SOCIAL SCIENCE REVIEW ARCHIVES
ISSN Online: 3006-4708
ISSN Print: 3006-4694
https://policyjournalofms.com

Iran and Israel Cyber Warfare and Interference of US

Muhammad Umar[1]

[1] Department of Political Science, University: University of Management and Technology, Lahore, Email: u5731584@gmail.com

DOI: https://doi.org/10.70670/sra.v3i2.824

Abstract:

The Israeli-Iranian struggle has also gone to the cyber battle space of cyber warfare. This matches the reality of evolving global power competition, in which states increasingly use cyberspace to achieve strategic ends, with the relative anonymity and reduced physical risk involved. At the heart of this cyberwar is a history of power struggle rooted in geopolitical competition, religious ideologue, and national security imperatives. Israel and Iran have engaged in a relentless back-and-forth of cyberattacks and counterattacks that have targeted critical infrastructure, security apparatuses and government services, proving both countries consider cyber the dominant theatre in their competition for dominance. One of the most serious cyberattacks was the deployment of the Stuxnet virus in 2010, made with the high technical cooperation between the United States and Israel. Stuxnet was built to sabotage Iran's uranium enrichment centrifuges at the Natanz plant by causing them to physically degrade. It was, at the time, the first publicly known cyberattack to inflict physical damage in the physical world, a perilous practice of precedent for digital-age international relations. It showed not only the power of state-directed cyber war, but also how deeply America had invested in Israel's cyber campaigns against Iran. Iran has drastically improved its cyber warfare program since then, and has targeted Israeli infrastructure, including an attempt to poison water sources, paralyze the public transit system and hack government websites. Israel has responded with its own cyberattacks, like one that temporarily shut down Iran's Shahid Rajaee port operations, as well as others that targeted fuel distribution networks and surveillance systems. These countermeasures have created a resilient and a volatile digital battlefield span the Middle East. The US has a complex and important role to play in this cyber war. The claim based on Israelis' use of American cyber offensive technology is, however, entirely unfounded, as the US is Israel's closest ally and co-developer of offensive cyber capabilities, who enables and aids Israeli efforts to curb Iran's technological and nuclear ambition. American intelligence agencies and military cyberunits cooperate closely with their Israeli counterparts, sharing information, offering technological know-how and providing operational support, when needed. At the same time, the U.S. is also locked in confrontations with Iran, manifested in Iranian-backed cyberattacks against U.S. banks, oil companies and government agencies. These copycats of cyber tensions have also more deeply drawn the U.S. into the Israel-Iran cyber battle. In spite of the extensive use of cyber tools, there is still no established international law framework to govern cyber war, prompting concerns about responsibility, proportionality and escalation. Enter the Israel-Iran war and we can see how fraught with problems it is to use cyber means for political reasons—especially when the infrastructure to be hit is civilian. Moreover, the cyber warfare raises (or seems to) bigger questions about global inequities in technology; about the role of secrecy and surveillance in the age of cyberpower; and about the defense-offense continuum within the cyber domain. In short, the Israel-Iran cyber war, helped along by an actively involved U.S., constitutes a new world of global conflict, in some ways mirroring the new necessities of civilian life, in which the digital is the foremost player in national security and geopolitics. It emphasizes the imperative for global norms and ethical limits in the fast-changing sphere of cyber war.

Key Words: Cyber Space, Israel-Iran Competition, Stuxnet, Cyber Attacks, Critical Infrastructure

Introduction:

The 21st century has been marked by the fact that war is no longer waged on the traditional massive fields, but it is fought in the virtual realm and one of the aspects that determine the relations among the countries and the safety of the nations is the cyber warfare. The cyber war between Israel and Iran is one of the most well-known cases of cyber war as the two countries are engaged in the on-going cyber war that includes spying, sabotage, and information manipulation. The blogging on this cyber war is not only the reflection of some basic geopolitical enmities, ideological conflict and strategic contest but has turned out to be a war of low-intensity and long-durability in cyber space. This cyber competition is even more complex and global in its consequences given the fact that most of these collisions are between the largest superpowers in the world and dominating its interests and actions to be sufficient in themselves to govern the course of the contest. The origins of cyber war between Iran and Israel can be traced back to the nuclear program of the Iran and the determination of Israel to refrain Tehran form turning into a nuclear state. The defining moment in this cyber war was when a very high advanced worm was launched in the year 2010 in the Iranian Natanz nuclear centre at Natanz and successful in paralyzing nuclear facility. This attack, which has been portrayed to have occurred as a result of a joint American-Israeli operation, was the initial-known use of a digital weapon with the ability to create real-world destruction, allowing precedent to be formed in the digital sabotage in international war. Since then, Israel and Iran have upped their hacking rhetoric, with Israel attacking Iranian infrastructure, financial and propaganda systems, and Iran hacking Israeli water supplies, transportation hubs and civilian targets. The United States is two-fold in this war of cyber warfare. On its part, it is an ally, a strategic partner of Israel through the provision of intelligence, technology and political support. On the other hand, the U.S. is one more global participant who is concerned about the maintenance of international cybersecurity standards, preventing cyber escalation, and ensuring its relations with Iran. especially since withdrawing its signature in the Iran nuclear plan in 2018. Iran is increasingly viewed by American cyber policy as the main enemy and the policy is also trying to balance its needs to defuse tensions and avoid war in the Middle East. It is an introduction to the investigation of the facets of the Israel-Iran cyber war, lawful and ethical impacts that it initiates, and the strategic position of the United States. The cyber space is not only an arena of opportunity, but also the one of danger: states are afforded the ability to pursue covert operations that are associable with impunity, but once miscalculations are made and escalation take place, the manner of cyber space can provide only so much damage limitation. In analysing this cyber competition, one should explore the way state practices in cyberspace are determined by geopolitics, security interests and new conceptions of norms of warfare in cyberspace. It also requires a reflection on the consequences of international stability and the international order of the digital world. Now, the Israeli-Iranian cyber battle does not only exist as a regional conflict, it is yet a case study of technology, power as well as politics in an age with internet. It indicates to the growing national security importance of cyber capabilities and the necessity of useful cyber governance systems. United States, having been both actor and judge, stands at the centre of the spinning wheel of unfolding cyber conflict, upon which it determines the direction and the consequences. The war in cyberspace between Iran and Israel, which involves the US as one of the participants, is gaining more and more attention in the scholarly community due to its complexity and significance to cybersecurity and international law, as well as stability in the region. The cyber capabilities of the two states, the strategic rationale of their behavior, and the broader outcomes to international relations and norms of digital warfare have been discussed by scholars.

Literature Review:

Stuxnet has been called a turning point in cyber warfare in most of the literature. Other researchers such as Lindsay (2013) and Sanger (2012) point out the novelty of Stuxnet as a state-sponsored cyber war, likely staged by Israel and the US collaborative effort, which had the aim to destroy in real life the nuclear enrichment complex of Iran. Stuxnet opened up a bottomless cyber war between the two neighbours. It left a precedent to the use of malware as a tool of covert statecraft as well and thus, this raises the question of legitimacy and morality of offensive cyber activities. The topic of Iranian cyber counterstrike with further development of offensive capabilities was brilliantly researched by such scholars as Thomas Rid and Collier (2020). Rid and Collier argue that Iran has been transformed into an offensive actor, empowered by cyber skills, launched an offensive against Israeli civilian infrastructure, financial institutions and critical facilities. Such operations have further eroded the distinctions between war and peace, between state and non-state actors as well as between infrastructure and infrastructures applied by the military and civilians. The contribution of United States in this cyber war is direct and indirect. Other researchers like Nye (2010) and Healey (2011) write about the U.S. cyber policy, its efforts to prevent the enemy and maintain freedom of action in the cyberspace. The United States is considered to be an excellent partner of Israeli cyber forces not only technologically or in the aspects of intelligence but also geopolitically. However, the literature also argues that the U.S has been destabilizing rules of cyberspace by launching pre-emptive strikes like Stuxnet that is likely to have influenced other states like Iran to develop retaliatory weapons. In theory, some realist authors, such as Dunn Cavelty (2012) view cyber conflict as an expansion of classical power politics. They argue that the cyber technologies have offered asymmetric capability to states, and thus weaker states like Iran can face more powerful states like Israel and United States without provoking a significant war. Instead, constructivist writers emphasise principles and international statute as the impetus behind online behaviour. They underline a lack of strict regulations and the inability to establish the authorship, which is a challenge to responsibilities in the cyber world. Humanitarian impact of cyber war is another aspect that has began to be discussed in recent writing. As an example, Deibert (2019) and the Citizen Lab address the possibility of cyberattacking the infrastructure of civilian populations arguing that pursuing such initiatives undermines the international humanitarian law. These researches create a dire need to hold international discussions of the legal and ethical framework of cyber operations. Conclusively, there exists more and more discussion of the Israel-Iran cyber war and U.S nexus, the discussion can be categorised as how the issue is detrimental with regard to security, legal, ethical and strategic aspects. Nevertheless, when it comes to long-term consequences with regards to international norms, civilian security and regional diplomacy, the lacunas exist. The question of what the balance of power and the prospects of peace are in the Middle East under the influence of cyber war needs the analysis.

Research Question:

This paper endeavours to peep the dynamic and diverse aspect of Israel- Iran cyber warfare, particularly in the international relations and the strategic positioning of the United States. The study tries to investigate how cyber activities are used as instruments of national strength, impediment and stealth in the extremely volatile geopolitical landscape. This investigation is guided by the below study questions:

1. Why is there a strategic and historical motivation of cyber confrontations between Israel and Iran?

This question tries to locate the sources of the cyber animosities like the political tensions, the nuclear rivals, the ideological rivalries, and the rivalry of power on the regions.

2. What have been the latest cyber war tactics between Israel and Iran since the Stuxnet attack and which have been the most significant cyber operation carried out by both nations?

The question will follow the time line of the major cyber attacks based on the tools, target and the effect that the cyber operations were supposed to have.

3. What has United States done to either facilitate, promote or instigate the cyber war between Iran and Israel?

In this instance, research will be conducted on U.S strategy, intensive coordination of intelligence and technological assistance and its role on international cyber standards.

4. What do realist theory explain about the moves of Israel, Iran and the USA, as far as cyber war is concerned?

The objective of this question is to apply the concept of international relations to analyse how power dynamics, national interest and the concept of strategic deterrence influence cyber behaviour in this triangle of conflict.

5. What does the Israel-Iran cyber war mean to the international law, the protection of civilians, and global cyber governance of the security issue?

The latter question addresses the moral and legal areas, including the probability of escalation, civilian casualties, and impunity in the cyberspace.

Taken together, such research questions will form the backbone of a powerful study of the dynamics and consequences of such new type of war.

Theoretical Framework:

Structure -- stands to mean political and ideological organisation where religious instruction governs the laws of the state, policies and foreign activities. In the Islamic Republic of Iran, this type of structure has become paradigmatic with regard to internal governance as well as the foreign policy. The government of Iran, whose constitution give the Supreme Leader (currently Ayatollah Ali Khamenei) powers, is supported by the doctrine of Velayat-e Faqih (Guardianship of the Jurist) which states that Islamic clerics should be given the last word in political power. This political system of religion has a strong hold on how Iran addresses the world even in the area of cyber war. Thus, the theocratic ideology locates the struggle of Iran with Israel not simply as the geopolitical struggle but the religious and moral conflict. In this story, Israel is an usurper regime taking control of Muslim land and threatens Islam cohesiveness and its fairness. Iranian government is the preserver of suppressed Muslims especially the Palestinians and opposition to Israel is mandatory according to religions. Such a view renders direct and proxy activities such as cyber attacks acceptable in the bigger picture of Iran defending Islam. The cyber war has become an extension to this battle ordained by God. The Iranian cyber actions against the Israeli infrastructures and intelligence machineries, and even against civilians, are aimed not only at strategic but also at religious resistance. These actions are regularly performed by the organisations or, in fact, inspired by the Islamic Revolutionary Guard Corps (IRGC) which identifies itself with being a historical army of religion that defends the Islamic Revolution. The secular Israeli and western organisations which are attacked by cyber hacking organisations are attacked as correct according to divine justice. The theocratic description of the world influences the Iranian perception of technological development, as well. Most theocratic regimes have opposed modernity but the leadership of Iran has embraced the use of modern means like cyber technologies as far as they promote causes of Islam. Ayatollah Khamenei has overtly assisted the growth of science and technology as long as it can be of assistance the system of Islam. Such selective adaptation helps the regime to gain the power in cyberspace but preserve ideological purity at the same time.

The international circle states that the theocratic structure of Iran is often in conflict with worldly secular norms of conduct in the cyber-space world. An example would be that since during cyber attacks against civilian infrastructure, it would be established by the Western governments as a violation of the international law whereas the Iranian officials may think of these operations as a legitimate response to aggression, sanctions or even the oppression of the Muslims. This presents more of a challenge to diplomatic work and cyber diplomacy. Moreover, not all the cyber activities in Iran are controlled or led by the state; in most cases these activities are controlled by religiously inspired hackers or cyber brigades acting at the behest of the theocratic aspirations of the regime. These are loosely-structured forces, whose ideological orientation increases the randomness and deniability of the Iranian cyber program. Finally, the theocratic system is also a source of the internal discourse of Iran. And government follows the political strategy to censor dissent, use cyber measures to track its citizens and ensure online control to enforce ideological pathways. Form of cyber repression becomes justified as the measure of protection of the Islamic moral order and prevention of the Western cultural influence. The paper adopts the qualitative nature of the research to explore the evolving patterns of cyber war between Israel and Iran, and strategic involvement of the United States. The focus is put on understanding the political, ideological, and strategic dimensions of cyber war and not on the enumeration of the technical facts of attack or on the summation of raw cyber facts. The qualitative approach is chosen as it lets inquire more about motivations, interpretations and meanings of cyber activities and responses by state actors.

First entity:

Israel is usually reputed to be one of most developed cyber countries in the world. Israel has futuristic defence and intelligence collection into the cyberspace enforced by introducing high-level cyber teams including Unit 8200. Israel is a mature technocratic country and a start up nation, and cyber has become part of its national security system. It sees Iran as its critical adversary due to Tehran nuclear ambitions, missile R&D programs and support of Militant Groups like Hezbollah and Hamas.

Cyberwar will enable Israel to assault the Iranian infrastructure without being detected leading to an absence of military escalation. Among its milestones of Israeli cyber competencies lies the Stuxnet virus, which allegedly was an Israeli-American intelligence community joint venture, and which shut down the Iranian Natanz nuclear facility in 2010. Israel has now performed numerous digital attacks on Iranian military gear, nuclear researchers, and even civil facilities including water installations and ports. These are the indications of proactive defence and anticipatory containment practiced by Israel.

Cyber policy of Israel is strongly dominated by the precepts of Realism-national survival, strategic deterrence and technology superiority. In the case of cyber operations, Israel disables a danger before it manifests itself kinetically and, simultaneously, still maintains plausible deniability.

Second party: Iran,

Iran is another player in the cyber world to counter both Israeli, and western influence. It is not as sophisticated technologically as Israel, but Iran compensates using sheer tenacity, state-sponsored hacking and asymmetry. The Revolutionary Guard Corps (IRGC) of Iran is in charge of a huge cyber infrastructure used to collect intelligence, to conduct propaganda, and to attack critical infrastructure.

The cyber policy in Iran is reactionary and ideological. Following the Stuxnet attack, Iran accelerated development of its cyber capacity, targeting the Israeli institutions, American banks, Saudi oil companies and rebels. Key ones are the Shamoon virus attack on Saudi Armco in 2012, attacks on Israeli universities and transport system and influence. actions against the political systems found in the West.

Iran uses its cyber strategy in defence as well as in offence. On the defensible side, it tries to prevent future attacks and the defence of national sovereignty. Offensively, it expands the influence of Iran on regional and international affairs and often through cyber-proxy organisations as the country avoids using state actors but instead leverages non-state actors to conduct kinetic adaptation. With respect to again, the regime would prefer deniable low-cost disruption and hence would target social media, phishing, and ransomware.

Third Party: the United States,

The third great actor is the United States that contributes to the Israel-Iran cyber war equation. It acts as a strategic player and facilitator as well. The U.S. is both an old friend of Israel and a resounding enemy of Iran, and it can play both offences and establishment of international norms in setting cyber security.

Stuxnet was the initially known and developed and deployed state-created weapon of chaos that caused physical damage; it was co-developed and deployed by the U.S. Severe since then, it has been using its Cyber Command attacking Iranian networks, retaliating election meddling, and defending its infrastructure. Valuable intelligence sharing and technological support and political strength is also provided to Israel by the U.S. As all this goes on, the sanctions Washington imposes and the military threats still provoke the Iranian cyber revenge.

A Realist approach to the U.S. engagement in the war is the best way to describe the nation as one that views cyberspace as just another domain where hegemonic control can be imposed, where the threats to a nation and its allies can be dominantly executed as well as where security of a nation and its allies can be effectively managed. However, the U.S., too, is faced with a dilemma: it is facilitating attacks by Israel in the sphere of cyber operations and, on the other hand, it has no right to allow acts that will result in a chain of uncontrollable incidents especially when the civilian networks are involved in it.

Methodology:

To complete the work, case study analysis is used as the key method, and the major cases studied are the most outstanding cyber incidents, such as the one of the Stuxnet, 2010, the attacks of Shaman, and the recent tit-for-tat cyber hack of Iran and Israel. These events are key examples through which we should look at the behavioural patterns, decision processes, and foreign motivations of the participating states. Case study research can be used to conclude the existing themes and approaches to cyber warfare which is independent of an event.

Constructivist approach is used in conjunction with the realist theory which is used in guiding the interpretation of evidence. Realism focuses on national interest and national security, constructivism explains identity, ideology, and norms (i.e., theocratic thought of Iran or existential security of Israel). This is a requisite two-theory methodology in addressing the case of why these states behave this way in cyberspace, but not only due to material capabilities.

The research uses secondary data as the source of analysis. These include:

Literature involving academic books and peer reviewed journal articles on international relations, warfare on cyber space, and Middle East security

U.S., Israeli and Iranian official publications and statements and government sources Reports by cybersecurity firms and think tanks (e.g. FireEye, Recorded Future, RAND corporation)

International news agency news reports (e.g., The Guardian, New York Times, Al Jazeera) Intelligence evaluations and political speeches by heads of states that have been declassified These texts are subjected to content analysis to extract such outstanding themes as deterrence, sovereignty, retaliation, ideological narratives, and strategic alliances. Particular concern is given to words and actions indicating the alterations to the cyber doctrine, collaboration of states, and escalation patterns. The research is absolutely non-intrusive ethically. There is no compilation of primary data on human subjects in front of it and all is in the open. Despite that, the critical evaluation of the sources is needed particularly in cases when the sources are owned by states or leaks of intelligence which can include propaganda or disinformation. To attain validity and triangulation, the information of more than one type of source (academic, technical and political) is cross-verified. By way of example, the reported incident of a cyber incident is only tracked to have happened when more than one independent cyber security account or government verification has reported it. Its shortcomings are that it cannot access classified cyber intelligence and the fact that it is inherently difficult to point the finger of blame squarely at a cyber attack. However here the analysis will not be on the technical forensics but on the strategic and ideological implications that has enough open sources to document. Altogether, this case study-based qualitative method provides a good structure to study the Israel-run versus Iran case of cyber warfare and the United States connection, so that one can have a complete insight into the incorporation of cyber warfare in the contemporary world politics.

Disassociation:

Defined as a term in the field of international cyber warfare, is a subjective way in which state actors are deliberately disengaged/separated with direct liability over cyber affairs. This is particularly true in the case of Israel and Iran where the two countries conduct the high end cyber attacks however, they like to deny them. United States being one of the most influential actors in the development of the cyber world in the Middle East is usually eminent in the use of dissociation to create a situation of plausible deniability in advancing such strategic interests. Dissociation is one of the strategic and tactical tools that is used in cyberspace wars. Cyber attacks per se are difficult to attribute with a certain degree of certainty due to the anonymity of the internet, the exploitation of the third-party infrastructure, and proxy actors such as the use of hacker groups or shell companies. Thus, such states as Israel and Iran are capable of offensive cyber actions, e.g., hacking to steal data, attacks on infrastructure, or malware releases, yet publicly deny such activity. This activity that falls in that grey zone allows them to achieve strategic aims, but does not incite an immediate military action or break the international norms entirely. Among the most prominent examples of dissociation one may mention the Stuxnet worm developed by the United States and Israel and designed to destroy the Iranian nuclear enrichment program in 2010. International observers agreed that the action marked a milestone in the field of cyber warfare, although both countries publicly denied their part in the attack, even though journalists and computer security firms later confirmed their involvement publicly. The dissociation, in this case allowed them to shut down the Iran program without going to an open war or censorship of international law. In addition, Iran has been credited to other cyber campaigns against Israeli infrastructure, American banks, even Saudi petroleum firms, through the group like APT33 or Charming Kitten as online proxies. Such groups allow Iranian state to remain detached in the activities and they have repudiated the existence of state support even though evidence is clear regarding effects of Iranian government involvement. There are two roles of the United States in this system of dissociation. On the one hand, it helps Israel in the collecting of intelligence, logics, and technology development towards cyber-based activities. On the one hand, it conducts an international discourse of a rule-based international order and encourages responsible state behaviour online.

Dissociation therefore makes the U.S justify its secret alliances and open diplomacy. It can morally aggress in cyberspace through such operations as the U.S. Cyber Command and the National Security Agency with the shifting of blame onto non-state actors or official denial simplicity. Ethical and legal consequences of dissociation are also very serious. It also blurs the chain of accountability, and it becomes difficult to tell who is to be held next after a cyber attack leads to loss of money or injuries to civilians. It even contravenes norms of the international level focused in controlling cyber action to de-escalation. In practice, dissociation has enabled the powerful to be aggressive yet seem to remain modest in the society. Lastly, this is dissociation, which is the most ideal tactic of the Israel-Iran cyber war and the U.S. junction. It enables the states to exercise their power, define the opinion, and avoid responsibility. Amidst the increasing efforts to engage in cyber warfare as the centre piece of world politics, there is need to understand the concept of dissociation so as to deliberate what major participants do and develop appropriate international regulatory orders.

Conciliation:

The cyber war between Iran and Israel has become a continuous cyber battle characterised by spying, sabotage as well as targeting of essential infrastructure. Amidst this strategic interest between the sides, conciliation may prove to be rather an intricate and a daunting venture. The situation regarding the involvement of the United States is the core issue of any possible reconciliation because the United States involvement has in many more cases escalated the tension instead of pacifying it. Making peace between Iran and Israel would entail developing trust on both sides that they do not enjoy nowadays since they have been at odds with each other over decades, philosophical attributes as well as proxy wars. Such cyber activities like the suspected Israeli attack on the Iranian nuclear station, the stuxnet and the counterattacks on Israeli state infrastructure by Iran have entrenched positions on either side. Nevertheless, joint weaknesses in the cyber-space can serve as points of discussion, including dangers to key facilities, systems supporting civilian infrastructures and jeopardises economies. Regional agreements on cyber security or backchannel diplomacy are examples of initiatives that can become the first step towards decreasing cyber hostility. A decisive force in the Iran-Israel scenario, the United States has a history of aiding Israel in cyber capacity and levying cyber sanctions against Iran. Although the U.S. usually claims that it only acts in the interests of regional stability and nuclear non proliferation efforts, the extensive role played by the U.S has been seen as bias and hostile by the Iranians. To host a successful conciliation, U.S would have to act in a more neutral and visible manner. It will involve de-escalating bilateral cyber-activity, facilitating multilateral talks, and enhancement of confidence-building agreements between Israel and Iran. Confidence-building might have such aspects as cyber hotlines, joint incident response systems, third-party monitoring of cyber actions that hopefully are organised within the framework of international institutions such as the United Nations. Although tricky, these measures would provide the basis toward de-escalation. There is however less political will behind such conciliation. Iran still does not recognise the legitimacy of Israel and Israel considers its survival to be threatened by Iran. Moreover, the domestic politics and strategic interests of the U.S in the Middle East area make it a doubtful prospect as a neutral mediator. To sum it up, rapprochement in such an area as cyber warfare between Iran and Israel cannot be an easy task but not impossible. That would necessitate drastic changes of policy prance and participation of all the three players. The lack of cooperation and reciprocity may turn the cyber-warfare into full-scale regional volatility, so the necessity of diplomacy is as critical as it has never been before.

References

Buchanan, B. (2017). Cyber threat by Iran; An enlarging menace to the US and its allies. Center of strategic and international studies. The author is J. Clarke, the source is retrieved here: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170530_Buchanan_CyberThreatIran_Web.pdf

Clarke, J. (2016). Stuxnet: A virtual first arms. Harvard Kennedy school Belfer centre of science and international affairs. Accessed on https://www.belfercenter.org/publication/stuxnet-first-digital-weapon

Hoffman, B. (2014). The cyber ability of Iran: a dimension of warfare. RAND Corporation.

Katz, S. T. (2016), Retrieved from https://www.rand.org/pubs/research_reports/RR610.html The cyber war, between Israel and Iran: A new dimension in the battle. The National Interest. It was retrieved on https://nationalinterest.org/feature/the-cyber-war-between-israel-and-iran-new-front-the-conflict-17363 The future of cyber warfare - Stuxnet.

H. Nissenbaum, (2017). The part that United States played in cyber operations against Iran. Journal of Cyber Policy 2, no. 1 (2017): 1-20. https://doi.org/10.1080/23738871.2017.1299565.