What are the motivations behind Israel’s cyber war with Iran, and the implications it has today?

Hunter Bishop

Old Dominion University

IDS300W

Dr. Kathryn LaFever

December 3, 2022

Israel and Iran – two countries with a large sphere of influence locally in the Middle East as well as globally. Historically, there has been a level of tension between the two countries which has been somewhat enigmatic to historians since both Syria and Iraq lie between the squabbling nations, so the disputes are not border disputes or local economic troubles. A present-day war fought over the medium of cyberspace, based on a tumultuous history between two nations, can have potentially far-reaching consequences that can affect more than just the Middle East. So, this begs the question: What led to the Iranian-Israeli cyber war of the present, and what are the implications today and into the future for the rest of the world? The lenses of history, geopolitics, and cybersecurity are three disciplines that are very helpful in dissecting the conflict between Israel and Iran. By using multiple fields of study, the research done can take information from many different angles to explain why this conflict has arisen and what course it might set for the future. Through the lens of history, motivations and previous tensions can reveal more about why Israel and Iran are at odds with one another today; by extension, geopolitics can also help reveal motivations for the conflict itself, but also leads to more knowledge about not only what has happened, but what is likely to happen based on previous conflicts of a similar nature. And finally, cybersecurity can help to identify the present-day applications to the historical and geopolitical findings, as the Israeli-Iranian conflict is one of the first international battles that is being fought through cyberattacks. Research on this topic can help historians, politicians, and experts in the field of cybersecurity and information technology to have a baseline of what a true cyber war might look like, and the research can also be used to aid in the de-escalation of the conflict.

Cyberspace, publicize/publicity, and escalation/de-escalation are key terms that are present in this paper. *Cyberspace*, as defined by the NIST Computer Security Resource Center

(CRSC for short), is “the interdependent network of information technology infrastructure, and includes the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries” (CRSC, n.d.). In simple terms, any device that can be used to connect to another device somewhere far away can be considered part of cyberspace. *Publicize* means to make something widely known, with *widely* being the key part of that definition. A rumor spread around a high school does not count as being publicized; in this case, *publicize* is referring to major news outlets or social media being the vector of information spreading. And lastly, *escalation*, is “the increase in the intensity of a conflict and in the severity of the tactics used to pursue it” (Maiese, 2016). Escalation can happen on either side of a conflict, or even from parties that were not originally included in the conflict. Being the opposite, *de-escalation* refers to the process by which the intensity of a conflict and severity of tactics decreases.

In recent history, Iran and Israel have gone from a strained alliance to bitter enemies at each end of a cyber war, which neither country’s government desires to take the blame for. One prevailing issue of why hostilities grew between the two countries in the late 1990s and early 2000s was the rise of Islamic influence in Iran and their subsequent condemnation of Israel as an enemy to Islam (Menashri, 2004). With Jewish and Muslim people opposing one another’s ideologies, the tensions have only risen in the past two decades and come to a point where the Iranian and Israeli governments launch cyber-attacks against the other country on an almost weekly basis. Being at the center of Asian, European and African continental crossroads, this unrest has the potential to make waves that reach beyond the Middle East and into the aforementioned continents. Political unrest, economic hardship and a looming threat of multinational war are just a few possible outcomes of continued escalations between Israel and

Iran. With religion being a primary motivation for the hatred of these countries towards one another (Iran towards Israel more fiercely), the stage is set for other groups of shared beliefs to join in the fight. Should other Muslim nations decide to align themselves with Iran, it could quickly turn sour for Israel and by proxy the United States and several European nations whose hands would be forced to back Israel.

A main reason for Israel's uptick in cyber activity was their realization that they could use it as a means of war and defense as well as a way to gain intelligence. This began in the early 2000s, a time when Iran only focused on cyber activity as an intelligence-gathering strategy (MEPC, n.d.). As stated previously, Iranian cyber groups were reluctant to launch any sort of large-scale attacks against Israeli groups or government agencies because of the United States backing of Israel as a nation. This was the status quo until the Stuxnet attacks which are presently believed to be a joint effort between the United States and Israeli governments to try to cripple or disable Iran's nuclear program (Fruhlinger, 2022). Stuxnet was a worm, which is a self-replicating and rapid-spreading computer virus, that was created to target the Uranium enrichment centrifuges in the Iranian nuclear facilities, specifically in the Natanz facility. Without any external interference, the centrifuges were already delicate and apt to malfunction, or even break completely, due to the volatility of centrifuging out the lighter isotope uranium-235, which can be used in nuclear fission to make nuclear weapons, from the naturally occurring isotope of uranium-238 (Fruhlinger, 2022). This made an easier job for Stuxnet to destabilize the centrifuges, which allowed the worm to infiltrate the Natanz facility and derail the nuclear weapons program. Being so complex and without a predecessor, Stuxnet was likely being developed for many years throughout the mid and late 2000s up until it was launched in 2010, which meant that Israel had a large head start over Iran in their cyber warfare programs, especially in experience with coding and developing new tools to use. But the implications from Stuxnet went beyond just dismembering Iran's nuclear program and causing a large setback. Stuxnet is considered by many to be the first true cyber weapon, meaning that there was no precedent for how to implement it or how to handle its fallout, should there be any, and there certainly was. Stuxnet was not discovered by the Iranian Natanz facility crew members, but rather was only discovered when the worm left the facility which it initially targeted. Since the Natanz facility was not connected to the Internet, it is likely that poor security practices on the part of Iranian employees are to blame (Fruhlinger, 2022). The silver lining is that although Stuxnet is still present, it is not so much of a threat as it used to be since the zero-day vulnerabilities that were around when it was released were also patched many years ago. At the time, Iran did not know any of this though, and the vulnerabilities were still there, and the Stuxnet attack was likely the ultimate catalyst that caused Iran to ramp up their own programs for cyber warfare and cyber defense. As with any increase in a stance of power, this could affect more than just the surrounding countries of Iran. With cyberspace being a globally reaching network, a country of any size is able to cause a large amount of damage.

With more than two decades of increasing tensions between Iran and Israel, it is seemingly inevitable that things would come to a head eventually. Some might consider Stuxnet to have been that moment, but that was more of a one-sided "war." Israel had a large head start even when Stuxnet was first launched, while Iran was only using their cyber resources to gather intelligence and information for themselves, rather than creating tools of war. A decade on from Stuxnet, and the Israel-Iran cyber war has begun to gain more traction and be exposed to the public eye even more. Publicizing cyberattacks has different benefits and drawbacks that Israel and Iran have to consider when playing on the chessboard of cyber war. In April of 2020, one of the premier examples of using the public eye as a tool was first showcased. Israel told news outlets that there was a cyberattack that targeted the Israeli water and sewage systems but did not provide any information on who the perpetrating group or nation was. In doing so they were able to put themselves out in front of the situation and take control of the scene. The underlying assumption is that Iran is believed to be the malicious actor in this case, because of the historical context we have of the decades-long conflict of trading cyber blows. But by not pointing fingers, Israel is able to remove themselves from an accusatory position and in the same way, Iran is able to avoid escalation by choosing not to comment or take credit (Baram, 2022). Attacks like Stuxnet, which had no precedent, are serving to set new precedents. The United Nations has in place different laws that regulate international conduct, and most countries have agreed that the laws that apply to traditional interactions between nations should also apply to cyberspace interactions. This still leaves the laws open to interpretation on how to implement them in regards to cyberactivity and how to fairly take punitive actions when necessary (Baram, 2022).

There are three major findings disclosed by this interdisciplinary research. With so many different nations and groups involved either directly or by proxy, it is difficult to say that the Iranian-Israeli conflict is truly a conflict between only Israel and Iran. The first major finding is that the door is open for nations other than the United States to involve themselves in this conflict and gain from it on a geopolitical scale. Israeli and Iranian governments were reluctant to take credit (or blame, depending on perspective), until recent years where the two countries have decided to take their conflicts into the public eye. This has opened up the need for a more strategic approach by both Israel and Iran to ensure they do not escalate the conflict onto a global stage and attract unwanted attention to their opponents. Despite those efforts, Azerbaijan has become a staunch ally of Israel since the Russian invasion of Ukraine and has been dubbed as an information supplier to Jerusalem on the dealings and activities of Iran (Khanin, 2022). Present goings-on turn into potential implications for the future, and with the United States as a proxy ally and Azerbaijan as a local ally, this could be something that pushes Iran to search out allies for themselves and bolster their own information centers. A conflict such as the Israeli-Iranian cyber war is liable to have consequences that reach further than the neighborhood of the Middle East and could include more countries than many political scientists presume. The second finding is that cyberspace is a volatile environment, and many are still unaware of what potential problems cyber warfare could cause. A country the size of the United States is able to hold its own on the stage of global war with its sheer military might, but a country like Israel must rely on tact and other ways of striking at its enemies. Other small countries might see Israel as an inspiration to walk through the open door and lift themselves up on that geopolitical scale through the use of cyberspace as a tool or even a weapon. The third finding is that the old adage, "history is doomed to repeat itself" could once again prove to be true. Iran and Israel sit at two opposite ends of the spectrums of politics and religion, two factors which have contributed to countless wars throughout world history, one of the most notable being the Crusades. Christians fought Muslims for ownership of the Holy Land because each felt threatened by the other. The difference between now and then is that Iran and Israel do not meet on a battlefield with swords and spears, but rather they target water systems and hospitals from within their own borders in an attempt to outlast the other. These findings might possibly have not been found without the use of interdisciplinary research. In the eye of traditional war, smaller countries would be overlooked, but now with the advent of cyberwar, any nation is capable of causing damage to another. And without looking at the historical outcomes of similar conflicts, modern-day politicians would be without crucial information in how to best prepare their own countries and people.

While these three disciplines worked well to provide thorough insight into the Israeli-Iranian conflict, there are areas where they are not as cohesive in an interdisciplinary fashion. One such example is the unpredictability of cyberspace in the field of cybersecurity is at odds with the factual nature of history. History is a certain thing because it has already happened, but when looking through the lens of cybersecurity, it is difficult to have certainty because there is still so much left to discover about cyberspace and how it might be used. Another such discrepancy is again with the unpredictable nature of the field of cybersecurity and how that relates to geopolitics. Politicians like to have a sense of control but, due to the vastness of cyberspace and the sheer amount of data in transit at any given moment, there is no sense of control over greater cyberspace. The President cannot put troops at the border of cyber-Iran to protect its allies. Cybersecurity requires professionals who are quick learners and who are able to adapt to the rapidly changing landscape of the interconnected world. Though these seemingly conflicting views exist, time will serve to bridge these gaps. As people as a collective continue to learn about cyberspace more and more, it will begin to intertwine itself into history and the geopolitical scope. Decisions for the future will have to be made with cybersecurity in mind, because of how rapidly it is expanding. Therefore, though the field of cybersecurity is rather new compared to history and geopolitics, it is still a very viable lens through which to examine issues in today's society.

This research, while extensive and well thought-out, could always be improved. In order to create a more comprehensive understanding of the Israeli-Iranian conflict, a deeper look into the histories of the two countries and their relations with one another would be a good starting point. While most of their tensions have existed in recent history since the 90s, there were other times in the last century that the two countries have been at odds that were not directly relevant to this research but could certainly serve to improve the overall understanding. In reflection of the understanding of this conflict, there are many other disciplines that could be included in further interdisciplinary research of the Israeli-Iranian conflict. One such one that was considered was strategic warfare. While the conflict might not be a traditional war, it has opened up a new domain on which wars are fought. Cyberspace allows for many different attack vectors and opens up the possibility of more strategic warfare, which is a discipline all on its own. The lens of strategic warfare could be useful in studying the current actions between Iran and Israel and could also help to predict how wars will be fought in the near future.

The Israeli-Iranian conflict has been building to a boiling point for the past three decades. In 2010 with the launch of Stuxnet against the Iranian nuclear program, Iran began to fortify their own cyber warfare capabilities. The historical tensions between the two countries combined with the newfound cyberattack skills have led to a conflict which has the potential to escalate to a global scale. The United States and Azerbaijan have already aligned themselves with Israel in this century, which leaves the door open for Iran to try to find their own allies. The Middle East stands on the brink of war at any moment. Other countries could be tempted to join their powers to either Iran or Israel in order to boost themselves politically. And now with cyber warfare being an option, smaller nations are able to cause real damage that they could not have done with a traditional army. Russia and the United States might have the military might, but a small country like Lebanon or Kuwait with populations that are less than the state of Virginia have the ability to make a name for themselves. And if history is truly doomed to repeat itself, Iran and Israel are far off from de-escalation and making peace. Politicians, historians and other relevant professionals need to look carefully before they leap and cause a cascade of events that results in a global conflict.

References

Baram, G. (2022, July 25). *How the cyberwar between Iran and Israel has intensified*. Washington Post; The Washington Post. https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/

CSRC. (n.d.). *cyberspace - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/cyberspace

Fruhlinger, J. (2022, August 31). *Stuxnet explained: The first known cyberweapon*. CSO Online. https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html

Khanin, V. (2022, November 3). *Russia's War in Ukraine Shifts Dynamics in the Israel-Iran-Azerbaijan Triangle | Wilson Center*. Www.wilsoncenter.org. https://www.wilsoncenter.org/blog-post/russias-war-ukraine-shifts-dynamics-israel-iran-azerbaijan-triangle

Maiese, M. (2016, July 5). *Destructive Escalation*. Beyond Intractability. https://www.beyondintractability.org/essay/escalation

Menashri, D. (2004, February 4). *Iran and Israel: A Couple at Odds | Wilson Center*. Www.wilsoncenter.org. https://www.wilsoncenter.org/event/iran-and-israel-couple-odds

MEPC. (n.d.). *Cyber Capabilities: Israel vs. Iran | Middle East Policy Council*. Mepc.org. https://mepc.org/commentary/cyber-capabilities-israel-vs-iran