washington DC: Congressional Research Service, 2008)
32 Ibid

the enemy or public unaware of reality or of future outcomes.[33] During Operation Iraqi Freedom, the United States used deceptive methods such as the Navy's Tactical Air Launched Decoy system. This tool could divert fire from Iraqi air defenses using a digital capability, making aircrafts unsure of the target or source of attacks in the sky. The United States' attempts display that offensive methods, coupled with discrete operations such as building fake websites, yield the strength and magnitude to influence the political objectives/opinions of individuals.

Psychological operations are critical to the United States' endeavors and is deployed abroad and domestically. Today, the US counts on the Media Operations Center at Fort Bragg, which is accountable for printing and disseminating audio, video, and print psychological operation products.[34] Since the actual production of psychological warfare materials are done domestically, there must be an efficient and overt method of spreading this information abroad. Cyber is a primary means of deploying such materials through social media and satellite communications.[35] Additionally, Deployable Audio Production Systems is a technology widely used in PSYOPS. Missions can be carried out with SOMS B vehicles have the capacity to create audio and video in the air which can then be shared using DAP technology. One of the first uses of this technology was in Afghanistan (2001) when The Commando Solo aircraft transmitted pro US radio broadcasts.[36] Since its first use, the Commando Solo, alongside SOMS B, have been vital to US interests in bolstering support in the Middle East. These are just a handful of cyber technologies that make the spread of psychological warfare materials efficient and possible beyond conventional methods.

Case Study: Physical Cyber Tactics

The Department of Defense defines the cyberspace domain as consisting of three interdependent "layers" including the physical, the logical, and the cyber persona. "Physical" refers to the environment of devices and the

33 Clay Wilson, Information Operations and Cyberwar: Capabilities and Related Policy Issues, CRS Report No. RL31787, (Washington DC: Congressional Research Service, 2006)
34 Christopher J. Lamb, "Review of Psychological Operations Lessons Learned from Recent Operational Experience," (Washington DC: National Defense University Press, September 2005).
35 Ibid
36 Ibid

geographical location of these systems.[37] This is the network of people and materials. Therefore, a physical attack can also be on a computer or a system that causes a degradation of the material item itself.[38] This is a strategy that carries a human aspect because it requires one's presence and compliance to attack another entity. Past events of physical cyber-attacks suggest these types of operations carry a specific target and are motivated by a material or political gain since the nature is destructive and deliberate. A contemporary example of this would be the Stuxnet malware which stunted Iran's development of nuclear weapons by stopping uranium enrichment processes in nuclear facilities.

In 2010, fifteen plants across Iran reported technical failures and difficulties in nuclear plant processes. These malfunctions were later found to be the result of "Stuxnet," a malicious software and the first known "cyber weapon."[39] This event is also considered the first "act of force" using cyber. Stuxnet was the only malicious software of its kind, specifically designed to interact with and destroy a *nuclear* Industrial Control System. The Stuxnet code targets a Microsoft application that the nuclear ICS devices use daily during uranium enrichment operations. That being said, the virus can enter devices through a USB or gaps in internet connection. However, the nature of Stuxnet implied that it must have been implemented *in person* at the facilities or by an insider. Stuxnet is significant because it was the first code that set out to inhibit the production of nuclear materials. It was also a part of a larger campaign for offensive cyber operations entitled, Operation Olympic Games. This operation began under the Bush Administration in 2006 and continued under Obama as a cyber-campaign against Iran, which was made possible with the help of US friendly, Israel.[40]

Operation Olympic Games was a secretive joint effort made between the US and Israeli governments to cripple and destabilize Iran's nuclear program entirely. Cyber was the chosen domain of warfare for this operation and *cyber weapons* were central to the plan of Olympic Games.[41] This revelation

37 Catherine Theohary and Anne Harrington, Cyber Operations in DOD Policy and Plans: Issues for Congress, CRS Report No. R43848 (Washington DC, Congressional Research Service, 2015)
38 Ibid
39 David Sanger, "Obama Ordered Wave of Cyberattacks against Iran," The New York Times(June 1, 2012)
40 David Sanger, Confront and Conceal (Broadway Books, June 2012)
41 Ibid

starkly contrasts the notion that the United States is a victim to cyber threats given its role in the first contemporary mass cyber-attack. Eventually, cyber and tech experts from around the world revealed the dark components of the virus. This code held features described by scholars as "*dual warheads,"* that remain dormant and send false signals to computer systems signaling that things are running normally when they are not.[42] The code is a weapon in every way given its precise duty and properties. One part was designed to specifically command 984 machines linked together. This is the same number of downed uranium- enrichment centrifuges, inspectors at the Natanz plant reported following the attack.[43] With these attributes, Stuxnet was truly the first cyber-weapon, enabling a physical attack on a political target. The realities of the Stuxnet attack contradicts the notion that the US is only developing weapons and not utilizing harmful offensive components. Stuxnet was formulated not to only send a message, but to destroy the enemy target just as any military operation might seek to do.

Stuxnet was used as a weapon against Iran for the advancement of US political goals in that it delayed Iran's nuclear program by downing almost 10,000 Industrial devices. Furthermore, I have found several manifestations of the intent and use of cyber weapons as a part of a political/material gain by the United States. In 2017, The United States-Israel Cybersecurity Cooperation Enhancement Act passed the House of Representatives. This bill requires The Department of Homeland Security to create a fund limited to US and Israeli citizens for research and development on cyber protection, response, and strategies.[44] The adopted amendment provides for a "Cyber Center of Excellence," for the development of new capabilities. This example directly displays the intent to continue developing and using cyber strategies or weapons on a political target.[45] The strategic relationship with Israel can be applied to any other country the US seeks intelligence from in developing new capabilities of warfare such as cyber weapons. This update indicated that the US is willing to negotiate and work with other nations to

42 Paul Kerr, John Rollins, Catherine Theohary, The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability, CRS Report No. R41524 (Washington DC: Congressional Research Service, 2010)
43 Ibid
44 [1]U.S. Congress. House of Representatives. Cybersecurity Cooperation Enhancement Act. 2017. 115thCongress.
45 The American Israel Public Affairs Committee, "Bill Summary Cybersecurity Cooperation Enhancement Act," (March 2018)

create offensive cyber strategies on specific political targets such as Iran. Through my research, I have found the intent of the United States has not changed since the inception of Operation Olympic Games in 2006. These are just a few examples that have been exposed as linked to US intelligence and military operations but there are still many unknowns.

Implications

With the emergence of cyber, leaders are faced with new issues and challenges their predecessors did not have to contemplate. Stuxnet is an important example for world politics in that it was the first well-known cyber weapon and was able to conduct a physical threat and influence later events. I believe the United States must take accountability for developing these technologies. The United States set a precedent by utilizing cyber for physical, psychological, and informational gains and must be responsible for the repercussions. Both states and independent actors have learned from the US example. As cyber becomes a legitimate domain of war, it is inevitable states will compete for the most powerful cyber weapons. This leads me to question, just how far the US and other states are willing to go for cyber dominance. History reveals that weapons such as the nuclear bomb had the power to change history forever. I can imagine a cyber-weapon of this magnitude as being possible in the future.

Addressing US cyber offensive strategies is vital in recognizing the power and influence of the United States in areas such as military strength. Although common rhetoric puts the United States at the hands of foreign cyber threats, it is vital to understand that the United States remains a global power and is willing to utilize cyber in international politics. The US has proven its willingness to use cyber weapons through these three case studies. As cyber weapons are increasingly developed and utilized, the public remains unaware. Today, top news stories detail foreign involvement in the US political process through the Internet and social media outlets. These recent events signal that cyber-attacks or war is increasingly viable and can be hidden for long periods of time. This leads me to ask the future capabilities of sabotage by the United States and foreign actors as well in addition to attacks the public might never know about. Therefore, it is important that instances such as Stuxnet are discussed for security and the formation of future policy or norms.