HIGH SCHOOL EDITION
Journal of Student Research
Volume 11 Issue 2 (2022)

Cybersecurity Policies and International Relations: The Case of the US and Iran

Ryan Aminloo[1] and Tyler Vitone[#]

[1]Portola High School, Irvine, CA, USA
[#]Advisor

ABSTRACT

One area of increased attention for defense departments around the world is the area of cybersecurity. This paper takes two very different players in cybersecurity--the US and Iran--to outline their general approaches, find areas of potential conflict, and outline confrontations that may be possible in the future. In this sense, this paper makes a wider contribution to the many ways in which states are pursuing cyber goals today and also contributes to the discussion of how even non-allied states might work together in this sphere.

Introduction

Increasingly in the twenty-first century, the relationship between the United States and Iran has been one that has become more and more contentious. For instance, on January 3, 2020, tensions between the US and Iran reached new heights, after the US assassinated Iranian general Qasem Soleimani. This incident was one of many examples of raised tensions between the two countries, just in this century. Within these rising tensions, perhaps the area that is most contentious is the area of cyberspace. Cyber security is a major concern everywhere. But particularly, in recent years, it has been used by both the US and Iran as a means by which to further their wider foreign policy goals.

This paper examines cyber policy in both states individually and in conjunction to begin assessing the importance of cyber to US-Iranian relations. Critically, this paper argues that when it comes to cyber, the US and Iran are following their conventional foreign policy procedures. When looking at the bridge between foreign policy and cyber policy for each nation, it is clear that their foreign policy goals are aligned with their cyber goals. For example, back-and-forth cyberattacks between the two nations have mimicked the wider dynamic of the US-Iran relationship.

In some ways, this paper aligns with other studies of cybersecurity. In one aspect, however, this consideration of US-Iranian cyber relations stands out: specifically, scholars typically address cyberspace in a way that fails to consider the result of the US-Iran cyber relationship. First, what is lacking in existing scholarship is a study that compares the US and Iran directly. This paper addresses this gap in the literature by comparing the cyber policies and actions of both countries. Typically, scholars writing on cyber look narrowly at only one small part of the entire cyber policy for either country. For example, Jacquelyn Schneider has analyzed concepts like “no first use” and “defending forward”[1] rather than holistically considering both countries’ strategies. Because of this focus on one particular slice of the policy, scholars have missed out on critical insights about the relationships between conventional foreign policy and cyber policy. Second, when it comes to Iran and the US, scholars have examined the single biggest confrontation between the two countries: the cyber attack dubbed “Stuxnet.” Although this attack is crucial to study, these reports, such as the recent one by Ralph Langner, have focused more on the technology and have lacked the wider context of

[1] Jacquelyn Schneider, “A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem,” *The Washington Quarterly* 43 (2020), https://www.tandfonline.com/doi/abs/10.1080/0163660X.2020.1770970?journalCode=rwaq20&.

the relationships between the two countries or the bigger foreign policy goals behind the attack.[2] This paper addresses this gap in scholarship by placing Stuxnet within its wider context, both within the US and Iran and also in the relationship between the two countries.

This paper begins by exploring the goals and capabilities of the United States in the Middle East, with an eye toward the role that cyber security plays in these foreign policy goals. In particular, this section explores how the US has wanted to maintain a foothold in the Middle East to counter Iran. The section proves how the long-standing idea of maintaining order through US power also applies in the cyber domain, making cyber increasingly important to the US in the region. The US has dedicated more attention and resources to its cyber capabilities in order to compete with Iran (along with other adversaries of Russia and China). Next, this paper turns to Iran and similarly shows its foreign policy goals along with its behaviors and strategies in cyberspace. The main takeaway is that Iran has done and will do whatever is necessary to achieve its biggest foreign policy goal, which is to change the power balance in the Middle East to align with its interests. That means that Iran is also dedicating its time and resources into its own cyber capabilities. The third part then examines the cyber relationship between the two states and how their two strategies interact with each other in practice. This relationship is illustrated through Stuxnet. Ultimately, this paper shows that cyber is becoming a new focus to continue traditional foreign policy aims for both the US and Iran.

Section One

Subsection One: US Foreign Policy Interests in the Middle East and Iran

The Middle East is a complex region for the United States. The US sees it as a region in which they need to have a presence in order to deter possible conflict and stabilize the region in a way that protects the US itself. The US turned its attention to the Middle East after WWII when American strategists realized that the US must discourage any hostile nation whose goal is to dominate a region of high geopolitical and material significance.[3] The Middle East fits that definition of being a region of high geopolitical and material significance in three ways.

One way the Middle East is critical to US foreign policy interests is via energy supply and oil. Approximately ten percent of US total oil reserves come from Persian Gulf countries. Of these countries, Iran has the fourth-largest oil reserves in the globe and the second largest in the Middle East.[4] Iran's vast oil reserves put pressure on the United States to not make hasty decisions. In the Iran-Iraq War of 1980-1988, American intelligence reported in 1982 that Iraq was on the verge of collapse. The US aided Iraq to push back in order to avoid Iranian control of the Persian Gulf and its huge oil reserves.[5] In addition, the Strait of Hormuz is a point of contention. This strait in the Persian Gulf is one of the world's most important chokepoints in global trade. It is mostly controlled by Iran, but countries like the US make sure that Iran can't threaten the flow of oil around the globe by militarizing the strait. The US needs to be in the Middle East to reverse the Iranian military buildup in the strait to avoid economic repercussions.[6]

---

[2] Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy* 9, no. 3 (2011), https://ieeexplore.ieee.org/abstract/document/5772960.

[3] Hal Brands, "Why America Can't Quit The Middle East," no. 1921 (March 21, 2019), https://www.hoover.org/research/why-america-cant-quit-middle-east.

[4] "OPEC Share of Crude Oil Reserves, 2018," n.d., https://www.opec.org/opec_web/en/data_graphs/330.htm.

[5] Seymour Hersh, "U.S. Secretly Gave Aid to Iraq Early in Its War Against Iran," *New York Times*, January 26, 1992, https://www.nytimes.com/1992/01/26/world/us-secretly-gave-aid-to-iraq-early-in-its-war-against-iran.html?pagewanted=1.

[6] Janae Diaz and James Di Pane, "Iran Is Targeting the Strait of Hormuz. The World Needs to Take Heed.," *The Heritage Foundation*, October 22, 2020, https://www.heritage.org/middle-east/commentary/iran-targeting-the-strait-hormuz-the-world-needs-take-heed.

In addition, there are more geopolitical incentives for the US to have one foot in the Middle East. Iran is considered to be a destabilizing actor in the Middle East. The US has counterbalanced the Iranian threat by allying itself with Arab governments friendly to the United States and militarily assisting Israel to bolster their defense.[7] The US has been doing this since the Cold War era, where the Nixon Doctrine dictated the "twin pillar policy" in the Middle East. Back then, however, the US kept Iran and Saudi Arabia as their "pillars." After the Iranian Revolution in 1978, Iranian hostilities grew into the highly frictional relationship that the US and Iran have today because of the removal of a regime that was in favor of friendly relations with the US as well as a disenchanted Iranian population.[8] Today, Iran also makes use of its anti-Western ideology by funding groups like Hezbollah,[9] which the US State Department has named a "Foreign Terrorist Organization."[10]

The third key reason as to why the US continues to occupy the Middle East is the threat Iran poses to the rest of the Middle East and even the world through its nuclear program. Iran's behavior could be grave and this notion has shaped US foreign policy towards Iran. Iran is in breach of numerous anti-nuclear laws like the Nuclear Non-Proliferation Treaty and refuses to take part in a UN proposal for the Middle East called MENWFZ (Middle East Nuclear-Weapon-Free Zone).[11]

Subsection Two: US Cyber Strategy

The Department of Defense (DoD) has only recently laid out its cybersecurity framework that consists of different mechanisms as well as procedures. According to the DoD's 2018 unclassified summary of the cyber strategy, there are five overarching priorities. The first is to build a more lethal Joint Force. This consists of ramping up cyber capability development, innovating what exists, utilizing intelligence to improve effectiveness, and using commercial-off-the-shelf software to constantly secure when needed. The second goal is to preserve our "peace through strength" motto, a phrase coined by former US President Ronald Reagan, by consistently competing in cyberspace. This means deterring malicious activity from any adversary (organization or country), defending forward when the US comes across malicious activity, and increasing the resilience of US infrastructure. The third goal is to strengthen current alliances and potentially create new ones. This incorporates building private sector partnerships since they hold much of US infrastructure, information sharing with international partners to create combined cyberspace operations, and adhering to the international norms of cyberspace. The fourth goal is reforming the basic ideals of the DoD which means making cyber awareness a core foundation for the DoD. The fifth and final goal is cultivating talent within the department's workforce by increasing cyber talent and ensuring career progression of cyber personnel.[12] These goals show how the DoD is increasingly invested in cyberspace and also show how cyber concerns have become a major focus in national security.

---

[7] Stephen Zunes, "Why the U.S. Supports Israel," *Institute for Policy Studies*, May 1, 2002, https://ips-dc.org/why_the_us_supports_israel/.

[8] Krysta Wise, "Islamic Revolution of 1979: The Downfall of American-Iranian Relations," *Legacy* 11, no. 1 (n.d.), https://opensiuc.lib.siu.edu/legacy/vol11/iss1/2/?utm_source=opensiuc.lib.siu.edu%2Flegacy%2Fvol11%2Fiss1%2F2&utm_medium=PDF&utm_campaign=PDFCoverPages.

[9] "State Sponsors of Terrorism," *U.S. Department of State*, n.d., https://www.state.gov/state-sponsors-of-terrorism/.

[10] "Foreign Terrorist Organizations," *U.S. Department of State*, n.d., https://www.state.gov/foreign-terrorist-organizations/.

[11] François Carrel-Billiard and Christine Wing, "Iran and the NPT," n.d., https://www.ipinst.org/wp-content/uploads/2010/04/pdfs_iranchapt.pdf.

[12] "Department of Defense Cyber Strategy 2018," *Department of Defense*, n.d., https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Alongside DoD investment in cyberspace, other branches of the government have also passed laws encouraging US action in cyberspace. The US is tactfully setting itself up to conduct offensive preventive cyber operations through various legislation like the 2019 National Defense Authorization Act, which (1) established cyber-surveillance as a "traditional military activity" and (2) gave the authority to deter and disrupt cyberattacks from adversaries like Iran. Former President Donald Trump proceeded to create a cyber operation process that parallels the goals of defending forward called the National Security Presidential Memorandum 13. It essentially allows for the use of offensive cyber operations.[13] The Former President also signed the Cybersecurity and Infrastructure Agency Act in 2018 which reappropriated resources and redesignated the Department of Homeland Security's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency.

Section Two

Subsection One: Iran Foreign Policy Interests in the Middle East and the US

Iran is a forceful power in the Middle East with an agenda that often contradicts those of its neighboring nations and the US. Iran believes that it should be recognized as a major power in the region and its ultimate goal is to overturn the power structure of the Middle East which currently favors the US and its allies.[14] It is important to recognize the driving force behind Iran's efforts-- prioritizing regime survival and, in intended consequence, destabilizing the Middle East. Iran has many options for attempting to change the balance of power in the region; among these, Iran's government has prioritized three.

The first way Iran works to survive and become a major power is its making of political alliances, whether for religious or strategic reasons. Iran has expressed commitments to nations that are pro-Iranian and Shiite in the Middle East. One example is the Iranian support of President Bashar Al Asad of Syria. Iran has provided intelligence, communication, training, and weapons to Syria.[15] Syria has even secured $5 billion in credit lines directly from Iran since the start of the war in Syria.[16] In addition, Iran has tactfully allied itself with Turkey despite Turkey once being a believer that Al Asad should be ousted. Turkey has since realized that Al Asad is likely to remain in power and, therefore, has strengthened economic and diplomatic ties with Iran. Iran and Turkey have also united in the common goal of halting border attacks from Kurdish groups.[17] A third example is Iran's efforts to manipulate the re-emergence of the Iraqi state in a way that favors the future of Iran.[18] On the other hand, Iran has also butt heads with US allies in

[13] Samantha Ravich and Ed Cardon, "Defending Forward in the Cyber Domain," *Foundation for Defense of Democracies*, n.d., https://www.fdd.org/analysis/2020/12/15/defending-forward-defending-forward-in-the-cyber-domain/.
[14] Itamar Rabinovich, "How Iran's Regional Ambitions Have Developed since 1979," *Brookings Institution*, January 24, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/01/24/how-irans-regional-ambitions-have-developed-since-1979/.
[15] Madyson Hutchinson Posey, "Here Are 4 Ways Iran Is Destabilizing the Middle East," *The Heritage Foundation*, October 16, 2017, https://www.heritage.org/middle-east/commentary/here-are-4-ways-iran-destabilizing-the-middle-east.
[16] Claire Brenner, "Iran's Destabilizing Activities in the Middle East," *American Security Project*, March 5, 2021, https://www.americansecurityproject.org/irans-destabilizing-activities-in-the-middle-east/.
[17] "Iran's Foreign and Defense Policies," *Congressional Research Service* R44017 (January 11, 2021), https://fas.org/sgp/crs/mideast/R44017.pdf.
[18] "Iran's Networks of Influence - Chapter Four: Iraq," *International Institute for Strategic Studies*, November 2019.

the region and sees itself as an ideological rival to Gulf Cooperation Council countries, especially Saudi Arabia.[19] These are all part of Iran's plans to present itself as a better partner than the US while also conflicting with pro-US governments.

The second way Iran has presented itself as a power in the Middle East is through its nuclear program. The Iranian thought process is that nuclear capabilities reduce Iran's vulnerability to invasion or to attempts to overthrow the government. In the last decade, the members of the United Nations Security Council believed that to unwind Iran's nuclear program, it was necessary to make a pact that implemented nuclear restrictions on Iran to prevent a Middle Eastern and global crisis. These restrictions limited the number of centrifuges Iran could operate, and Iran had to agree to Internal Atomic Energy Agency (IAEA) inspections. In exchange, the European Union, United Nations, and the US agreed to alleviate sanctions on Iran. This nuclear agreement was called the Joint Comprehensive Plan of Action (JCPOA) and went into effect in late 2015. However, despite initial 2016 inspections clearing Iran, former President Trump withdrew from the JCPOA due to the belief that the agreement did not respond to Iran's ballistic missile program and intense proxy involvement.[20] Since the US withdrawal, the agreement crumbled and Iran felt economic repercussions, experiencing 5.4 percent negative growth in 2018.[21] On the nuclear side of things, Iran quickly reacted. Iran claimed the other signatories were in violation of the agreement by not abiding by their financial commitments to the deal. Iran then exceeded the limit on its low-enriched uranium stockpile and began enriching uranium to higher concentrations in 2019.[22] After the killing of Iranian general Qasem Solemani, Iran's Foreign Ministry spokesman Abbas Mousavi announced that Iran would move away from limiting uranium enrichment.[23] Overall, Iran has accelerated uranium enrichment to bolster the nuclear program that makes them a force to be reckoned with regionally and globally.

The third way Iran tries to become a major power is its support for terrorist groups. The State Department lists Iran as the number one state sponsor of terrorism globally.[24] Hama militants use Iranian weaponry to carry out attacks in the Gaza Strip, and Iran reportedly had ties with the Taliban in Afghanistan. Iranian-backed Hezbollah fighters have also attacked the Lebanese-Israel border and have played a role in propping up the Assad regime in

[19] "Annex to U.S.-Gulf Cooperation Council Camp David Joint Statement," *The White House*, May 14, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/05/14/annex-us-gulf-cooperation-council-camp-david-joint-statement.

[20] Kali Robinson, "What Is the Iran Nuclear Deal?," *Council on Foreign Relations*, June 29, 2021, https://www.cfr.org/backgrounder/what-iran-nuclear-deal.

[21] Saeed Ghasseminejad and Richard Goldberg, "The Impact of Sanctions Two Years After U.S. Withdrawal From the Nuclear Deal," *Foundation for Defense of Democracies*, May 6, 2020, https://www.fdd.org/analysis/2020/05/06/sanctions-impact-two-years-after-jcpoa-withdrawal/.

[22] Robert Einhorn, "Averting a New Iranian Nuclear Crisis," *Brookings Institution*, January 17, 2020, https://www.brookings.edu/policy2020/bigideas/averting-a-new-iranian-nuclear-crisis/.

[23] Laurel Wamsley and Emily Kwong, "Iran Abandons Nuclear Deal Limitations In Wake Of Soleimani Killing," *National Public Radio*, January 5, 2020, https://www.npr.org/2020/01/05/793814276/iran-abandons-nuclear-deal-limitations-in-wake-of-soleimani-killing.

[24] Matthew Lee, "Iran Still Top State Sponsor of Terrorism, U.S. Report Says," *Public Broadcasting Server*, July 19, 2017, https://www.pbs.org/newshour/world/iran-still-top-state-sponsor-terrorism-u-s-report-says.

Syria.[25] Former Deputy Secretary of State Richard Armitage identified Hezbollah as the "A team of terrorism". Hezbollah is considered to be crucial to Iran's destabilizing activities in the Middle East.[26] Iran is estimated to fund Hezbollah $700 million a year.[27]

Subsection Two: Iranian Cyber Strategy

Iran has been very active in the cyber domain. Although they are not a leading nation of cyber capabilities, they are still in an elite group of countries with high strategic and organizational attributes when it comes to the cyber realm. Even an Israeli general said in 2017 that "they are not the state of the art, they are not the strongest superpower in the cyber dimension, but they are getting better and better."[28] Iran has stepped up the sophistication and scope of its cyberattacks to antagonize adversaries and defend forward, the idea that a country should ensure its security offensively. Iranian cyber methods have evolved over the past decade from simple website defacement to more destructive attacks, which include denial of service attacks that deny access to network resources and even the destruction of a computer's hard drive.[29] Iran has displayed a willingness to allocate its resources to building up cyber power. Iran is a perfect example of a country that has high intent of using cyber capabilities and is in the process of accelerating its capabilities to match the cyber power of its adversaries.[30]

Iran's priority is neither deterrence nor defense. In most cases, cyberattacks are used as coercion or retaliation.[31] Iran's focus is not only on Western adversaries like the US but also on regional targets in the Middle East, especially Saudi Arabia. These targets, whether Saudi Arabian, American, or any other target, experience different calibers of attacks. A typical attack is like the Iranian hacking group that hacked LinkedIn users related to energy, financial, and government entities in the Middle East in 2019. Another common, typical example is when an Iranian espionage group targeted Saudi and American government and industry digital infrastructure, also in 2019.[32] Less commonly, there are attacks on multiple states. In 2012, Iran deployed its Shamoon malware against the US and its allies. The malware targeted Saudi and Qatari oil companies. Saudi petroleum company Saudi Aramco had three-quarters of its business computers destroyed, and Saudi petrochemical company Tasnee's hard drives were wiped. The same malware also was used against other Middle Eastern countries like Kuwait and the United Arab Emirates. US and European banks were hacked by the same malware in this time frame.[33]

---

[25] Madyson Hutchinson Posey, "Here Are 4 Ways Iran Is Destabilizing the Middle East."
[26] Matthew Levitt, "Hezbollah Finances: Funding the Party of God," *Washington Institute*, February 13, 2005, https://www.washingtoninstitute.org/policy-analysis/hezbollah-finances-funding-party-god.
[27] Ashley Lane, "Iran's Islamist Proxies in the Middle East," *Wilson Center*, n.d., https://www.wilsoncenter.org/article/irans-islamist-proxies.
[28] James Andrew Lewis, "Iran and Cyber Power," *Center for Strategic and International Studiees*, June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power.
[29] "Iranian Offensive Cyber Attack Capabilities," *Congressional Research Service*, January 13, 2020, https://fas.org/sgp/crs/mideast/IF11406.pdf.
[30] Julia Voo et al., "National Cyber Power Index 2020," *Belfer Center for Science and International Affairs*, September 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.
[31] James Andrew Lewis, "Iran and Cyber Power," *Center for Strategic and International Studies*, June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power.
[32] "Publicly Reported Iranian Cyber Actions in 2019," *Center for Strategic and International Studies*, n.d., https://www.csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019.
[33] Quinten E Hodgson et al., "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace," *RAND Corporation* RR-2961-OSD (n.d.), https://www.rand.org/pubs/research_reports/RR2961.html.

There are three military organizations that contribute to the Iranian cyber campaign. The first is the Iranian Revolutionary Guard Corps (IRGC). The IRGC has specifically launched attacks on American targets, Israeli infrastructure, Saudi Arabia, and other Gulf nations. The second organization is the Basij. The Basij is a paramilitary group that manages roughly 120,000 cyberwar volunteers. The third organization is Iran's Passive Defense Organization. This organization is made up of military and intelligence officials to conduct proper coordination of the Iranian cyber campaign.[34] These three organizations were dispatched in order to strengthen Iran's cyber regime. Although separate, each organization performs a unique function to contribute to the overall Iranian cyber agenda.

Section Three

Subsection One: Iranian and American goals in the cyber conflict

The last decade has seen heightened tensions between the two nations in the invisible cyberspace. Both nations see this area as central to their strategies to counter each other. The virtual battlefield is much more preferred than kinetic military action. As time passes, attacks on one another will become more sophisticated and staggering.[35] To understand how aggressive the nature of the cyber conflict is, there are two reasons why tensions in cyberspace have the potential to spiral out of control: a lack of deterrence and a refusal to follow laws and frameworks.

The first reason that tensions in cyberspace can become aggressive is that deterrence simply does not exist in the realm of cyberspace. Deterrence theory says that no country wants unwanted military aggression because the consequences of war far outweigh the benefits. Deterrence is a pillar of US foreign policy and even Iran's.[36] Deterrence has kept these two nations at bay in regards to nuclear war, but there is an overwhelming amount of analysis to support the fact that deterrence is nonexistent in the realm of cyberspace. Analysis from the National Defense University Press states that "anonymity, global reach, scattered nature, and interconnectedness of the domain reduce the effectiveness of deterrence and can render it useless."[37] This means that the US and Iran theoretically have a forum of open, unrestrained conflict due to the absence of deterrence in cyberspace. Escalation is very common.

The second is that the US and Iran have laid out certain rules for themselves, yet do not abide by them in the first place. Signatories to the North Atlantic Treaty Organization (NATO), predominately the US, have created a doctrine called the "Allied Joint Publication," which sets basic principles of basic conduct for cyber operations. These principles of conduct help identify what type of threat is being posed to NATO, what offensive and defensive cyber operations look like, and what legal considerations are necessary when calculating a response.[38] Iran's Armed Forces released their version of the Allied Joint Publication called the "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to Cyberspace." It declares that if Iran's sover-

[34] James Andrew Lewis, "Iran and Cyber Power," *Center for Strategic and International Studies*, June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power.
[35] Andrew Hanna, "The Invisible U.S.-Iran Cyber War," *United States Institute of Peace*, October 25, 2019, https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.
[36] Michael Mazzar, "Understanding Deterrence," *RAND Corporation*, n.d., https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.
[37] Clorinda Trujilo, "The Limits of Cyberspace Deterrence," *National Defense University Press*, Quarter 2014, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf.
[38] Michael Schmitt, "NOTEWORTHY RELEASES OF INTERNATIONAL CYBER LAW POSITIONS—PART I: NATO," *Lieber Institute*, August 27, 2020, https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/.

eignty is impeded upon (which is decided by Iran), appropriate defensive attacks would be measured in their response.[39] These legal frameworks should have governed the way the US and Iran carry out their cyber agendas. Time and time again, both states have tossed their own rules to the side.

Due to the absence of deterrence and a lack of rule-following, devastating attacks have occurred. For example, in 2018, former President Donald Trump granted more authority to the Central Intelligence Agency to conduct cyberattacks against not only government infrastructure but also civilian infrastructure around the world. Iran's Foreign Minister Seyed Abbas Mousavi claimed to have identified a series of attacks on Iranian infrastructure perpetrated by the United States, and he vowed "legitimate defense and proportional and appropriate response to the aggression."[40] On the other side of the conflict, Iran has been responsible for its own cyber campaign against the United States. The Iranian government hackers APT 33 targeted the US electrical grid, a target of immense importance to the US, with password-spraying attacks.[41] Although unsuccessful, it is just one of many examples of Iranian cyberattacks that have attempted to damage or gain access to American infrastructure.

Subsection Two: Stuxnet

The single biggest and also most infamous case of back and forth conflict between the US and Iran in cyberspace is the case of the Stuxnet worm. Stuxnet is a malicious computer worm that was used by the United States to delay the enrichment of Iranian uranium. The worm was discovered in June 2010, which targeted programmable logic controllers (PLCs) used to automate machine processes.[42] Stuxnet exploited a weak point in the software of Iran's nuclear computers. David Sanger, chief Washington correspondent for the New York Times, reported that the Stuxnet attack on the Natanz facility was conducted by a joint program between the US and Israel with the codename "Olympic Games." The program's goal was to delay the development of Iranian weapons-grade uranium.[43] Now the question arises: was Stuxnet a success? The answer is twofold.

On one side of the argument, the worm did delay the production of uranium. Specifically, Stuxnet infected about 200,000 machines and destroyed roughly 1,000 centrifuges.[44] It was also a success in embarrassing the Iranian regime. Natanz is a hardened fuel enrichment plant built deep underground. The malware was responsible for the firings of Iran's top engineers and scientists, who were unable to explain what was going on at the time. The Iranians were essentially unable to protect their most prestigious facility.[45] The attack reportedly delayed full nuclear enrichment by two years[46], but later reports claim that these figures were exaggerated and only set back the program by a matter of months.

---

[39] Michael Schmitt, "NOTEWORTHY RELEASES OF INTERNATIONAL CYBER LAW POSITIONS—PART II: IRAN," *Lieber Institute*, August 27, 2020, https://lieber.westpoint.edu/iran-international-cyber-law-positions/.

[40] Hanna, "The Invisible U.S.-Iran Cyber War."

[41] "Targeting of U.S. Grid," *Council on Foreign Relations*, January 2020.

[42] Paul Mueller and Babak Yadegari, "The Stuxnet Worm," *The University of Arizona*, n.d., https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic9-final/report.pdf.

[43] "Stuxnet: Tool of Nonproliferation or Pandora's Box," *Columbia University K=1 Project Center for Nuclear Studies*, August 19, 2012, https://k1project.columbia.edu/news/stuxnet.

[44] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," *Institute for Science and International Security*, February 15, 2011, http://large.stanford.edu/courses/2011/ph241/grayson2/docs/stuxnet_update_15Feb2011.pdf.

[45] Max Smeet, "The Strategic Promise of Offensive Cyber Operations," *Air University Strategic Studies Quarterly*, Fall 2018, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf.

[46] Yaakov Katz, "'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years,'" *The Jerusalem Post*, December 15, 2010, https://www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years.

On the other side of the argument, Iran may have gained more from the attack. Although centrifuges were destroyed, the IAEA reported that during the Stuxnet attack window, Iran actually increased their number of operating centrifuges and production of low-enriched uranium.[47] This proves that Iran was inspired to step up their efforts in the face of the attack. Stuxnet merely temporarily slowed down efficiency and did not make any meaningful change in favor of the United States. It could even be considered counterproductive for incentivizing Iran to speed up the development of weapons-grade uranium. In addition to the development of uranium, Stuxnet might have also aided Iran in developing cyber attacks. Reports have revealed that Iran is capable of reverse engineering cyber attacks. Many security researchers believe that Iran learned from the 2010 Stuxnet attack on its systems and can now develop the same technology to then use against the US. A National Security Agency document from 2013 concurs and states that attacks from the West were studied and even replicated by Iran. These replicated attacks were then launched back at the US and Israel.[48]

Conclusion

These developments aforementioned in this paper only yield questions about the future. The foreign policies and cyber strategy of the US and Iran are not inherently violent, but the exchanges these two nations have previously had in the cyber domain prove that peace will never be guaranteed. One of the two nations will always try to "one-up" each other because that is what their foreign policies incentivize. The US needs to maintain its control of the Middle East to counter Iran and Iran wants to be recognized as a major power. These two distinct goals, by their nature, will always clash and cause confrontations like seen in the past. The biggest confrontation was Stuxnet, but attacks of this magnitude may be more common in the future. There are many considerations to be aware of when evaluating what potential escalation could look like.

Although conflicts in the cyber domain are mostly limited to the cyber domain, nations could potentially take the conflict out of the cyber realm. As seen in US and Iranian foreign policy, the chances of this are minimal. However, changing dynamics and different scenarios could be a viable reason for physical retaliation. For example, the Israeli Defence Force accused Hamas hackers of attacking Israel and in retaliation launched an airstrike on a building that had housed the infrastructure for the attack. Indeed, the consequences for a premeditated cyberattack might be even larger. The IPI Global Observatory states, "If the US believed that Iran was imminently about to target critical infrastructure in a cyberattack, this could provide legitimate justification under international law for a pre-emptive physical strike against Iranian targets."[49] This statement is also applicable to Iran. These physical attacks could have destructive results down the road and possibly push these two nations to the brink of kinetic warfare.

Ultimately, this paper demonstrated that cybersecurity is a growing concern for both the US and Iran. It has the possibility of undermining traditional political alignments. Both states have cyber policy goals that are aligned with their foreign policy goals. In the case of Stuxnet, the US tried to damage Iranian nuclear power capabilities, which is a major aspect of the country's wider foreign policy. In the case of Iran, the country has also used cyber capabilities to pressure its adversaries, as seen in the Shamoon malware. Looking forward, cyber security will be a complication for both the US and Iran in their foreign policy goals.

---

[47] John Glaser, "Cyberwar on Iran Won't Work. Here's Why," *CATO Institute*, August 21, 2017.

[48] Glenn Greenwald, "NSA CLAIMS IRAN LEARNED FROM WESTERN CYBERATTACKS," *The Intercept*, February 10, 2015, https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/.

[49] Vasileios Karagiannopoulos, "How Real Is the Threat of Cyberwar Between Iran and the US?," *IPI Global Observatory*, January 23, 2020, https://theglobalobservatory.org/2020/01/how-real-is-threat-of-cyberwar-between-iran-and-us/.

Acknowledgments

I would like to thank my advisor for the valuable insight on this project.

References

Jacquelyn Schneider, "A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem," The Washington Quarterly 43 (2020), https://www.tandfonline.com/doi/abs/10.1080/0163660X.2020.1770970?journalCode=rwaq20&.
Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Security & Privacy 9, no. 3 (2011), https://ieeexplore.ieee.org/abstract/document/5772960.
Hal Brands, "Why America Can't Quit The Middle East," no. 1921 (March 21, 2019), https://www.hoover.org/research/why-america-cant-quit-middle-east.
"OPEC Share of Crude Oil Reserves, 2018," n.d., https://www.opec.org/opec_web/en/data_graphs/330.htm.
Seymour Hersh, "U.S. Secretly Gave Aid to Iraq Early in Its War Against Iran," New York Times, January 26, 1992, https://www.nytimes.com/1992/01/26/world/us-secretly-gave-aid-to-iraq-early-in-its-war-against-iran.html?pagewanted=1.
Janae Diaz and James Di Pane, "Iran Is Targeting the Strait of Hormuz. The World Needs to Take Heed.," The Heritage Foundation, October 22, 2020, https://www.heritage.org/middle-east/commentary/iran-targeting-the-strait-hormuz-the-world-needs-take-heed.
Stephen Zunes, "Why the U.S. Supports Israel," Institute for Policy Studies, May 1, 2002, https://ips-dc.org/why_the_us_supports_israel/.
Krysta Wise, "Islamic Revolution of 1979: The Downfall of American-Iranian Relations," Legacy 11, no. 1 (n.d.), https://opensiuc.lib.siu.edu/legacy/vol11/iss1/2/?utm_source=opensiuc.lib.siu.edu%2Flegacy%2Fvol11%2Fiss1%2F2&utm_medium=PDF&utm_campaign=PDFCoverPages.
"State Sponsors of Terrorism," U.S. Department of State, n.d., https://www.state.gov/state-sponsors-of-terrorism/.
"Foreign Terrorist Organizations," U.S. Department of State, n.d., https://www.state.gov/foreign-terrorist-organizations/.
François Carrel-Billiard and Christine Wing, "Iran and the NPT," n.d., https://www.ipinst.org/wp-content/uploads/2010/04/pdfs_iranchapt.pdf.
"Department of Defense Cyber Strategy 2018," Department of Defense, n.d., https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
Samantha Ravich and Ed Cardon, "Defending Forward in the Cyber Domain," Foundation for Defense of Democracies, n.d., https://www.fdd.org/analysis/2020/12/15/defending-forward-defending-forward-in-the-cyber-domain/.
Itamar Rabinovich, "How Iran's Regional Ambitions Have Developed since 1979," Brookings Institution, January 24, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/01/24/how-irans-regional-ambitions-have-developed-since-1979/.
Madyson Hutchinson Posey, "Here Are 4 Ways Iran Is Destabilizing the Middle East," The Heritage Foundation, October 16, 2017, https://www.heritage.org/middle-east/commentary/here-are-4-ways-iran-destabilizing-the-middle-east.
Claire Brenner, "Iran's Destabilizing Activities in the Middle East," American Security Project, March 5, 2021, https://www.americansecurityproject.org/irans-destabilizing-activities-in-the-middle-east/.
"Iran's Foreign and Defense Policies," Congressional Research Service R44017 (January 11, 2021), https://fas.org/sgp/crs/mideast/R44017.pdf.
"Iran's Networks of Influence - Chapter Four: Iraq," International Institute for Strategic Studies, November 2019.

"Annex to U.S.-Gulf Cooperation Council Camp David Joint Statement," The White House, May 14, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/05/14/annex-us-gulf-cooperation-council-camp-david-joint-statement.
Kali Robinson, "What Is the Iran Nuclear Deal?," Council on Foreign Relations, June 29, 2021, https://www.cfr.org/backgrounder/what-iran-nuclear-deal.
Saeed Ghasseminejad and Richard Goldberg, "The Impact of Sanctions Two Years After U.S. Withdrawal From the Nuclear Deal," Foundation for Defense of Democracies, May 6, 2020, https://www.fdd.org/analysis/2020/05/06/sanctions-impact-two-years-after-jcpoa-withdrawal/.
Robert Einhorn, "Averting a New Iranian Nuclear Crisis," Brookings Institution, January 17, 2020, https://www.brookings.edu/policy2020/bigideas/averting-a-new-iranian-nuclear-crisis/.
Laurel Wamsley and Emily Kwong, "Iran Abandons Nuclear Deal Limitations In Wake Of Soleimani Killing," National Public Radio, January 5, 2020, https://www.npr.org/2020/01/05/793814276/iran-abandons-nuclear-deal-limitations-in-wake-of-soleimani-killing.
Matthew Lee, "Iran Still Top State Sponsor of Terrorism, U.S. Report Says," Public Broadcasting Server, July 19, 2017, https://www.pbs.org/newshour/world/iran-still-top-state-sponsor-terrorism-u-s-report-says.
Madyson Hutchinson Posey, "Here Are 4 Ways Iran Is Destabilizing the Middle East."
Matthew Levitt, "Hezbollah Finances: Funding the Party of God," Washington Institute, February 13, 2005, https://www.washingtoninstitute.org/policy-analysis/hezbollah-finances-funding-party-god.
Ashley Lane, "Iran's Islamist Proxies in the Middle East," Wilson Center, n.d., https://www.wilsoncenter.org/article/irans-islamist-proxies.
James Andrew Lewis, "Iran and Cyber Power," Center for Strategic and International Studies, June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power.
"Iranian Offensive Cyber Attack Capabilities," Congressional Research Service, January 13, 2020, https://fas.org/sgp/crs/mideast/IF11406.pdf.
Julia Voo et al., "National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.
James Andrew Lewis, "Iran and Cyber Power," Center for Strategic and International Studies, June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power.
"Publicly Reported Iranian Cyber Actions in 2019," Center for Strategic and International Studies, n.d., https://www.csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019.
Quinten E Hodgson et al., "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace," RAND Corporation RR-2961-OSD (n.d.), https://www.rand.org/pubs/research_reports/RR2961.html.
James Andrew Lewis, "Iran and Cyber Power," Center for Strategic and International Studies, June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power.
Andrew Hanna, "The Invisible U.S.-Iran Cyber War," United States Institute of Peace, October 25, 2019, https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.
Michael Mazzar, "Understanding Deterrence," RAND Corporation, n.d., https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.
Clorinda Trujilo, "The Limits of Cyberspace Deterrence," National Defense University Press, Quarter 2014, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf.
Michael Schmitt, "NOTEWORTHY RELEASES OF INTERNATIONAL CYBER LAW POSITIONS—PART I: NATO," Lieber Institute, August 27, 2020, https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/.
Michael Schmitt, "NOTEWORTHY RELEASES OF INTERNATIONAL CYBER LAW POSITIONS—PART II: IRAN," Lieber Institute, August 27, 2020, https://lieber.westpoint.edu/iran-international-cyber-law-positions/.
Hanna, "The Invisible U.S.-Iran Cyber War."
"Targeting of U.S. Grid," Council on Foreign Relations, January 2020.

Paul Mueller and Babak Yadegari, "The Stuxnet Worm," The University of Arizona, n.d., https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic9-final/report.pdf.
"Stuxnet: Tool of Nonproliferation or Pandora's Box," Columbia University K=1 Project Center for Nuclear Studies, August 19, 2012, https://k1project.columbia.edu/news/stuxnet.
David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," Institute for Science and International Security, February 15, 2011, http://large.stanford.edu/courses/2011/ph241/grayson2/docs/stuxnet_update_15Feb2011.pdf.
Max Smeet, "The Strategic Promise of Offensive Cyber Operations," Air University Strategic Studies Quarterly, Fall 2018, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf.
Yaakov Katz, "'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years,'" The Jerusalem Post, December 15, 2010, https://www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years.
John Glaser, "Cyberwar on Iran Won't Work. Here's Why," CATO Institute, August 21, 2017.
Glenn Greenwald, "NSA CLAIMS IRAN LEARNED FROM WESTERN CYBERATTACKS," The Intercept, February 10, 2015, https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/.
Vasileios Karagiannopoulos, "How Real Is the Threat of Cyberwar Between Iran and the US?," IPI Global Observatory, January 23, 2020, https://theglobalobservatory.org/2020/01/how-real-is-threat-of-cyberwar-between-iran-and-us/.