The Middle East in the Geopolitics of Digital

Julien Nocetti
Research Fellow
French Institute of International Relations (IFRI), Paris

The analysis of the political and strategic implications of digital technology has traditionally focused on the transatlantic relationship and the policies of certain authoritarian powers (China, Russia). Beijing's proactive policy in this field is as much about challenging the West's perceived technological hegemony as it is about shaping its own global digital vision and, in so doing, shifting the planet's digital centre of gravity to Asia. The United States is seeking to maintain its technological pre-eminence – particularly through its tech giants' capacity to attract and innovate – and that of its military by controlling the infrastructure and the data circulating through it. Russia and Europe seem to be more secondary players, with the former essentially showing an ability to be a cyberspace nuisance, whilst the latter remains caught between the strategies of the American and Chinese powers.

Within this swiftly changing global landscape, the Mediterranean and, more generally, the Middle East continue to play a relatively secondary role. However, the region is not immune to the turmoil caused by the digital revolution. The events of the "Arab Springs" in 2011 demonstrated to the world the power that social media and social networks afford oppressed populations to coordinate and mobilize. Faced with the new political potential of digital tools, those in power have proven able to adapt and are leading influence campaigns to discredit their opponents and "the street." Finally, regional power struggles have likewise not been spared from an increasingly sophisticated cyber component, as witnessed by the actions in this regard of Israel, Iran and even Saudi Arabia.

The Rise of a Protean Digital Activism

Over the last twenty years, Arab country's populations' lack of or very limited access to the digital sphere and the Internet has given way to its omnipotence, to the point where it has helped to destabilize political regimes. Since the advent of a more participatory and interactive Web towards the end of the first decade of the 2000s, the Arab-speaking digital sphere has emerged as a major forum for engagement, demands, protest and social, political, ethnic, cultural and religious struggles.

These virtual spaces go beyond the framework of states and their borders to the image of young bloggers from the Arab-speaking diaspora, who relay information and the various forms of mobilization. Whether for democratic or nationalist aspirations or religious radicalization, people's participation in the Arab-speaking digital sphere has become as important as their participation in physical spaces, which are sometimes prohibited, insufficient or blocked.

However, cyberactivism, which can lead to cybercrime, in many cases remains linked to real and physical forces with great potential to destabilize public order. This would include the digital strategies of social movements, such as the Tunisian UGTT trade union's mobilization in 2011, the Hirak protest movement in the Moroccan Rif region, or even the propagandistic activities of the Islamic State, Hezbollah or al-Qaeda, which spread their messages in part through militant groups. Since 2011, the "Arab Springs" have underscored the power of social media such as Facebook, YouTube and Twitter, which put the image of young Syrians who mobilized to report beyond their country's borders at the start of the civil war at the forefront of cyberactivists and netizens.

Tunisian bloggers have leveraged their connections to foreign networks to share information about events

in real time. For the latest news, journalists and bloggers around the world have turned to the blogs, Facebook pages and Twitter accounts of citizen-activists following events as closely as possible. A few days after the Tunisian uprisings, similar dynamics were on display in Egypt. And even though the Egyptian government blocked access to the Internet for more than five days, Twitter and Facebook could still be used to get around the censorship, especially with mobile phones. The Internet itself has become a *casus belli*.

Cyberactivism, which can lead to cybercrime, remains linked to real and physical forces with great potential to destabilize public order

Egypt and Tunisia offer two different examples of how social media can come into play. In the case of Egypt, long-term activism developed on the Internet. In Tunisia, such activism has failed to flourish due to state censorship and repression; however, social media have played an important role in bringing the regime to the brink. Social media can both give impetus to political and social reform and function full-time, in times of crisis, as a mobilization tool and information bank. In the cases of both Egypt and Tunisia, the outcome of this mobilization was hardly predictable.

New Influence Brokers

Social media have a horizontal operating logic that is often completely at odds with the prevailing vertical logic. They reconfigure traditional forms of allegiance, thereby transforming both real and virtual public spaces. We are witnessing the emergence of new ways of shaping opinion and new opinion brokers that elude and compete with the power of states. These new intermediaries transcend borders and the information they convey is disseminated in Arabic-speaking diasporic communities. It is necessary to speak of communities and diasporas in the plural (or sub-communities) insofar as they are home to heterogeneous feelings of belonging, values, and symbols. So it is with the Arab-speaking community in France, which brings together immigrants and children of immigrants, but also converts to Islam and students with no connection to the Arab world in either case. Although they share a language as a formative feature of a community, their norms and symbols of belonging are very different and are the source of contradictory expressions and mobilizations on social networks. The latter can even include propaganda, indoctrination and involvement in criminal activities that give rise to situations of tension leading to major destabilization.[1]

These forms of cyberactivism are also the preserve of state or parastate organizations, which use fake accounts and profiles to launch cyber influence, propaganda and counter-information campaigns. Since 2017, disinformation campaigns in Qatar, but also in Israel or the United States, have made headlines, reminding states of the importance of monitoring social networks and the Internet.

The Predominance of States

In the conflict-ridden context of the Middle East, states use every means at their disposal to defend and protect their interests. The cyber arena has emerged as a particularly useful strategic tool, given the wide range of actions it enables in terms of intelligence, sabotage and military operations, but also communication, information and attacks. These actions are not only difficult to identify and detect, but also, in some cases, quite inexpensive. However, not all players in the region have the same capabilities or perception of the strategic importance of the cyber arena. Whilst for some, cyberspace is a national priority, for others, interest in this subject can be limited to the issue of control of the Internet, when it is not directly approached solely from the point of view of crime.

States are the main players in cyberspace in the Middle East for the simple reason that mastery of this field requires not only technological know-how, suitable infrastructure and people with the necessary skills. The development of certain defensive and offensive

[1] Hecker, Marc. "Web social et djihadisme : du diagnostic aux remèdes," IFRI, *Focus stratégique*, No. 57, June 2015, 49 p.

capabilities also requires considerable funding, beyond the abilities of non-state groups. It is thus possible to establish a typology of the region's states, based on these criteria. This typology, in turn, will make it possible to address each one's national strategies.

Israel: The Regional Engine

Since 2009, the Netanyahu government has considered cyberspace a national and strategic priority. The Israeli Prime Minister wants to make his country a global leader in the field by allocating substantial financial and human resources to it.

However, not all players in the region have the same capabilities or perception of the strategic importance of the cyber arena. For some it is a national priority, for others it is limited to control of the Internet

The Israeli government has implemented a strategy that can be broken down into four largely complementary areas: raising public awareness of cyber issues and "computer hygiene," youth education, scientific and academic research, and the creation of a solid industrial foundation for information system security (ISS). Perhaps nowhere else is the "merging" of the civilian and military so clear: the two dimensions are perceived as heavily intertwined. More specifically, this characteristic is on display in the close civilian-military cooperation and the IDF's strong presence in the cyber ecosystem and national industry.

Conscription plays a key role in this regard, as young Israelis are placed in specialized units faced with specific cyber challenges on a daily basis, allowing them to swiftly acquire cutting-edge skills. The most well-known and famous is Unit 8200. Its area of expertise is electromagnetic intelligence and code decryption. Unit 8200 is particularly adept at cryptography and also has an elite unit that is regularly deployed in the field. It should be recalled that the IDF has both defensive and offensive technical know-how, human skills, and a structured infrastructure that afford it a real advantage over the armies of other states in the region.

Although the Israeli authorities publicly acknowledge their offensive activities in cyberspace, they have not admitted to being the source of viruses such as Flame or Stuxnet. This ambiguity seems to be part of a "cyber deterrence" strategy not unlike the Israeli nuclear doctrine. Israel thus seems to have moved on to a new stage in its approach to the cyber issue. But why now, when, to date, it had largely kept silent? Because in so doing Israel keeps up the pressure on Iran and the countries negotiating with Tehran. It is an indirect way of asserting that Israel has a wide range of means, including cyber resources, to conduct a potential military operation against Iran's nuclear facilities. This choice is thus not trivial. Iran, which has been the target of several computer viruses, has since become aware of the strategic importance of cyberspace and has moved to tackle the problem head-on.

Iran: A Narrowing Gap?

Needless to say, Tehran was sensitive to the issue of cyberspace well before it was targeted by sophisticated attacks. Nevertheless, those attacks have clearly led the Iranian authorities to question and readjust their cyber strategy, especially since the sudden emergence of the "Green Movement" in June 2009 and, especially, the Stuxnet computer virus in 2010. With these developments in mind, the Iranian leadership undertook the construction of a "national Internet," parallel to the global Internet, to which the population has been fully connected since 2015.

The Internet therefore occupies a special place in the Iranian strategy, even if the defensive measures that Iran has taken are not limited to this aspect alone. In fact, since 2010, the Iranian government has undertaken a renationalization of its cyberspace infrastructure, creating the Cyber Defence Command in 2010 and, in 2012, the Supreme Council of Cyberspace.

With regard to the offensive aspect, Iran has opted for indirect confrontation with the countries it deems hostile. Rather than frontal opposition, the Iranian authorities prefer to operate through intermediate adversaries. Iran thus supports movements that, although not officially attached to it, act in its interest. In this regard, the Iranian leadership has maintained the same

strategy in cyberspace that it has followed in other areas for several years. Such a choice makes it possible to avoid direct involvement and, thus, allows Iran to deny any responsibility for potential incidents quite easily. For instance, when the Saudi authorities accused Iran of being behind the cyberattacks on the Aramco facilities, the Iranian leaders said they had nothing to do with the operation, for which a group called the Cutting Sword of Justice had claimed responsibility. Technical experts believe that the computer virus used for that operation could not have been designed by a mere group of hackers, but nor could they prove that Iran was responsible for the attack.

To coordinate its strategy of asymmetrical confrontation in cyberspace, in 2010, Iran created the Basij Cyber Council, a cyber unit in the Basij Resistance Force, a branch of the Revolutionary Guard. This council works closely with several hacker groups and mobilizes cyber specialists from the Revolutionary Guard to train new hackers and help them acquire high-level skills.

With regard to all these initiatives, several countries regularly accuse Iran of being the source of attacks against them. These include Saudi Arabia and Qatar, for example, but also Israel, which claims that its information systems are targeted daily by Iranian infiltration attempts, and the United States, which blames Tehran for the cyberattacks affecting several US banks between September 2012 and January 2013. The US authorities believe that these incidents were a response to the economic sanctions that the Obama Administration imposed on Iran for the military dimension of its nuclear programme.

Cyberspace: A Strategic Communication Weapon

Mastering the "communication" dimension of cyberspace is, for some movements, as important as having efficient military means. This is because it is part of a form of psychological warfare that aims not only to damage the adversary's morale, but also to conquer hearts and minds. From this point of view, non-state groups are not the only ones concerned; states also see the interest in using such methods. This is not, of course, a novelty due to the emergence of new technologies; the notion of propaganda and counter-propaganda has always been part of international relations. However, the rise of these technologies has enabled broader dissemination of and greater exposure to each player's official discourses.

Mastering the "communication" dimension of cyberspace is, for some movements, as important as having efficient military means

For example, the Islamic State or Al-Qaeda in the Arabian Peninsula (AQAP) have made several films featuring portraits of and interviews with militants. Indeed, these groups have their own websites and video production centres. These videos are then uploaded to the Internet, through platforms such as YouTube and Facebook or on jihadist forums. Al-Qaeda has its own websites whose content is not limited to video. The movement also uses them to publish texts laying out its ideology, stating its demands and describing its means of action. The target audience is broad. It includes both groups that would like to join the movement and individuals who would like to act on its behalf. Its online magazine, *Inspire*, offers DIY instructions for building explosive devices. IS does the same with its magazine *Dabiq*.

Digital as an Intelligence Tool

Middle Eastern states and Islamist movements from the region use Open-Source Intelligence (OSINT) to gather information. The most widely reported example is that of Hezbollah, which has created fake Facebook profiles to obtain sensitive information about Israel. Hamas has followed suit, posing as "friends" of IDF soldiers on Facebook to trick them into sharing sensitive information about their assignments and missions or downloading spyware onto their phones.[2]

[2] "Hamas uses fake Facebook friends to dupe 100 soldiers into downloading spyware," *The Times of Israel*, 3 July 2018.

For armies, as for non-state groups, social networks are a risk that they must learn to manage. But that is not all they are. They also offer considerable benefits in terms of gathering information. The example of Hezbollah's fake profiles illustrates how some organizations, by freely chatting with Facebook members, obtain intelligence and sometimes even recruit agents.

Middle Eastern states and Islamist movements from the region use Open-Source Intelligence (OSINT) to gather information

Social media are thus an efficient tool for monitoring populations. Israel also conducted extensive monitoring of the leaders of the social protests that took place in the country in 2011 and 2012. The Arab countries are doing the same with opposition leaders, and these methods have become widespread in states where the people have risen up against their leaders, such as Iran, Syria, Egypt or Bahrain. Nor have the opponents of these regimes been left behind. In Syria, they benefit from the help of hacker groups, both Syrian and foreign, who work to provide them with documentation. Additionally, the information posted online by some platforms, mainly to report on events on the ground, makes it possible to understand how the situation is evolving in a more complete, less fragmented way. This information is used by both foreign intelligence services and the people fighting the Syrian regular army, offering them a global view of all the fronts.

All of these techniques involve OSINT, which is, by definition, public and accessible to all. In contrast, the creation and spread of computer viruses is a more technical means of collecting information. There are numerous examples of the use of such malware by authorities from the region. In the United Arab Emirates, as well as in Syria, authorities have deployed viruses targeting different factions of the opposition.

However, there are more sophisticated and powerful computer viruses than those used in those two countries. Flame is a perfect example of this type of cyber tool. Discovered by chance in May 2012 by the company Kaspersky, Flame is one of the most sophisticated examples of malware known to date. In light of the proliferation of these kinds of cyber tools, the Middle East as a whole remains vulnerable, relying on mostly Western technological expertise and facing a Chinese economic breakthrough.

References

Gonzalez-Quijano, Yves. *Arabités numériques. Le printemps du web arabe*. Paris: Actes Sud/ Sindbad, 2012.

Tohme, W. et al. *Cyber Security in the Middle East*. Strategy &, Report, 2015.

World Economic Forum. *The Digital Arab World: Understanding and Embracing Regional Changes in the Fourth Industrial Revolution*, White Paper, January 2018.