EuroMeSCo policy brief

No. 99
8 October 2019

THREE STEPS IN ENSURING Digital Security of Egyptian Activists Abroad

*Žilvinas Švedkauskas**

Throughout recent years under Abdel Fattah al-Sisi, Egyptian activists have faced numerous arrests for alleged online offences, ranging from blasphemy to inciting protests or opposing the government. In August 2018, the final clampdown on online media was enacted with a cybercrime law, signed into power by the President, imposing life sentences without the possibility of parole for crimes presumably aiming to disrupt public order, jeopardise citizen safety or harm national unity. Moreover, article 2 of the legislation requires internet service providers to retain users' personal information and details of their online activity, which must be released to security bodies upon request (al-Abd, 2018). In other words, the Egyptian government under al-Sisi has successfully tamed digital communication technologies. The tight grip of the government on the digital sphere has turned the 2011 "generation protest", empowered at a time by social media revolution, into, what today many call, "generation jail" (Amnesty International, 2015).

After shutting down venues for criticism at home, the military regime headed by al-Sisi has turned to curbing any opposition arising from Egyptian diaspora abroad. To this end, it uses the same techniques for controlling the digital sphere, successfully tried out before. This policy brief aims to draw the attention of Western policy-makers and pinpoint how contemporary autocrats are able to transcend national borders to suppress and harass dissidents even under asylum of liberal Western democracies. Using the case of Egypt as an illustration, it starts by unpacking how European high-tech companies have already helped to broaden the "authoritarian toolkit" of the Egyptian regime, empowering it to monitor and suppress opposition figures at home. Subsequently, the policy brief reviews empirical fingerprints left by the application of similar techniques by the Egyptian government pursuing its critics in the West. Finally, the brief concludes with three recommendations on how protection of diaspora activists could work against digital

*PhD candidate, Eberhard-Karls-Universität Tübingen

IEMed.

transnational authoritarian threats and how respective practices and laws could be successfully integrated into broader frameworks of European cyber security.

"With a little help from my friends"

With private European tech companies on the supply side, for the past few years the Egyptian government has heavily invested in online-monitoring software for tracking activities of political dissidents. As indicated by leaked documents, the Technical Research Department at the Egyptian General Intelligence Service (GIS), in charge of providing both domestic and foreign intelligence, and accountable only to the President himself, has been at the centre of an authoritarian tech upgrade (Privacy International, 2016).

Nokia Siemens Networks, a Helsinki-based joint venture of German Siemens AG and Finnish Nokia, has already been under fire since 2009, when it was revealed that it had sold monitoring centre equipment to the Iranian government, which allegedly used it to crack down on protesters. In a similar vein, Bahraini government authorities were reported to have arrested opponents who were then tortured, while being read transcripts of their text messages and phone conversations, obtained with Nokia Siemens Networks tech solutions ("European Technology Company Accused of Enabling Torture", 2011). Leaked documents about Nokia Siemens Networks activities in Egypt reveal that it had sold an x25 network[1] to the Egyptian GIS, which allows dial-up internet access, enabling access to the internet even if the main national internet infrastructure is shut down. In addition, Nokia Siemens Networks has also sold an interception management system and a monitoring centre for fixed and mobile networks, which offers mass surveillance capabilities and enables the Egyptian government to intercept phone communications (Privacy International, 2016).

Two other private European companies, Gamma International and Hacking Team, repeatedly exposed for selling highly intrusive spyware to oppressive regimes, have also helped the Egyptian government to boost its surveillance capacities by providing intrusion malware. Hacking Team's remote control system grants the Egyptian secret services complete control of the computers of its targets. The Egyptian government is able to access any content stored on computers of opposition activists, monitor their online actions in real time, log keystrokes and passwords, capture screenshots and activate webcams to its liking. Judging from leaked documents, the Egyptian secret services benefit from a sizeable budget allocated for boosting the regime's monitoring capabilities. For instance, leaked documents show that Hacking Team expected to earn 1 million euros from a deal on intrusive surveillance technologies (Toor, 2016).

[1] X.25 is a protocol suite for converting and delivering data in a given network (see Mitchell, 2019).

As a result of importing Western-manufactured software and hardware, the Egyptian regime now possesses wide-ranging surveillance capabilities, including a communication monitoring centre, interception management systems and highly intrusive spyware.

Egyptian Secret Services Gone Phishin'

Recent large-scale phishing campaigns against Egyptian civil society have exemplified the scope of al-Sisi's "authoritarian toolkit" and interdependencies between the regime's online and offline tactics. In 2016-17, a number of non-governmental organizations (NGOs) and civil society activists were targeted by the so-called Nile Phish. Nearly all targeted activists were at the same time implicated in Case 173, brought against NGOs by the Egyptian government over issues of foreign funding (TIMEP, 2019). The Nile Phish demonstrated sophistication and awareness of the legal persecution facing its targets offline. For instance, within hours after a prominent Egyptian lawyer, Azza Soliman, was arrested at her home on 7 December 2016, several of her colleagues received emails with fake Dropbox shares of Soliman's arrest warrant (Scott-Railton et al., 2017). Moreover, using the wording of an original announcement, another widely distributed phishing message appeared to come from the Nadeem Center for Rehabilitation of Victims of Violence and invited activists to participate in a non-existent panel discussing Egypt's draft NGO law. Both of these attacks were designed with a view to gaining access to email and cloud storage accounts of its victims (Scott-Railton et al., 2017).

Another wave of digital attacks has followed in 2019, parallel to constitutional amendments, enabling al-Sisi to stay in power until 2030, though a different strategy for stealing personal data has been used this time – "OAuth Phish". It abuses a legitimate feature of many online service providers, including Google, that allows third-party applications to gain direct access to an account. For example, a legitimate external calendar application might request access to a user's email account in order to automatically identify and add upcoming events or flight reservations. The total number of targeted individuals in this phishing cycle is several hundred (Amnesty International, 2019).

Transnational Authoritarian Aspirations

In the backdrop of the incumbent power grab and intensifying crackdown on Egyptian civil society and political activists, a considerable number of Egyptians have chosen to exit the country. Many have left for Western countries, offering freedom of expression, movement and space to coalesce into a tangible political network with capacities to mobilise and make its voice heard (Ali, 2019a). Nonetheless, digital threats faced by Egyptian activists abroad remain somewhat undiscussed, though the Egyptian government has attentively followed this relocation, looking to make the reach of "al-Sisi's hand" effective beyond the geographical borders of Egypt.

In 2018, the Egyptian Ministry of Immigration announced its willingness to find and record statistics of the Egyptian expatriate community under the Egyptian Expatriate Database Project (Dunne & Hamzawy, 2019). The Egyptian Minister of Foreign Affairs Sameh Shukry, for his part, has openly stated that Egyptian embassies across the world are seeking to counter attempts to undermine the state by any means possible ("Egypt Lawmaker Mulls 'Ban'", 2018). In addition, parliamentary initiatives aiming to toughen existing laws criminalising incitement against the state from abroad and banning foreign-based dissidents from returning to the country have followed ("Egypt Admits Embassies Abroad Play Role in Crackdown", 2019). Finally, in a recent meeting with the Egyptian community in Toronto, Egypt's Minister of Immigration and Expatriates' Affairs Nabila Makram threatened to "slice" the throats of those who criticise the current administration, openly referring to Egyptian activists abroad ("Egyptian Immigration Minister Threatens to 'Slice' Critics in Canada", 2019).

In such a context, the application of the Egyptian government's online surveillance capabilities to track the activities of Egyptian activists in exile and the use of digital technology for their harassment is highly likely. Like other contemporary authoritarian regimes, Egypt's military government understands the importance of controlling online venues for expression very well and has obviously learned from the mistakes made by governments toppled by the Arab Spring and the colour revolutions around the world. Being able to monitor activists' profiles at home and abroad and possessing the needed resources, these regimes flood social media platforms like Facebook with legal requests, gather outsourced troll armies to report, harass or simply hack activists online. As a result, it has been increasingly difficult for Egyptians abroad to make their voice heard, even in liberal democratic surroundings.

Empirical Fingerprints of Digital Authoritarianism

Sawsan Gharib, spokesperson for Egypt's April 6 Youth Movement, influential in the ouster of Hosni Mubarak in 2011, currently resides in the United States (US) and has nearly 7,000 followers on social media. She has been reported to have her Facebook page shut down numerous times during the past years. She has tried to create new pages, but they have also been banned, allegedly because of complaints from pro-Sisi digital agents (Akkad, 2018). Another Egyptian diaspora activist, Bahgat Sabr, based in New York and known for his popular Facebook broadcast on Egyptian politics, has also been targeted by online trolls who frequently report on his account. Moreover, Sabr's live streams have been cut off repeatedly without a warning. Ahmed Abdel-Basit Mohamed and Amr Boktar are among other prominent Egyptian activists living in the US, who had their Facebook profiles suspended in a similar fashion (Akkad, 2018).

Similarly to activists harassed by the Nile and OAuth Phish in Egypt, Mona Eltahawy, an Egyptian born American columnist, was also targeted by cyber attacks in 2017. With a

malicious email sent to Eltahawy, she was attacked by the same password-stealing technique used to try to compromise staff of Egyptian human rights organisations with connections to a prominent Egyptian lawyer, Mrs. Azza Soliman. Just like in the case described before, Mona Eltahawy received an email labelled “an important document about Azza Soliman,” followed by additional suspicious emails and activities on her account she did not recognise in the course of the next days (“Egypt Targets American-Egyptian Activist With Cyber Spies”, 2017).

On the European side, Spain-based Egyptian actor Amr Waked has been actively critical of the Egyptian regime’s abuses. For instance, through his Twitter account he has openly rejected the Egyptian Parliament’s decision to approve a controversial land deal with Saudi Arabia, handing over two Red Sea islands, Tiran and Sanafir, previously under Egyptian control, and criticised recent constitutional amendments, consolidating al-Sisi’s authoritarian rule and allowing him to stay in office until 2030. In response to his online activism, back in Egypt, military courts had sentenced him to eight years in prison for “spreading fake news” and “slandering state institutions” (Ali, 2019b). In March 2019, Waked and a prominent Egyptian film director, Khaled Abol Naga, joined over 100 Egyptians from around the world for meetings with members of the US Congress and State Department during the “Egypt Advocacy Day”. In response, the Egyptian authorities have started a systematic defamation campaign against Waked and Naga via state-owned media (Human Rights Watch, 2019). This also has sparked a polarised debate online, with pro-government supporters and possibly trolls branding Amr Waked and Khaled Abol Naga as traitors and demanding for their citizenships to be stripped off.

Finally, as a telling example of the interplay between online and offline threats faced by the Egyptian diaspora activists, in May 2017, Egyptian secret services successfully tracked down and infiltrated a Euromed Rights group meeting in Rome, hosting prominent Egyptian activists working in exile or active abroad: Bahey eldin Hassan (Director of the Cairo Institute for Human Rights Studies), human rights lawyer Khaled Ali, political scientist Amr Hamzawy, Mohamed Zarea (President of the Arab Penal Reform Organization), Ahmed Samih (Executive Director of Andalus Institute for Tolerance and Antiviolence Studies), Nancy Okail (Executive Director of the Tahrir Institute for Middle East Policy), and Moataz al-Fegiery (Middle East and North Africa [MENA] Protection Coordinator at Front Line Defenders). The material gathered by the Egyptian secret service in Rome was later used to incite a smear campaign against these activists online and offline. For instance, back in Egypt, Moustafa Bakry, a public figure and a vocal supporter of the President in the Parliament, stated on his TV show that the Egyptian security bodies should kidnap Egyptian human rights defenders from Europe and bring them back to Egypt “in coffins,” referring to similar operations under

previous Egyptian presidents ("Haqaq Wel Asrar ma Mustafa Bakri", 2017).[2] In March 2018, the same TV host called on the Egyptian authorities to follow the example of Russian secret services and deal with eldin Hassan in a similar fashion as Russians had done with Sergey Skripal and his daughter in the United Kingdom (UK) (Euromed Rights, 2019).

The meeting in Rome, which sparked a wave of threats against Egyptian activists abroad, was a part of Euromed Rights internal work, and therefore had not been publicised beyond the participants themselves (Italian NGOs Joint Statement, 2017). Judging from this, it is highly likely that the infiltration resulted from digital hacking or activists leaving "digital traces" (information on travel, participation in conferences, friends and collaborators online), which have already been reported to be of high relevance in other cases of extraterritorial authoritarian harassment (see, for instance, Michaelsen, 2019).

Recommendations

Reflecting on the above-described aspirations of the Egyptian regime to track and crackdown on dissenting voices abroad and feasible digital risks facing members of the Egyptian diaspora, Western governments should consider three main steps in ensuring digital security of Egyptian activists in exile:

- First, considering that digital surveillance may be targeting dissidents at home, as well as activists under political asylum in Europe or the US, strict vetting procedures for digital surveillance software and hardware exported to third countries should be implemented. Exports by companies, such as Nokia Siemens Networks, Gamma International and Hacking Team, should be effectively banned to governments deemed non-compliant with international human rights standards. This would complement the recent European Parliament resolution on Egypt, notably the situation of human rights defenders (2018/2968[RSP]), which calls on the Member States to halt exports of surveillance technology and security equipment to Egypt that can facilitate attacks on human rights defenders and civil society activists, including on social media.

- Second, Western governments should initiate a dialogue with social media platforms to explore ways to recognise and counter troll armies used by authoritarian regimes to monitor, harass and flood social media content moderators with negative reports on activists online. To this end, Facebook and Twitter need to implement more thorough procedures of content moderation and install checks against authoritarian exploitation of their policies for censoring critical voices under asylum. In Western countries, installing checks could be done by governments cooperating with social networks,

[2] For background on kidnappings of Egyptian opposition activists abroad, see, for instance, the case of Abu Omar (European Court of Human Rights, 2016).

using the existing track record to pinpoint activists facing the highest risks of being attacked online and assisting social media platforms in examining negative reports about diaspora activism, as well as working together to determine sources of online harassment or hacking. This would make it more challenging for autocrats to take advantage of the digital sphere and step over national boundaries to intimidate their opponents abroad.

- Third, cyber responses to digital transnational authoritarian threats should be integrated within broader policies of the European Union (EU) and its member states, targeting MENA dissidents in exile: implementing digital security training for political activists and supporting collaborations between technologists, researchers, activists and governments, paving the way for real digital resilience against transnational digital threats. Allowances for this purpose could be successfully integrated within the new European Cybersecurity Competence Centre, expected to take a leading role in cyber security within the next multiannual financial framework of the EU (European Commission, 2018).

References

Amnesty International. (2015, June 30). *Egypt: Generation Jail: Egypt's youth go from protest to prison.* Retrieved from https://www.amnesty.org/en/documents/mde12/1853/2015/en/

Amnesty International. (2019, March 6). *Phishing attacks using third-party applications against Egyptian civil society organizations.* Retrieved from https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

Akkad, D. (2018, January 25). Revealed: Seven years later, how Facebook shuts down free speech in Egypt. Retrieved from https://www.middleeasteye.net/news/revealed-seven-years-later-how-facebook-shuts-down-free-speech-egypt

al-Abd, R. (2018, June 5). Parliament passes cybercrime law regulating web content and ISP surveillance. *Mada Masr.* Retrieved from https://madamasr.com/en/2018/06/05/news/u/parliament-passes-cybercrime-law-regulating-web-content-and-isp-surveillance/

Ali, A. (2019a, April 25). On the need to shape the Arab exile body in Berlin. Retrieved from https://amroali.com/2019/01/on-the-need-to-shape-the-arab-exile-body-in-berlin/

Ali, R. (2019b, March 5). 'Syriana' actor says he was threatened with military prison in Egypt over critical views. Retrieved from https://abcnews.go.com/International/syriana-actor-threatened-military-prison-egypt-critical-views/story?id=61477578

Dunne, M., & Hamzawy, A. (2019). Egypt's political exiles: Going anywhere but home. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2019/03/29/egypt-s-political-exiles-going-anywhere-but-home-pub-78728

Egypt targets American-Egyptian activist with cyber spies. (2017, February 14). *Associated Press.* Retrieved from https://www.mintpressnews.com/egypt-targets-american-egyptian-activist-with-cyber-spies-2/224900/

Egyptian immigration minister threatens to 'slice' critics in Canada. (2019, July 24). *Daily Sabah.* Retrieved from https://www.dailysabah.com/mideast/2019/07/24/egyptian-immigration-minister-threatens-to-slice-critics-in-canada

Egypt lawmaker mulls 'ban' on return of foreign-based dissidents. (2018, May 21). *The New Arab.* Retrieved from https://www.alaraby.co.uk/english/news/2018/5/21/egypt-lawmaker-mulls-ban-on-return-of-foreign-based-dissidents

Egypt admits embassies abroad play role in crackdown on dissent against regime. (2019, March 11). *The New Arab.* Retrieved from https://www.alaraby.co.uk/english/ news/2019/ 3/11/egypt-admits-embassies-abroad-part-of-crackdown-on-dissent

Euromed Rights. (2018, April 18). Death threats against CIHRS director, Bahey el-Din Hassan. Retrieved from https://euromedrights.org/publication/death-threats-against-cihrs-director-bahey-el-din-hassan/

European Court of Human Rights. (2016, February 23). The CIA's abduction and extrajudicial transfer to Egypt of the imam Abu Omar infringed the applicants' rights under the Convention [Press release].

European Commission. (2018, September 19). Proposal for a European Cybersecurity Competence Network and Centre. Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

European Parliament. (2018, December 12). Resolution on Egypt, notably the situation of human rights defenders. Retrieved from http://www.europarl.europa.eu/doceo/document/RC-8-2018-0568_EN.html?redirect

European technology company accused of enabling torture. (2011, August 24). *Deutsche Welle.* Retrieved from https://p.dw.com/p/12MIn

Haqaq Wel Asrar ma Mustafa Bakri (Facts and secrets with Moustafa Bakry). (2017, May 25). *Sada Elbalad.* Retrieved from https://www.youtube.com/watch?v=eirJclgosPs

Human Rights Watch. (2019, April 2). Egypt: Reprisal against award-winning actors Amr Waked and Khaled Abol Naga for speaking out against repression. Retrieved from https://www.hrw.org/news/2019/04/02/egypt-reprisal-against-award-winning-actors-amr-waked-and-khaled-abol-naga-speaking

Italian NGOs Joint Statement. (2017). *Egyptian activists and Human Rights defenders stalked and spied on in Rome, slandered in Cairo.* Retrieved from https://d21zrvtkxtd6ae.cloudfront.net/public/uploads/2017/05/24122108/Italian-NGOs-joint-statement-May-23-English.pdf

Michaelsen, M. (2019, April). *Responding to transnational repression: Authoritarian threats and diaspora activists from Egypt, Syria and Iran.* ECPR Joint Sessions, Mons, Belgium.

Mitchell, B. (2019, July 9). A Guide to X.25 in computer networking. Retrieved from https://www.lifewire.com/x-25-816286

Privacy International. (2016). *The president's men?: Inside the Technical Research Department, the secret player in Egypt's intelligence infrastructure.* Retrieved from https://privacyinternational.org/sites/default/files/2018-02/egypt_reportEnglish_0.pdf

Scott-Railton, J., Marczak, B., Raoof, R., & Maynier, E. (2017, February 2). *Nile Phish: Large-scale phishing campaign targeting Egyptian civil society.* Retrieved from https://citizenlab.ca/2017/02/nilephish-report/

TIMEP. (2019, February 28). *Case 173: Egypt's foreign funding case.* Retrieved from https://timep.org/reports-briefings/timep-brief-case-173-egypts-foreign-funding-case/

Toor, A. (2016, February 24). European companies sold powerful surveillance technology to Egypt, report says. Retrieved from https://www.theverge.com/2016/2/24/11104524/egypt-surveillance-nokia-finfisher-hacking-team-spyware

IEMed.

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Union or the European Institute of the Mediterranean