INSS Insight No. 1190, July 10, 2019

How Prepared is Saudi Arabia for a Cyber War?

Yoel Guzansky and Ron Deutch

One facet of the recent American-Iranian escalation is the cyber realm. Moving the conflict into cyberspace enables one side to commit retaliatory acts while reducing the impact that requires the other side to respond and escalate: this is how the cyberattack by the United States in response to Iran's downing of the American drone should be understood. Yet considering the rapid development of knowledge and technology in all that is related to cyberspace, integration of the cyber dimension into the sphere of international conflicts poses a real danger to countries that lag in the technological race. In this context, Saudi Arabia is particularly vulnerable.

Since Saudi Arabia is in the "line of fire" in the conflict between the United States and Iran and could well suffer a kinetic blow, its readiness for a scenario in which escalation spills into the cyber realm merits examination.

Although Saudi Arabia is not directly involved in the current escalation in the Gulf, geopolitical circumstances place it in the direct line of fire from a cybernetic perspective. Iran does not shy from attacking civilian-financial targets that it identifies as less protected and therefore more vulnerable than military ones. Moreover, Saudi Arabia is among the countries that suffer the greatest number of cyberattacks in the world, and it is believed that most of the attacks against it come from Iran. For example, 42 percent of the cyberattacks carried out by an organization known as APT33, which is identified with Iran, were directed over the past three years against Saudi targets, while "only" 34 percent of the attacks were directed against American ones.

Both the United States and Iran face a strategic dilemma. On the one hand, they do not want a comprehensive conflict in the Gulf (as statements from the highest echelons of both countries indicate). Therefore, both sides have an interest in not taking measures that will escalate the situation. However, escalation in the Gulf can occur not only as the result of a terror attack by Iran, but also in response to American action against Iran's nuclear program. On the other hand, Tehran believes it must respond to the latest wave of sanctions imposed by the US administration. Similarly, the United States fears that Iran and the Gulf states may view a lack of response to provocations as weakness, and Gulf

confidence in the United States as an ally could be undermined, which in turn could encourage Iran to persist in its acts of aggression.

As the main United States ally in the Gulf, Saudi Arabia is at risk. Since the strong United States abilities as far as cyber protection may make it difficult for Iran to carry out a significant attack directly against it, Iran might choose to strike at Saudi Arabia, the "soft underbelly" of the United States in the Gulf, in order to pressure the administration to lighten its policy of sanctions without requiring it to respond on a large scale. Saudi Arabia's relatively low capability in the cyber realm makes it a fairly easy target. Moreover, given its economic and geopolitical importance to the international community, cyberattacks against Saudi targets could result in substantive damage.

There are two main potential channels for Iranian cyber activity against Saudi Arabia. The first is the "direct" channel, which includes attacks against Saudi installations and infrastructures, military and civilian alike, that could inflict heavy financial damage and even claim a high number of lives. An example of this kind of destructive potential occurred in 2017, in a cyberattack against one of the kingdom's petrochemical plants. The purpose of this attack, which failed due to a code error that disrupted its activity, was not to steal or harm Saudi databases, but rather to cause actual kinetic damage – in this case, an explosion by interfering with the plant's systems.

Joining this channel is an "indirect" one – the use of fake accounts on popular online platforms, such as Facebook or Twitter, in order to support for opponents of the regime and nurture internal dissent within the kingdom. The advantage of this type of action is that it can have an even lower signature than direct cyberattacks, due to the attacking country's ability to conceal its activity and portray it as authentic internal protest. The possibility of a multi-pronged attack cannot be ruled out either. In this kind of scenario, a low signature cyberattack causes a large scale civilian disaster that shocks Saudi society. At the same time, increased cyber subversion exploits the sensitive internal situation to encourage an active uprising against the royal house. Iran has an interest in strengthening fears in Saudi Arabia that it is able to stimulate Shiite subversion against the royal house – a fear that in the past "helped" stop Saudi Arabia from acting against Iran.

Aware of the risks of a cyberattack, the Saudi royal house is working on building a suitable cyber strategy, but internal elements are hard pressed to cope. First, the structural administrative split in the Saudi regime divides the relevant powers among many power centers in different ministries and agencies. This situation makes it difficult to create and enact a uniform cyber policy that will meet the kingdom's diverse security needs.

Another major obstacle is that Saudi society is technologically backward, which is a problem that bests the kingdom at large. Decades of oil wealth made it unnecessary to develop other economic sectors. In addition, the quiet on the civil front purchased with generous subsidies, together with an inflated number of government jobs, gave the population no incentive to work hard or pursue advanced education. As a result, Saudi Arabia lacks the human and technological infrastructure required for advanced capabilities in the cyber sphere as well. The information technology industry comprises approximately 0.4 percent of Saudi Arabia's gross national product, and the kingdom relies mainly on outside assistance for cyber-related civilian needs.

In order to overcome these difficulties, Saudi Arabia has taken measures in recent years that have improved the situation slightly. It established three main branches linked to the cyber sphere that work concomitantly. The first is the National Cybersecurity Authority (NCA). Established in 2017, the NCA, which is subordinate to King Salman and Crown Prince Mohammad bin Salman, is responsible for policy coordination, regulation, and training in cyber defense for all government and private organizations. For all practical purposes, the NCA is the main agency in charge of security technology itself in the kingdom. It is joined by the Saudi Federation for Cyber Security and Programming (SAFCAP), which is subordinate to the Saudi Olympic Committee and is responsible mainly for preparing personnel and the technological infrastructure required for the cyber sector and for programming. As part of its ongoing work, SAFCAP organizes conferences and competitions in order to increase awareness of cybersecurity issues and encourage young Saudis to specialize in that field and become a technological reserve. Both these agencies are joined by a third, secret, and more aggressive entity, which was run (at least until the assassination of Saudi journalist Jamal Khashoggi) by Mohammed al-Qahtani, the Crown Prince's right-hand man. This agency employs hundreds of Saudis who act as a "troll army" on the social media channels, monitor opponents of the regime, delete disparaging comments about sensitive subjects, and plant comments that support the policy of the royal house.

Despite the measures that the Saudi royal house has taken, the kingdom remains fairly vulnerable. A recent study found that only four out of ten Saudi CEOs reported that their organizations were prepared to deal with cyberattacks – this despite the Saudis' attempts to encourage education in this area (such as the international conference on cyber security that the kingdom hosted last February). Nor has the kingdom yet developed any real aggressive technologies, and relies on foreign technology for the small amount of such technologies in its possession.

As recent developments in the Gulf indicate, it is quite possible that the escalation between the United States and Iran will spill over increasingly into cyberspace. Such a

development poses a particular danger to Saudi Arabia, due to the possibility that the kingdom will be a means for Iran to harm American interests in the region. An examination of the kingdom's current situation in the cyber realm shows that it is unprepared for such a scenario, and the measures that Saudi Arabia has taken in recent years will bear fruit only in the long term. Therefore, for the sake of its security, Saudi Arabia must find short term solutions, such as acquiring technologies and assistance from foreign companies, in order to emerge from the crisis with as little damage as possible. The high level of vulnerability of the kingdom's oil production, refining, and transport system and its importance to the global energy economy strengthen the need for the United States and perhaps Israel as well to give of their knowledge and ability to upgrade Saudi Arabia's ability to protect itself in the cyber realm.