Use of Surveillance Technology in MENA

ISSUE

REGIONAL

SUMMARY:

Governments across the Middle East and North Africa (MENA) have increasingly procured surveillance technology, often from technology firms based in North America and Europe, in the form of spyware, monitoring centers to intercept communication, and deep packet inspections that monitor and redirect internet flow. While some of these tools ostensibly could have legitimate use for law enforcement, it is unclear whether they have been in fact used for such purposes. States in the region have instead employed them against journalists, activists, and political dissidents, violating rights such as the those to life, privacy, and freedom of expression.

Information on which technology is used, by whom, and against which targets is still scarce, given that these spying operations are by their nature clouded in secrecy. Most of the data currently available comes from the work of journalists and civil society organizations.

POLITICAL CONTEXT:

Surveillance technology encompasses several different kinds of tools, though most of the prominent cases in the MENA region involve malicious software known as spyware.

Spyware can infect a smartphone and manipulate it to record phone calls, keystrokes, and videos. Saudi authorities, for example, allegedly used spyware to spy on those close to journalist Jamal Khashoggi, whom they then killed and dismembered in their consulate in Istanbul in 2018. The United Arab Emirates has also been accused of using a spyware of unknown origin, called Karma, to spy on its citizens. Some regional governments operate monitoring centers through which they intercept communication. Bahrain, for instance, used this technology to spy on the activist Abdul Ghani al-Khanjar, who was tortured while being shown his own intercepted messages; in 2011, Syria's President Bashar al-Assad was in the process of building a monitoring center with the help of Italian company AreaSPA

Spyware	Malicious software that can infect a device and allow the collection and exfiltration of data. Text, audio, video, and keystrokes are compromised. For example, Saudi Arabia has used Israeli spyware to spy on dissidents.
DPI	Deep Packet Inspection is used to monitor and redirect internet flow at a large scale. Governments can use this to block websites or to force users to access sites that are infected with spyware.
Social engineering	A technique through which users are led to perform certain actions such as clicking on a link. A government can hide spyware in an email promising information about human rights violations, for example, knowing that activists may be likely to click on them.
Phishing	A strategy in which users are fooled into revealing their passwords, allowing governments to access their private accounts. Attackers may pretend they are sharing a report on torture, for instance, and ask for the user to enter their account and password in order to read it.

(though the company later pulled out). Another frequently used technology is Deep Packet Inspection (DPI), employed to monitor vast internet data flows and block or redirect them; with the help of the company See Egypt, the Egyptian "sister company" to US-based Blue Coat Systems, Egypt has employed DPI to monitor online communications in the country. In the UAE, facial recognition technology has been employed on a mass scale as part of the "Oyoon" (Eyes) project, and was used to arrest 319 individuals in 2018.

Country	Technology	Case
Saudi Arabia	Pegasus, an Israeli spyware sold by NSO Group to the Saudi government	Saudi Authorities allegedly monitored private communication between the journalist Jamal Khashoggi and the dissident Omar Abdulaziz. Khashoggi was killed in 2018 inside a Saudi consulate in Turkey.
United Arab Emirates	Karma, a spyware of unknown origin used by the Emirati government in its clandestine surveillance project Raven	The Emirates spied on its citizens with the help of former NSA employees working on a project known as Raven.
Bahrain	Monitoring center sold by the German company Trovicor	Abdul Ghani al-Khanjar claims he was shown transcripts of his private communication while being tortured. Experts believe the information was obtained through surveillance.
Syria	Monitoring center sold by the Italian company Area SpA	Syria used this technology as part of its efforts to monitor and crack down on protests.
Egypt	Deep Packet Inspection provided by the Canadian company Sandvine	Egypt used DPI to monitor internet access and block at least 34,000 websites in a single shot in the context of wider repression of dissent.

Governments are able to employ covert surveillance technologies using means of varying sophistication, oftentimes through "social engineering," in which attackers manipulate their targets to perform certain actions. Bahraini activists, for instance, received messages disguised as reports on torture that were loaded with malicious software. In another example, the Citizen Lab found an infected Android app sharing news about a predominantly Shia region of Saudi Arabia. The technique of phishing, in which a false message is sent disguised as a legitimate request to encourage a recipient to enter a password, was used in Egypt in late 2016, when Egyptian NGOs received emails purportedly containing sensitive information—a technique that allows for surveillance without utilizing advanced technology.

Although governments may not admit their role in these cases and rights advocates have not documented the use of surveillance technology in court proceedings in any of the countries in the region, researchers point to a series of factors that indicate the coordination of official campaigns behind the attacks. The fact that spyware can be extremely costly is seen as an indication that non-state actors are often not likely to be able to acquire and use them—the technology behind the Israeli spyware Pegasus, used against Khashoggi, could cost from several hundred thousand dollars to a million dollars, for example. The nature of the targets is another clue; activists, journalists, political dissidents, and minorities are victims in patterns that mirror the physical threats that these groups face from the governments under which they live and may oppose.

Civil society organizations in the region monitor these violations and are engaged in advocacy around use

or export of surveillance technology. Beirut-based Social Media Exchange (SMEX), for instance, advocates against the use of DPI technology and asks for a stronger legal framework to protect personal data. Cairo-based Association for Freedom of Thought and Expression (AFTE) has criticized recently-passed Egyptian cybercrime legislation for its facilitation of mass surveillance. Given the lack of legal protection for citizens and the use of predominant use of surveillance in rights violations, international organizations also campaign against surveillance in the MENA region, including the Electronic Frontier Foundation, Access Now, and Privacy International. These organizations most recently expressed their concerns and engaged on these issues with stakeholders across different fields during the 2019 RightsCon Summit in Tunis.

LEGAL CONTEXT:

Many constitutions in the Middle East and North Africa, including the Egyptian Constitution and the Emirati Constitution include provisions protecting the right to privacy to various decrees, the right to due process, and the rights to freedom of assembly, expression, association, and belief. The Saudi Arabian Constitution, for example, protects the right to privacy, although it states that correspondences "may not be confiscated, delayed or read, and telephones may not be tapped except as laid down in the law." By abusing mass surveillance technologies to monitor the speech and activities of their own citizens, states are violating their domestic legal obligations to respect the right to privacy, but also furthering restrictions on the ability of citizens to exercise their constitutionally-guaranteed rights and in effect, violating rights including the rights to freedom of association and expression. Abuse of surveillance technology also implicates international law, as states have a duty to protect and respect the aforementioned rights and freedoms, as well as the right to life, recognized in treaties including the International Covenant on Civil and Political Rights.

In addition to the aforementioned obligations, the United Nations Guiding Principles on Business and Human Rights lays out stipulations for both states and business to protect human rights, including the right to privacy. Pillar II of the UN Guiding Principles, for example, sets out duties of business, including undertaking due diligence to ensure their products will not be used in nefarious ways.

The United Nations High Commissioner for Human Rights published a report in September 2018 which discusses challenges to the right to privacy in the digital age and states that a person's right to privacy can be restricted only if the action furthers a legitimate government aim, is based in domestic law, and is necessary and proportional. Under these parameters, using mass technology to monitor political opponents or journalists, for example, violates international law. The United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, published a report in May 2019 discussing the challenges to the rights to freedom of peaceful assembly and of association in the digital age. The report discusses how surveillance technologies are used to monitor minorities, LGBTQ individuals, human rights defenders, political opponents, and activists, and how vague domestic surveillance laws allow governments to continue this practice. The findings of that report were reinforced by the Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, which highlighted how targeted surveillance regimes are "linked to detention, torture, and extrajudicial killings." He called for a moratorium on the export of these technologies until a more strict, transparent, and uniform export regime can be set up that puts human rights at the forefront.

TREND ANALYSIS:

MENA governments continue to purchase, weaponize, and employ surveillance technology, regardless of the fact that abuses related to use have been credibly documented. Beyond increasing efforts at naming and

shaming, authorities have largely not been held accountable for violating their domestic and international legal obligations.

The killing of the Saudi journalist Jamal Khashoggi is a telling example of this trend. While several reports tied Khashoggi's killing to the Israeli spyware Pegasus, including a U.N. document, there is no sign of Saudi Arabia slowing down or ceasing its surveillance activities, and there are no signs of foreign companies moving towards more transparency in their sales. Media attention to the case, however, has led to international debate and mobilization among civil society. There are indications of a nascent trend of investors refusing to fund companies providing surveillance technology, given the bad publicity generated by reports on violations, an indication of the impact that investigations done by the press and civil rights organizations can have. Some reports also indicate that computer science students are increasingly losing interest in working for big tech companies in the United States, partially as a result of the perception that those firms contribute to human rights violations.

IMPLICATIONS:

Most citizens in MENA countries already live in repressive environments in which spaces for dissent are limited and where governments act and issue legislation to curtail rights like freedom of the press, expression, association, and assembly. While the use of these tools is admissable for law enforcement purposes when states respect the principles of necessity and proportionality as described above, application thus far has failed to take these international legal principles into account. Additionally, some of these tools, like Deep Packet Inspection, are inherently indiscriminate and so cannot not comply with the principle of proportionality.

The use of surveillance technologies to monitor and repress in virtual spaces—monitoring private communications, for example—leads to an even more stifling environment, in which people are increasingly cautious of expressing discontent or opposition to government policies. In some instances, aware of the fact that the government might spy on emails or even phone messages, sources and whistleblowers avoid talking to the press. Without a free press and free expression, citizens face insurmountable challenges to hold governments and officials accountable. This also makes citizens hesitant to take part in the political process. Moreover, some of these tools are extremely costly and depend on foreign companies for transfer, maintenance, and training. MENA states, therefore, may expend much-needed resources that could otherwise be invested in critical sectors such as healthcare and education. Thus, although states claim they monitor citizens to guarantee their security, the massive use of surveillance technology in an authoritarian context may promote instability instead

TIMEP COVERAGE:

- TIMEP Brief - Export of Surveillance Technologies to MENA Countries
- TIMEP Brief - Press Freedom in Egypt