Cyberspace: The Next Arena for the Saudi-Iranian Conflict?

Ron Deutch and Yoel Guzansky

The combination of structural vagueness embodied in large cyber operations and their potential to cause real damage makes cyberspace the ideal field of action for Saudi Arabia and Iran and matches their strategic outlook and their concept of the use of force. The risk and the opportunity that cyberspace offers to each of these countries make it tempting, particularly when it concerns the long-term investment of resources. Cyberspace can therefore be expected to become another central arena of conflict between Saudi Arabia and Iran, given the limitations of conventional force.

Keywords: Saudi Arabia, Iran, cyber warfare, asymmetric warfare, Israel, United States

Introduction

Saudi Arabia and Iran have had a strong rivalry for some time. In spite of attempts over the years to reach a compromise, or, at least, certain strategic understandings to reduce the tensions between them, the two countries have continued to regard each other as a significant threat. Nonetheless, and despite their territorial proximity, they have never had substantial and direct military conflict between them but rather isolated clashes (especially during the Iran-Iraq war) and usually through third-party forces. The reason could be because of the nature of their armed forces and their operational concept. Historical, social, and geopolitical reasons have led to a situation

Ron Deutch is an intern at the Institute of National Security Studies. Dr. Yoel Guzansky is a senior researcher at the Institute of National Security Studies.

where neither Saudi Arabia nor Iran have ground forces that are able to perform extensive maneuvers beyond their borders, including against each other. Moreover, the Saudi army suffers from being extremely inefficient despite huge budgets, while the Iranians maintain an operational concept of their forces derived from a rationale of opposition and asymmetric warfare, as expressed by the central status and role of the Revolutionary Guards, and, in particular, the branch of the missile forces.[1]

Saudi Arabia and Iran's operational concept of the military force translates in theory into a broader strategic-political view, emphasizing psychological warfare and the use of terror and "proxies" under the radar in order to undermine their enemies. Perhaps it is possible to see a resemblance (whether rightly or wrongly) between this operational concept and the Gerasimov Doctrine, a relatively new concept in recent years that is gaining in importance as a potential approach to warfare and foreign policy in general.[2] Ascribed to the Russian General Valery Gerasimov, this doctrine is based on what he wrote in 2013, in which he described a kind of "new form" of wars. Alongside conventional military efforts, this new form included other channels of action, such as the use of the media, internal subversion, cyber, and any other means that can sow chaos in the enemy's ranks.[3]

This approach could acquire a particularly interesting angle when it is examined in the light of the development of cyber warfare. The combination of structural vagueness with the potential for real damage embodied in large cyber operations makes this the ideal field of action for Saudi Arabia and Iran's concept of the use of force. Thus, this article seeks to examine to what extent, if at all, cyberspace could become the main arena for the clash between Saudi Arabia and Iran. For this purpose, the article compares the cyber capabilities of each country, at both defensive and offensive levels, and tries to reach a conclusion as to whether cyberspace could provide one with the ability to achieve what they have failed to attain by conventional military means.

---

1 Uzi Rubin, "Missiles as the Flagships of the Iranian Regime's Vision," (Jerusalem: Jerusalem Institute of Strategic Studies, November 23, 2018).

2 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018.

3 Molly K. McKew, "The Gerasimov Doctrine," *Politico Magazine*, September/October 2017.

Cyber in Saudi Arabia

The field of cyber did not attract much attention or consideration in Saudi Arabia until recent years. However, the kingdom's vulnerability to potentially dangerous cyber threats is constantly increasing. There are two main channels for potential damage. First is the "direct" channel, including possible attacks on both military and civilian infrastructures and facilities, which could lead to extensive economic damage, and even a high number of human casualties. A striking example of the destructive capability of this type of attack was witnessed in 2017, in the cyberattack directed at one of the Saudi Kingdom's petrochemical plants.[4] The purpose of the attack was not to steal information or harm Saudi databases but rather to cause real physical damage and an explosion that would disrupt the plant's systems. The operation failed due to an error in the attack code. Investigators believe that Iran was behind the attack, which has since corrected the error in the attack code, and now it is only a matter of time until it again acts against Saudi Arabia with greater intensity and sophistication.[5] Besides the focus on the threat to critical infrastructures and control systems that aim to interfere with the chain of supply and even cause physical damage, it is also possible now to identify a growing threat to information systems in Saudi organizations, for both disruptive and espionage purposes. At the end of 2016, several Saudi government targets were attacked, including the computer systems of the Central Bank of Saudi Arabia, by means of the Shamoon malware. This virus was first used back in 2012, in a large-scale cyberattack against Aramco, the Saudi national oil company. These examples are just some of the much larger series of attacks, hinted at by a senior figure in the Saudi cyber sector and who estimated that in 2015 alone, the kingdom had absorbed about 60 million cyberattacks, at a rate of about 164,000 attacks per day.[6]

In addition to the direct cyberattack channel, there is also the "indirect" channel, using the popular internet platforms such as Facebook and Twitter in support of elements opposed to the Saudi regime to ferment internal unrest. The advantage of this method is in the fact that it could have a much

4 Nicole Perlroth and Clifford Krauss, "A Cyber-attack in Saudi Arabia Failed to Cause Carnage, but the Next Attempt could be Deadly," *The Independent*, March 21, 2018.

5 Ibid.

6 Ibrahim al-Hussein, "60 Million Cyber-attacks Targeted Saudi Arabia in One Year," *Al Arabia*, May 2, 2018.

lower signature than direct cyberattacks, because of the attacking country's ability to disguise its activity as authentic internal protest, partly by using fictitious social media accounts. A combined action scenario should also not be ruled out: low signature cyber activity, causing a large civilian disaster that shocks Saudi society, combined with increased cybernetic subversion, exploiting the sensitive situation in order to encourage an active uprising against elements in the Saudi royal family.

The Saudi elite is beginning to understand the destructive potential of the cyber dimension and is trying to deal with it. At the same time, however, there are several internal factors that hamper these efforts. Above all, there is the structural split in the Saudi government, whereby the powers to deal with cyber strategy are divided between many power centers belonging to different ministries and organizations. This situation makes it difficult to draw up and implement a uniform cyber doctrine to meet the kingdom's various security needs.[7]

Another major obstacle that hampers Saudi efforts to deal with cyber threats is the relative technological backwardness of Saudi society. This problem is not new and is not unique to the cyber issue, but it touches on many of the deep ills affecting the kingdom. For many decades, oil wealth made it unnecessary to develop other economic sectors. The regime also "bought" popular acceptance through generous subsidies and a multiplicity of superfluous government posts, but, to a large extent, this deprived people of the incentives to work hard and acquire higher education. As a result, Saudi Arabia lacks the human and technology infrastructure needed to achieve the cyber capabilities it needs, including for civilian purposes, and is forced to rely on external help (information technologies account for only 0.4 percent of Saudi GDP).[8]

To try to overcome these difficulties, in recent years Saudi Arabia has taken a number of steps that have slightly improved the situation. Today it is possible to distinguish three major agencies in the kingdom operating simultaneously in the cyber field. The first is the National Cyber Defense Authority (NCA), which was established in 2017 by a royal order and is

7 Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm, *Kingdom of Saudi Arabia Cyber Readiness at a Glance* (Potomac Institute for Policy Studies, 2017), pp. 23–24.

8 Ibid, p. 3

subordinate to the king and the crown prince. It is responsible for coordinating policy, guidelines, and training in cybersecurity for all government bodies, as well as private ones.[9] In essence, this is the organization with the overall responsibility for security technology in the kingdom. The second is the Saudi Federation for Cyber Security & Programming (SAFCSP), which is subordinate to the Saudi Olympic Committee and mainly responsible for preparing personnel and technological infrastructure for the cyber and programming sector in the country. Part of its regular activity is to organize conferences and competitions, in order to increase awareness of cybersecurity issues, encourage young people to specialize in this field, and serve as a potential technological reserve.[10]

While these two agencies operate openly, a third one is more attack-oriented and covert by nature, which, until recently at least, was reported to be run by Mohammed al-Katani, a close associate of Crown Prince Mohammed Bin Salman. This agency, the Center for Studies and Media (CSMA) in Riyad employs hundreds of Saudis who function as "an army of trolls" on social media channels, and their job is to monitor opponents of the regime, delete critical responses on sensitive matters, and post positive responses to Saudi royal policy.[11] Although many of its activities are carried out far from the spotlight of western media, the murder of the journalist Jamal Khashoggi put al-Katani on center stage together with the information war taking place under his direction, to which Khashoggi represented a significant threat.[12]

Notwithstanding the recent developments in Saudi Arabia in the field of cyber, it will take time to fully bridge the considerable gaps. Until the processes that were mentioned above gain momentum, Saudi Arabia will try to compensate for the gaps in its technological knowledge and infrastructure by purchases from other countries in the short to medium term. In the case of military procurement, Saudi Arabia is the largest customer of the United States, and the two countries have fruitful cooperation in the cyber field. The

9 "Follow Basic Cyber Security Standards, Govt Agencies Told," *Saudi Gazette*, October 7, 2018.

10 Official website of the Saudi Federation for Cyber Security and Programming, https://safcsp.org.sa/en.

11 Adam Goldman and Karam Shoumali, "Saudis' Image Makers: A Troll Army and a Twitter Insider," *New York Times*, October 20, 2018.

12 David Ignatius, "How a Chilling Saudi Cyberwar Ensnared Jamal Khashoggi," *Washington Post,* December 7, 2018.

MOU's signed by President Trump during his visit to Saudi Arabia in May 2017 included agreements on cybersecurity to help fill Saudi gaps in this area. It was also reported that contractors on behalf of the US administration are providing cyber defense consultation and training to Saudi Arabia and are also operating directly within Saudi ministries to protect them against cyberattacks. One of these companies, Booz Allen Hamilton, even felt it necessary to stress that its cyber involvement in Saudi Arabia does not include building offensive capabilities.[13]

The gaps in Saudi cyber capabilities could also influence its relations with Israel, which, as a cyber power, has a lot to offer the kingdom in this field. According to various reports, it is possible that such links already exist, or at least have existed in the past. In this framework, it was reported that parties connected to the Saudi regime had used the Pegasus spyware from the Israeli company NSO in an attempt to eavesdrop on its opponents.[14]

Another possible channel for Saudi Arabia is to create a shared cyber defense infrastructure jointly with the Gulf States under the Gulf Cooperation Council (GCC), or some of them, who face similar threats. Calls for such cooperation have already been heard, although the considerable tensions between some of these states mean that effective practical steps are still nowhere in sight.[15]

Iran's Cyber Capabilities

Unlike Saudi Arabia, Iran has a fairly well established infrastructure of cyber capabilities, both defensive and offensive. Iran's main targets of attack in recent years include Saudi Arabia, Israel, and the United States.[16] Iranian cyber activity is supervised at the highest levels of the regime, including the president and the commander of the Revolutionary Guards, and is maintained in several ways. First, the Iranian regime invests heavily

13 Michael Forsythe, Mark Mazzetti, Ben Hubbard, and Walt Bogdanich, "Consultants Stick with the Saudis," *New York Times*, November 8, 2018.

14 "Israeli Hacking Firm NSO Group Offered Saudis Cellphone Spy Tools – Report," *Times of Israel*, November 25, 2018.

15 Ramola Talwar Badam, "GCC Urged to Coordinate Cyber Security following Wannacry Attack," *The National*, May 21, 2017.

16 Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat, Espionage, Sabotage and Revenge," *Carnegie Endowment for International Peace*, 2018, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

in research and training, based on a strategic perception of the importance of cyber.[17] Second, signing the nuclear treaty with the superpowers in 2015 opened up an opportunity for Iran to establish numerous opportunities for cooperation with universities and scientific institutes around the world. Iran exploited this opportunity to promote its cyber capabilities through working with institutions possessing the relevant knowledge.[18] Third, Iran's exploitation of foreign cyber knowledge is not limited to official cooperation. In 2013, Iran established the Mabna Institute, with the aim of gaining access to scientific resources from outside Iran.[19] While this goal is focused not only on the field of cyber, this is another possible channel with the potential to help Iran build its cyber capabilities.

Iran has certainly experienced the dangers embodied by cyberspace. The clearest example of this is the Stuxnet malicious worm that damaged Iranian nuclear infrastructures in 2012. But even before that, Iran had experienced cybernetic danger of another kind: The widespread protests in the streets of Teheran in 2009 illustrated the destructive potential of internal opposition groups and the flow of subversive ideas from outside. At that time, the Iranian regime started a project of isolating networks, with the aim of transferring all Iranian communication to an internal state-run network, cut off from the international arena, giving the regime full control of all content entering the country and better protection against cyberattacks.[20] This objective is backed by the Iranian "cyber police's" aggressive enforcement activity against subversive elements active on the internet.[21]

Apart from that, Iran invests extensive efforts in the development and assimilation of cybernetic capabilities, as well as practicing its operating

17 Gabi Siboni and Sammy Kronenfeld, "Developments in Iran's Cyber Warfare 2013–2014," *Military and Strategic Affairs* 6, no. 2 (August 2014): 84.

18 Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018.

19 According to FBI data, the victims of the Mabna Institute's activity include 3,768 professors in 144 universities in the United States alone, and 4,230 professors spread among 176 universities in 21 different countries, including Israel, Germany, China, South Korea, Britain, and Turkey. See Lior Tabansky, "Iran's Cybered Warfare Meets Western Cyber-Insecurity" in *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace* ed. Fabio Rugge (Italia: ISPI, 2018), p. 130.

20 Siboni and Kronenfeld, "Developments in Iran's Cyber Capabilities," p. 85.

21 Ibid., p. 88.

concepts. Examples can be seen in the exercises carried out in 2012 and 2013, which tested respectively the Iranian cyber defense systems in the naval and ground forces of the Revolutionary Guards.[22] Recently, Iran has reported that it has discovered a more advanced version of the Stuxnet worm, although they claim that it has not yet managed to cause any damage. Following that, the head of the Iranian cyber system, General Gholam Reza Jalali, estimated that Iran was no longer under significant cyber threat and was therefore making the issue low priority. This report could indicate that Iranian cyber capabilities have been considerably improved, although this could be no more than psychological deception.[23]

While developing advanced defensive capabilities, Iran has also made impressive strides in the development of its offensive cyber arsenal. Iran is undoubtedly at a more advanced stage than Saudi Arabia in these capabilities, although it is apparently still lagging behind the large cyber powers like China, Russia, the United States, and Israel. The Iranian offensive cyber system is largely under the responsibility of the Revolutionary Guards and belongs to a sub-organization called the Iranian Cyber Army (ICA). This system suffers from a structural weakness due to its semi-contractual nature as most of Iran's cyber offensives are not carried out by Revolutionary Guards people but rather by semi-independent individuals and hacker groups, who are paid according to their success. In the absence of ideological commitment and the search for greater profits, many of these Iranian hackers become problematic candidates for the Revolutionary Guards. Consequently, the regime is adopting a multi-layered approach: At middle level management, they place officers who are ideologically committed to the regime, and they determine the objectives and assign tasks to ad-hoc sub-contractors; that is, groups of civilian hackers who are paid per task.[24] In addition, there are the cybernetic "proxies" who operate in a more ideological context. A prominent example is the Lebanese Hezbollah organization, whose ties to the Islamic Republic of Iran provide it with relatively advanced cyber capabilities in

22 Ibid., p. 87.

23 "Iran accuses an Israeli company of a cyber attack," *Jerusalem Center for Public & Political Affairs*, November 5, 2018.

24 Gundert, Chohan, and Lesnewich "Iran's Hacker Hierarchy Exposed," p. 5.

contrast to other terror organizations.[25] These capabilities are activated as necessary and represent a further cybernetic attack arm for the Iranian regime.

In addition, the Iranian regime activates its "soft" attack capabilities, namely the psychological warfare conducted by means of manipulating information on social networks and news websites, similar to what Saudi Arabia does. A prominent example of this capability— which was recently exposed—is an operation dubbed "Ayatollah BBC," a large-scale campaign on behalf of the Iranian regime in which news sites all over the world were faked, led by the Persian-language BBC site. The fake sites contained deliberately manipulative content, to meet the needs of Iran's psychological warfare.[26]

Conclusion

This article examined the feasibility of cyberspace developing into the next arena for widespread conflict between Saudi Arabia and Iran. In fact, cybernetic clashes between the two have already occurred, although this is not yet the focus of friction between them. Therefore, when discussing the Saudi-Iranian conflict in cyberspace, a distinction must be made between the short to medium term and the long term. As their experiences show, both these countries suffer from cybernetic weaknesses, which have the potential of opening them up to highly significant strategic damage. These weaknesses could turn out to be the cracks that bring down one of the two regimes, if one succeeds in landing a sufficiently severe blow. Since this is the case, the risks and opportunities that cyberspace represents for both Saudi Arabia and Iran make it tempting, particularly when it is a question of long-term investment of resources.

At present, it appears that the cybernetic capabilities of both these countries are too meager to cover full-scale conflict between them. They fulfill an important supporting role but are still insufficiently developed to provide a response for each country's security concept. Evidence of this can be found in the relatively simple means of aggression used by both Saudi Arabia and Iran in cyberspace. They include, above all, the dissemination of "fake news" and subversion through social media. Neither Saudi Arabia

25 Ben Schefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018.

26 "Ayatollah BBC – An Iranian Disinformation Operation against Western Media Outlets," *Clearsky Cyber Security*, 2018.

nor Iran possess wide-scale cyberattack capabilities; as far as it is known, Saudi Arabia still lacks independent technological abilities, and while Iran may be more advanced in this respect, it still relies to a large extent on semi-random "mercenaries."

The more interesting question that should be asked concerns the long-term trends. As already mentioned, decision makers in both Saudi Arabia and Iran are well aware of the potential for both damage and benefit inherent in cyberspace and are taking steps to position themselves as players in this field for the long term. To this must be added the strategic balance that the two have between them: neither Saudi Arabia nor Iran has the capabilities to defeat the other side using only conventional military means. This being the case, the decision to turn to the cyber channel—with the options it presents—is the obvious step. In this sense, we cannot rule out the possibility that we are seeing the first signs of a Saudi-Iranian technological race, in addition, of course, to all the cybernetic threats that separately occupy each of these two countries.

It is hard to predict the outcomes of such a race: On one hand, although it is possible to argue over Iran's status as a regular cyber power, at present Iran undoubtedly has an advantage over Saudi Arabia in this field. Iran has relatively well developed defensive infrastructures and valuable experience gained during the years of dealing with Israeli and American attacks. Also, unlike Saudi Arabia, which lacks real "hard" attack capabilities, Iran has demonstrated its ability to attack Saudi and western targets—American in particular—over the internet, even if it is apparently unable to mount a systematic and broad attack like Israel, Russia, and the United States. Finally, and above all, while Saudi Arabia is lacking technological and human infrastructure in the cyber field (or at most, only the first stirrings of such infrastructure), Iran has already invested extensive resources in providing university training and in working with foreign institutions, and even in stealing knowledge. All this has placed Iran several steps ahead of Saudi Arabia, and over time, this gap could become fatal for the kingdom.

On the other hand, there are two important factors that could work to the benefit of Saudi Arabia in the long-term technological race and block Iran's advancement. The first is the Saudi Kingdom's huge advantage in resources. The Saudi security forces enjoy some of the largest annual budgets in the world. If they are properly channeled and the smart investment in cyberspace

is increased, alongside those in advanced technological education, Saudi Arabia can accelerate its technological progress. Meanwhile, Iran, buckling under the burden of international sanctions, has difficulty in allocating similar resources to the development and acquisition of new capabilities.

Another important factor is the defense umbrella and the cooperation existing between Saudi Arabia and the world's largest cyber power—the United States. As a central ally, the United States can provide Saudi Arabia with the cybernetic defense umbrella and technological capabilities that will enable it to catch up with the Iranians. To this can be added what appears to be covert but frequent cooperation with Israel, which, as already stated, is a cyber power in itself. The relative weight of these benefits will increase as time passes. If they are wisely exploited by the kingdom, they could emerge as a real asset and give it a decisive advantage over Iran.

An examination of the current cyber capabilities of Saudi Arabia and Iran shows that a wide cybernetic conflict between these two countries is probably not imminent; however, the nature of cyberspace and its structural vagueness make it particularly suited to the way their concept of operational conduct. Therefore, in the medium-long term, we can expect both to make increased use of cyberspace as an additional way of damaging the enemy, in contrast to the limitations of their conventional forces, which have held them back until now.