



# Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa

## Citation

Horak, Gail. 2023. Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa. Master's thesis, Harvard University Division of Continuing Education.

## Link

<https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374983>

## Terms of use

This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material (LAA), as set forth at

<https://harvardwiki.atlassian.net/wiki/external/NGY5NDE4ZjgzNTc5NDQzMGIzZWZhMGFIOWI2M2EwYTg>

## Accessibility

<https://accessibility.huit.harvard.edu/digital-accessibility-policy>

## Share Your Story

The Harvard community has made this article openly available.  
Please share how this access benefits you. [Submit a story](#)

Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa

Gail Horak

A Thesis in the Field of International Relations  
for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

May 2023



## Abstract

Much attention has been devoted in recent years to the dangers of spyware such as Pegasus, which its creators said would make the world safer by allowing government agencies to monitor and thwart terrorism and criminal activity. However, before the advent of spyware, governments used traditional tools to surveil, and in some instances, to repress. Thus, spyware in many countries continues past practices of stifling dissent in order to preserve regime stability. Spyware isn't the only digital tool used to silence opposition voices; it is one of several tools in the authoritarian ruler's digital repression toolkit. This thesis seeks to understand whether spyware like Pegasus has made human rights worse since it became commercially available in the early 2010s, and as it is just one of the many tools used to digitally repress, if it poses a unique threat. This research also seeks to understand whether different variations of autocracies, which have a high correlation with using repression to maintain power, use spyware differently. To examine these questions, this research will focus on the Middle East and North Africa (MENA) region, where most systems of governance are either electoral autocracies or closed autocracies. The Arab uprisings that began in late 2010 will serve as a reference point as they signify a period when most governments in the MENA region were tamping down protests but had not yet harnessed the power of the internet.

## Frontispiece



Figure 1. The power of the smartphone

*A Palestinian woman and member of the Israeli security forces take pictures of each other on a street in Jerusalem on December 16, 2017, amid demonstrations over the U.S. President's decision to name Jerusalem the capital of Israel. Ahmad Gharabli / AFP / Getty*

## Author's Biographical Sketch

Gail Horak is a foreign affairs and technology professional focused on the nexus of these sectors. As both a civil servant and Foreign Service Officer with the U.S. Department of State for over 15 years, Gail specialized in political affairs in the Middle East and North Africa. She served at the U.S. Embassies in Romania, Iraq, Kuwait, as a Director for Iraq at the National Security Council, and as a Political Advisor at the U.S. Mission to the United Nations. In this last role, she was the U.S. government's primary negotiator at the UN Security Council on issues involving Syria, Israel-Palestine, Yemen, and Western Sahara during the Arab uprisings.

Gail currently works as a senior manager at YouTube in Trust and Safety where she leads a team charged with preparing for and reducing risks to users to maintain a safe platform experience.

Gail lives with her husband and daughter in New York City.

## Dedication

This thesis is dedicated to my family, Matt and Olivia, whose support made this long-held goal a reality.

## Table of Contents

|                                                              |     |
|--------------------------------------------------------------|-----|
| Frontispiece.....                                            | iv  |
| Author's Biographical Sketch.....                            | v   |
| Dedication.....                                              | vi  |
| List of Tables .....                                         | xi  |
| List of Figures .....                                        | xii |
| Part One: .....                                              | 1   |
| Chapter I. Introduction.....                                 | 1   |
| Key Findings.....                                            | 6   |
| Deterioration of human rights since spyware introduced ..... | 6   |
| Spyware poses a unique threat.....                           | 7   |
| Governance model does not always predict use of spyware..... | 7   |
| Roadmap .....                                                | 9   |
| Chapter II. Literature Review .....                          | 10  |
| On Repression and Systems of Political Governance.....       | 10  |
| On Digital Technology and Digital Repression.....            | 12  |
| On Spyware.....                                              | 16  |
| On the Arab Uprisings .....                                  | 19  |
| On Digital Technology and Human Rights .....                 | 19  |
| Rationale for Research Questions.....                        | 20  |
| Chapter III. Research Methods .....                          | 22  |

|                                                             |    |
|-------------------------------------------------------------|----|
| Definitions.....                                            | 22 |
| Interviews.....                                             | 25 |
| Case Studies .....                                          | 25 |
| Results.....                                                | 27 |
| Limitations .....                                           | 28 |
| Part Two:.....                                              | 30 |
| Chapter IV. Digital Repression and the Rise of Spyware..... | 30 |
| Evolving Forms of Digital Repression .....                  | 30 |
| Internet and ICT Shutdowns .....                            | 31 |
| Online Censorship.....                                      | 32 |
| Targeted Persecution of Online Users .....                  | 33 |
| Social Manipulation and Disinformation.....                 | 33 |
| Surveillance.....                                           | 34 |
| Passive Surveillance.....                                   | 34 |
| AI and Big Data Surveillance .....                          | 36 |
| Targeted Surveillance .....                                 | 38 |
| Spyware.....                                                | 39 |
| Who makes it .....                                          | 40 |
| NSO Group .....                                             | 40 |
| Other spyware manufacturers .....                           | 43 |
| Chapter V. Legitimacy of Spyware .....                      | 48 |
| Legitimacy and human rights.....                            | 49 |
| Human rights in the MENA region.....                        | 51 |

|                                             |     |
|---------------------------------------------|-----|
| Transnational questions of legitimacy ..... | 53  |
| Part Three:.....                            | 57  |
| Chapter VI. MENA Case Studies .....         | 57  |
| Chapter VII. Egypt.....                     | 58  |
| Ayman Nour.....                             | 62  |
| Mozn Hassan.....                            | 64  |
| Hassan Nafaa .....                          | 68  |
| Khaled Dawoud .....                         | 69  |
| Shady Al-Ghazaly Harb.....                  | 71  |
| Chapter VIII. Lebanon .....                 | 73  |
| Lama Fakih .....                            | 77  |
| Chapter IX. Morocco .....                   | 81  |
| Aminatou Haidar.....                        | 85  |
| Fouad Abdelmoumni .....                     | 87  |
| Hisham Almiraat.....                        | 88  |
| Omar Radi.....                              | 89  |
| Maati Monjib .....                          | 91  |
| Abdessadak El Bouchattaoui .....            | 91  |
| Chapter X. Saudi Arabia.....                | 93  |
| Manal al-Sharif .....                       | 100 |
| Saad al-Jabri.....                          | 102 |
| Omar Abdulaziz .....                        | 106 |
| Ghanem al-Masarir .....                     | 108 |

|                                             |     |
|---------------------------------------------|-----|
| Ghada Oueiss .....                          | 109 |
| Ben Hubbard .....                           | 111 |
| Chapter XI. United Arab Emirates.....       | 113 |
| Ahmed Mansour.....                          | 122 |
| Latifa al Makhtoum.....                     | 124 |
| Hanan Elatr .....                           | 127 |
| Rori Donaghy.....                           | 128 |
| Alaa al-Siddiq .....                        | 129 |
| Chapter XII. Results.....                   | 132 |
| Spyware poses a unique risk .....           | 135 |
| Governance systems and use of spyware ..... | 137 |
| Chapter XIII. Conclusion.....               | 140 |
| Mitigating the risks of spyware.....        | 140 |
| Governments .....                           | 141 |
| Multilateral efforts .....                  | 144 |
| Individual risk mitigation.....             | 144 |
| Outstanding questions .....                 | 145 |
| References.....                             | 148 |

## List of Tables

|          |                                                                        |     |
|----------|------------------------------------------------------------------------|-----|
| Table 1. | Forms of Digital Repression .....                                      | 13  |
| Table 2. | MENA Region Spyware Inventory .....                                    | 45  |
| Table 3. | Egypt's Freedom on the Net and Digital Repression Index Scores .....   | 60  |
| Table 4. | Lebanon's Freedom on the Net and Digital Repression Index Scores ..... | 74  |
| Table 5. | Morocco's Freedom on the Net and Digital Repression Index Scores ..... | 83  |
| Table 6. | Saudi's Freedom on the Net and Digital Repression Index Scores .....   | 95  |
| Table 7. | The UAE's Freedom on the Net and Digital Repression Index Scores ...   | 116 |

## List of Figures

|           |                                                                  |     |
|-----------|------------------------------------------------------------------|-----|
| Figure 1. | The power of the smartphone .....                                | iv  |
| Figure 2. | What Pegasus Can Extract .....                                   | 6   |
| Figure 3. | Types of Autocratization.....                                    | 12  |
| Figure 4. | Digital Repression Index Comparison of 2011 and 2021 levels..... | 133 |
| Figure 5. | Freedom on the Net for Select MENA Countries .....               | 134 |

Part One:

Chapter I.

Introduction

*It is often said that the most important thing that a house burglar steals  
is the peace of mind of the householder. The same must surely be true  
of phone hacking.*

– The Right Honorable Sir Andrew  
McFarlane, President of the Family  
Division, UK High Court of Justice<sup>1</sup>

Karma. Predator. Reign. Sherlock. RCS. FinSpy. Dark Caracal. Pegasus. These names represent some of the most powerful spyware used to target persons of interest by governments around the world, including in the Middle East and North Africa (MENA). Some of these products are sold exclusively to governments and government agencies with contractual stipulations that limit the spyware's use to fighting terrorism and crime. However, as seen in countless testimonies, leaks, and human rights and media reports, such spyware has been misused for targeting activists, political dissidents, lawyers, human rights defenders, journalists, and even in one instance, a leader's own family members.

---

<sup>1</sup> Dan Sabbagh, Dan Sabbagh Defence, and security editor, "'The Walls Are Closing in on Me': The Hacking of Princess Haya," *The Guardian*, October 6, 2021, sec. World news, <https://www.theguardian.com/world/2021/oct/06/walls-closing-in-story-behind-princess-haya-hacking-ordeal>.

While there are many kinds of spyware that rely on unique and evolving technical exploits to gain unauthorized access to a computer device, the result is the same: the spyware burrows into targeted computer devices, including smartphones, to share a target's most private information. This can include a target's location, emails, contacts, photos, and voice and text messages, even the ones supposedly protected by end-to-end encrypted apps. Some spyware can also open a smartphone's camera and microphone and take photos, videos, and recordings. Governments in the MENA region have used the extracted data to defame individuals with smear campaigns, to arbitrarily detain for extended periods of time, and in the most extreme cases, to hunt down dissidents with the intent to permanently silence them.

This technology was not always available to all countries. In the 2000s, only a small number of technologically advanced countries had the financial capital and expertise to build spyware capabilities in-house. However, since the early 2010s, private companies have been developing commercial spyware for sale, and governments seeking to bolster their surveillance capabilities have been paying top dollar to purchase it. In the MENA region, poor and wealthy countries alike are among the spyware industry's many customers.

Most governments in the MENA region were slow to embrace digital technology. When the Arab uprisings began in late 2010, individuals with access to the internet, predominantly via smartphones, were able to share previously banned or censored information with greater ease. Using smartphones, citizens were able to organize protests from the safety of their homes, document violence against protestors, and share how

government forces had reacted.<sup>2</sup> The images that they captured were often shared via social media, which in turn were publicized more widely by private satellite television stations. People consuming this information joined protests for a variety of personal and social reasons. This cycle propagated new protest waves throughout the region.<sup>3</sup>

Governments in the region scrambled to stop the threat to regime stability caused by the spread of information over the internet. They fought to keep up with their citizens' quick adoption of this rapidly evolving technology, and some chose to shut down the internet and mobile phone networks—most infamously in Egypt, but also in Syria<sup>4</sup> and Libya<sup>5</sup>—to attempt to control the narrative and stop protest mobilization. As history shows, these efforts had mixed results.

Ultimately, MENA governments faced a choice: to severely limit the use of the internet in their countries or to find a way to safely coexist with it.<sup>6</sup> Weighing the risks, most governments prioritized the development of capabilities beyond internet shutdowns and throttling,<sup>7</sup> which intentionally slows data transmission, to embrace spyware and other forms of “digital repression.” Digital repression, as defined by former U.S. government official and author Steven Feldstein, is the use of information and communications technology in parallel to “...surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state.” Digital

---

<sup>2</sup> Linda Herrera, “Citizenship under Surveillance: Dealing with the Digital Age,” *International Journal of Middle East Studies* 47, no. 2 (2015): 354–56, <https://doi.org/10.1017/S0020743815000100>.

<sup>3</sup> Inmaculada Szmolka, *Political Change in the Middle East and North Africa: After the Arab Spring* (Edinburgh University Press, 2018).

<sup>4</sup> Sanja Kelly et al., “Freedom on the Net 2013, A Global Assessment of Internet and Digital Media” (Freedom House, October 3, 2013), 7.

<sup>5</sup> Sanja Kelly, Sarah Cook, and Mai Truong, “Freedom on the Net 2012, A Global Assessment of Internet and Digital Media” (Freedom House, September 24, 2012), 3.

<sup>6</sup> Herrera, “Citizenship under Surveillance.”

<sup>7</sup> Sanja Kelly et al., “Freedom on the Net 2013, A Global Assessment of Internet and Digital Media,” 7.

repression can be conceptualized into the following categories: surveillance (including targeted surveillance such as spyware and data-extraction technology), online censorship, social manipulation and disinformation, internet shutdowns, and the targeted persecution of online users.<sup>8</sup> Spyware hacks into a targeted device remotely, while data-extraction technology is used to access and extract information from a device in an operator's physical possession. The latter has reportedly been used by government officials at border crossings and ports of entry globally, including by Customs and Border Protection in the United States.<sup>9</sup>

In 2021, Freedom House asserted that authorities in at least 45 of the 70 countries surveyed in its Freedom on the Net report likely have access to spyware or data-extraction technology.<sup>10</sup> This figure includes governments in the MENA region, some of which have dubious human rights records that call into question whether the technology is being used for legitimate reasons.<sup>11</sup>

The most recognizable name in the spyware industry is Pegasus, made by Israel-based NSO Group, owing to extensive media coverage of the spyware over the past several years. Pegasus can infect a person's smartphone without their knowledge using a digital exploit called a "zero day." A zero day is a flaw in software or hardware with no existing patch, which the spyware takes advantage of to gain access to the device.

---

<sup>8</sup> Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (New York, NY: Oxford University Press, 2021), 25.

<sup>9</sup> Drew Harwell, "Customs Officials Have Copied Americans' Phone Data at Massive Scale," *Washington Post*, September 19, 2022, <https://www.washingtonpost.com/technology/2022/09/15/government-surveillance-database-dhs/>.

<sup>10</sup> Adrian Shahbaz and Allie Funk, "Freedom on the Net 2021: The Global Drive to Control Big Tech" (Freedom House, November 2021), <https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech>.

<sup>11</sup> Bill Marczak et al., "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries" (University of Toronto, September 18, 2018), <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.

Persons targeted by Pegasus are either socially engineered into clicking a link that delivers the zero-day exploit<sup>12</sup> or, in more recent versions, the spyware infection can happen without a click or affirmative action by the user.<sup>13</sup> Once the spyware is installed, a remote operator can assume command and control of the device.<sup>14</sup> Figure 2 illustrates Pegasus’s capabilities. It is important to note that Pegasus is just one of many such spyware products that governments and government agencies can purchase. Additional kinds of commercial and government-developed spyware will be explored in Chapter IV.



<sup>12</sup> Marczak et al., 7.

<sup>13</sup> Bill Marczak et al., “FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild” (University of Toronto, September 13, 2021), 3, <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.

<sup>14</sup> Marczak et al., “HIDE AND SEEK,” 7.

## Figure 2. What Pegasus Can Extract

*Documentation allegedly from NSO Group illustrating the types of information that can be extracted from a targeted smartphone<sup>15</sup>*

This thesis seeks to understand how Pegasus and other forms of spyware used by governments in the MENA region have affected individuals' human rights since the Arab uprisings. A secondary question is whether spyware poses a unique threat given the variety of other digital repression tools. Third, this thesis will answer whether electoral and closed autocracies, the two prominent forms of governance in the region, use spyware differently. An examination of five countries—Egypt, Lebanon, Morocco, Saudi Arabia, and the UAE—facilitates the answering of these questions. The findings contribute to broader discussions around whether spyware poses a unique threat among the many tools of digital repression and how to counter it.

## Key Findings

### Deterioration of human rights since spyware introduced

A review of conditions in Egypt, Lebanon, Morocco, Saudi Arabia, and the UAE from the time of the Arab uprisings demonstrates that human rights have worsened for individuals in the region and those targeted abroad since the acquisition of commercial and government-developed spyware in the MENA region. The exception is Lebanon, where conditions have improved since 2011. Freedom of the Net and Digital Repression

---

<sup>15</sup> “WikiLeaks - The Hackingteam Archives,” accessed October 21, 2022, <https://wikileaks.org/hackingteam/emails/emailid/5391>.

Index scores support these findings. However, it is necessary to point out that it is difficult to quantify how much of the impact is caused specifically by spyware, as there are many other variables that cannot be controlled. Spyware is typically used in concert with other digital repression tools, and there are other socio-economic and structural factors at play in each person's situation that cannot be mitigated.

Most of the profiled individuals described the chilling effects of spyware, such as self-censoring and choosing topics or wording more carefully to avoid governmental responses that included defamation, loss of employment, imprisonment, and other negative reactions. They were more hesitant to socialize and make connections that may result in surveillance by association. Individuals found it more difficult to live their lives authentically, and in some the most extreme examples, spyware led to the arbitrary deprivation of life or to prolonged imprisonment in deplorable conditions.

Spyware poses a unique threat

Experts point to a number of concerns regarding the use of spyware that make it a unique threat: it is more intrusive than other digital repression tools and is hard if not impossible to block. Spyware operates secretively and often lacks the fingerprints that facilitate legal recourse against state actors. The tool is also easier for governments to use than traditional repression and coercion methods and some of the more technologically advanced passive surveillance systems.

Governance model does not always predict use of spyware

In the five countries examined that represent electoral and closed autocracies, each country uses spyware and digital repression differently. A comparison of Egypt and

Morocco's Freedom on the Net and Digital Repression Index scores confirmed that having a more liberal system of governance did not equate to less digital repression: Egypt boasts worse digital repression than Morocco, though Egypt is an electoral autocracy and Morocco is a closed autocracy. Distinct patterns of spyware use were observed in each country:

- Egypt: NGO representatives were subjected to travel bans and asset freezes in addition to surveillance via spyware. Regime critics were accused of sponsoring terrorist groups without prosecutors producing any real evidence; this allowed officials to keep them in pre-trial detention for up to two years.
- Morocco: Officials have used consensual sex and potentially trumped-up sexual assault charges to defame and shame individuals into silence. Charging dissidents as traitors or thieves instead of critics is also considered to be part of the Moroccan playbook for silencing dissidents.
- Saudi Arabia: All profiled individuals in the Saudi case study were targeted with Pegasus spyware. Several that live in exile have received warnings of credible threats against their lives, including around the time of the murder of Jamal Khashoggi, who was a Saudi insider turned dissident who wrote for the Washington Post. The detention of family members and relatives was used in several notable cases to try to coerce a target's return to Saudi Arabia.
- UAE: Keeping targeted Emiratis within the country's borders was a common theme for several of the individuals profiled. Several individuals were also subjected to smear campaigns intended to discredit them.

## Roadmap

This thesis is grouped in three parts. Part One introduces the thesis topic and explains the framework for answering it. This chapter describes Arab uprising dynamics and asks how human rights have been affected as spyware has been adopted since that period. It also asks whether there is a relationship between systems of governance and digital repression. Chapter II reviews the literature on the related topics of digital repression, spyware, and human rights, and demonstrates that there is a gap in analysis for the MENA region. Chapter III includes definitions for common terms appearing throughout this work and outlines research methods.

Part Two, Chapter IV explores the concept of digital repression and gives specific examples of its various forms in the MENA region, including targeted surveillance and the rise of commercial spyware. Chapter V provides a foundation to discuss the legitimacy of spyware use and analyzes the human rights laws and treaties that might be applicable in the region. It also describes current litigation against countries using spyware and spyware manufacturers.

Part Three, Chapter VI introduces the case study countries that follow: Egypt (Chapter VII), Lebanon (Chapter VIII), Morocco (Chapter IX), Saudi Arabia (Chapter X), and the UAE (Chapter XI). Each country profile summarizes digital repression since the Arab uprisings and catalogs the use of spyware. Five individuals who were confirmed targets of spyware are profiled in each chapter, except for Lebanon where there is only one profile due to a lack of victims that have publicized their experiences. Chapter XII summarizes results and Chapter XIII concludes the paper.

## Chapter II.

### Literature Review

There is a growing body of literature on the digital surveillance industry, but it is relatively nascent given that the technology itself is relatively new and operates behind a veil of secrecy. Analysis specific to the use of spyware by governments is limited, often comingled with other categories of digital repression, and is largely focused on its global use or on geographic regions outside of MENA. Human rights groups, think tanks, and the media often report on spyware with a focus on the technology itself or on specific subgroups of targets such as journalists or human rights defenders. I was unable to find a comparative study on the use of spyware across different systems of governance in the region. This thesis therefore presents an opportunity to examine an under-represented region, focus on a specific type of digital repression, targeted surveillance via spyware, and its effect on people. This research aims to answer three questions: how the use of spyware by governments in the MENA region has affected the human rights of those living in the region and beyond, whether spyware poses a unique risk among the many digital repression tools, and whether any variations in spyware usage across different countries and forms of governance is detected.

#### On Repression and Systems of Political Governance

Preceding research has demonstrated that the political system of governance relates to the use of repression as a tactic, whether physical or digital or both, and

repressive tactics are more commonly used by autocratic governments. Jacqueline DeMeritt summarizes the phenomenon as follows:

“Repression in a democracy is more costly than in an otherwise-comparable anocracy or autocracy, because democracy provides alternative mechanisms by which the population may control the state: participation and contestation. These reduce the need for the population to dissent, since grievances against the state may be communicated via ballot. They also raise the government’s cost of repression, since citizens who see the state’s use of coercion as illegitimate—those who believe that they or their fellow citizens are being repression—can vote authorities out of office.”<sup>16</sup>

The University of Gothenburg’s V-Dem Institute has created a quantitative framework for assessing MENA countries’ systems of governance, and tracking trends toward or against autocratization. In 2022, most all governments in the region are either closed autocracies, where absolute power is concentrated in an individual or group, or slightly more permissive electoral autocracies, where elections bring some representation (or semblance of it) to the system of governance. While Tunisia democratized following the Arab uprisings, it has since experienced democratic breakdown and nearly returned to its pre-revolution state as an electoral autocracy.

Currently, only one government in the region, Israel’s, falls on the democracy spectrum as a liberal democracy.<sup>17</sup>

---

<sup>16</sup> Jacqueline H. R. deMeritt, “The Strategic Use of State Repression and Political Violence,” Oxford Research Encyclopedia of Politics, October 26, 2016, <https://doi.org/10.1093/acrefore/9780190228637.013.32>.

<sup>17</sup> V-Dem Institute, “Autocratization Changing Nature?,” Democracy Report 2022 (V-Dem Institute, University of Gothenburg, March 2022), 45, [https://v-dem.net/media/publications/dr\\_2022.pdf](https://v-dem.net/media/publications/dr_2022.pdf).

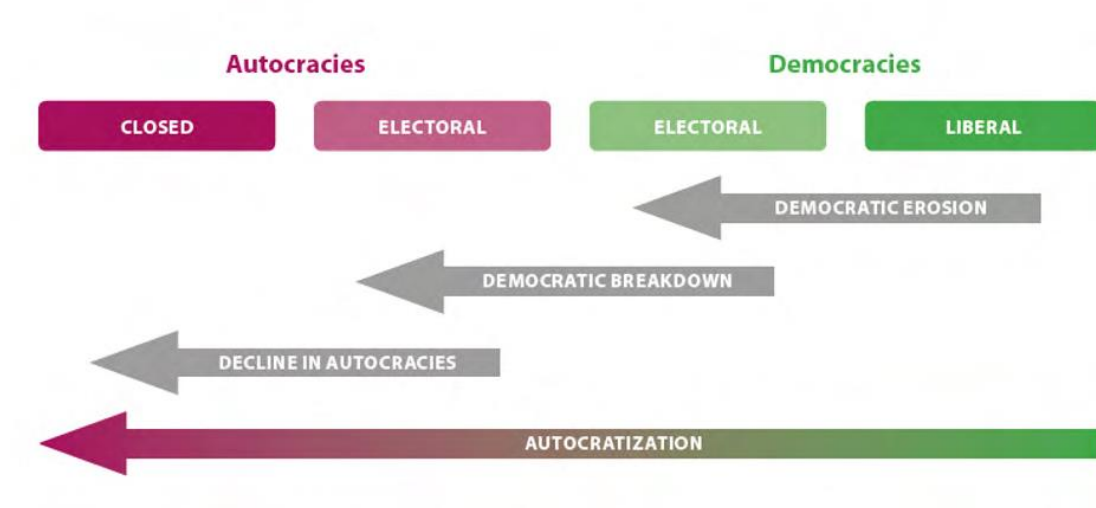


Figure 3. Types of Autocratization

*The V-Dem Institute's Varieties of Autocracy and Autocratization (V-Auth) research project defines four varieties of governance, from most liberal to most closed.<sup>18</sup>*

### On Digital Technology and Digital Repression

Four books stand out for their contributions to the topics of digital technology and digital repression, and only one is focused exclusively on the MENA region. None focuses exclusively on spyware.

Steven Feldstein's book, *The Rise of Digital Repression*, describes variations in how countries use digital repression tools owing to a country's technical expertise. Some countries with lower technical expertise use tactics such as internet shutdowns or jailing of online users posting dissenting views, while others develop higher technical expertise

<sup>18</sup> "Varieties of Autocratization – V-Dem," accessed December 30, 2022, <https://v-dem.net/our-work/research-programs/varieties-of-autocratization/>.

and invest in mass surveillance enabled by AI or big data, or smartphone targeting spyware such as Pegasus. His analysis focuses on Thailand, the Philippines, and Ethiopia.

Feldstein's work also highlights an important phenomenon: countries that rank highest in digital repression are autocracies, though democracies also use digital repression tactics. In addition, there is an overlap between countries that use digital repression and those that use traditional coercive strategies, including harassment, detention, beatings, and extrajudicial killings.

Feldstein developed a taxonomy for categorizing digital repression in Table 1; it provides a conceptual framework for understanding the various forms of repression carried out by governments. He also offers two tools for quantitative analysis: his digital repression index and v-auth scores from the V-Dem Institute, which are used in Figure 4. There is an important caveat to the digital repression index: it excludes data on targeted surveillance (including spyware).<sup>19</sup> For this reason, the index is referenced in this thesis but is not a core consideration.

Table 1. Forms of Digital Repression

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Surveillance | <ul style="list-style-type: none"><li>• Technologies, systems, or legal directives that enable control through identification, tracking, monitoring, or analysis of individual data or systems</li><li>• Passive surveillance: internet monitoring, mobile phone tapping, SIM registration, location monitoring, deep packet inspection, network interception, cable tapping, telecom surveillance</li><li>• Targeted surveillance: intrusion operations which manipulate software, data, computer systems, or networks in order to gain unauthorized access to user information &amp; devices (spyware/malware)</li></ul> |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

<sup>19</sup> Feldstein, *The Rise of Digital Repression*.

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        | <ul style="list-style-type: none"> <li>• AI &amp; big data surveillance: facial recognition, intelligent video, smart policing, smart cities/safe cities, social media monitoring</li> <li>• Surveillance laws: supports digital surveillance actions through the provision of intelligence &amp; national security laws, data disclosure, data retention, and data localization directives</li> </ul>                                                                                                                                                                                                                                                                                                                                                        |
| Online Censorship                      | <ul style="list-style-type: none"> <li>• Laws, regulations, or actions undertaken by state authorities to restrict content &amp; limit access to information</li> <li>• Content blocking and filtering</li> <li>• Social media / ICT apps blocked</li> <li>• Takedown requests; content removal</li> <li>• Distributed Denial of Service (DDOS) attacks</li> <li>• Infrastructure restrictions (internet firewalls; closed ICT infrastructure – e.g., Great Firewall, Halal Net)</li> <li>• Censorship laws &amp; directives: religion/blasphemy, cybercrime, false news/fake news, political/hate speech, lèse-majesté, security/terrorism, copyright infringement, defamation/libel/sedition, indecency/anti-LGBT, financial targeting of groups</li> </ul> |
| Social Manipulation and Disinformation | <ul style="list-style-type: none"> <li>• Strategies deployed by state or state-sponsored actors to shape narratives &amp; beliefs and to mislead &amp; manipulate users</li> <li>• Disinformation</li> <li>• Trolling, doxing, harassment</li> <li>• Flooding</li> <li>• Automated methods – bots, algorithms</li> <li>• Vandalism and defacement</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                  |
| Internet Shutdowns                     | <ul style="list-style-type: none"> <li>• Intentional restrictions or disruptions of ICT networks or electronic communications rendering them effectively unusable for a specific period of time</li> <li>• Total internet shutdowns</li> <li>• Partial shutdowns (restricted websites, blocked social media access)</li> <li>• Throttling, blackouts, slowdowns</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |
| Targeted Persecution of Online Users   | <ul style="list-style-type: none"> <li>• Online users persecuted by state authorities as a reprisal for posted political or social activity</li> <li>• Online users charged, arrested, imprisoned, or in prolonged detention</li> <li>• Online users physically attacked or killed</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

*Targeted surveillance is a subcategory of surveillance; targeted surveillance is referred to as spyware throughout this research*<sup>20</sup>

Nils Weidmann and Espen Geelmuyden Rød's book, *The Internet and Political Protest in Autocracies*, states that, given that autocracies are more likely to use repressive tactics, and most MENA governments are autocracies, it is unsurprising that digital repression is well documented in the region. However, autocracies use digital surveillance to support state aims in different ways. A closed autocracy is more likely to use digital repression in addition to traditional methods, while an electoral autocracy may opt to replace traditional methods with digital repression.<sup>21</sup> The book's underlying point that autocracies use digital repression tools differently sealed my decision to choose case study countries that represent variations in governance models.

Nicole Perlroth's book, *This is How They Tell Me the World Ends*, provides groundbreaking interviews and insights into zero days and the zero-day market that enhance understanding of the present-day spyware industry. The book has a U.S.-centric view and warns that the United States is focusing too much on cyber offense instead of investing in cyber defense.<sup>22</sup>

Marc Owen Jones's book, *Digital Authoritarianism in the Middle East*, describes digital repression in the MENA region with a focus on disinformation and

---

<sup>20</sup> Feldstein, 25.

<sup>21</sup> Weidmann, *The Internet and Political Protest in Autocracies* (Oxford University Press, 2019), 129–30.

<sup>22</sup> Nicole Perlroth, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race* (New York: Bloomsbury Publishing, 2020).

misinformation campaigns. He notes that Saudi Arabia and, to a lesser extent, the United Arab Emirates (UAE), are masters of online deception.<sup>23</sup>

In addition to these thought-provoking books, Freedom House's "Freedom on the Net" has detailed various forms of threats to internet freedom that amount to digital repression in annual reports since 2009. While the first report focused on 15 countries, the 2022 edition expanded to 70. Each edition assigns an internet freedom score to the assessed countries, providing a useful quantitative reference tool.<sup>24</sup> Freedom of the Net's analysis, which contains local NGO reporting, is a common source throughout this thesis.

### On Spyware

Research specific to spyware is limited for several reasons. First, commercial spyware is typically sold and purchased via non-disclosure agreements. Second, spyware is used clandestinely by government operators who want to stay undetected on a target's computer device for as long as possible. Third, this technology is also relatively new: commercial spyware was developed over the last decade and has only been revealed through leaks, hacking, investigative reporting, and digital forensic analysis in recent years. The existence of in-house spyware created by governments, also known as an advanced persistent threat, has similarly only been revealed indirectly.

One of the first and most informative leaks concerning commercial spyware was the hacking of the Hacking Team by a self-proclaimed human rights vigilante in 2015.

---

<sup>23</sup> Marc Owen Jones, *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media* (New York, NY: Oxford University Press, 2022).

<sup>24</sup> "Freedom on the Net Research Methodology," Freedom House, accessed January 21, 2023, <https://freedomhouse.org/reports/freedom-net/freedom-net-research-methodology>.

The hacker released over 400 gigabytes of data, including emails that shed light on previously secret business deals. The leaks exposed more than the Hacking Team; it also shed light on NSO Group and FinFisher's government clients and contracts.<sup>25</sup>

Another glimpse into the spyware industry was provided by the leak of more than 50,000 phone numbers that were targeted for surveillance using Pegasus spyware, hereafter referred to as the "Pegasus list." Analysis by the Forbidden Stories media consortium and Amnesty International allowed researchers and journalists around the globe to identify the persons targeted and chronicle how governments had used NSO Group technology against human rights defenders, academics, activists, businesspeople, lawyers, diplomats, and heads of states. The Pegasus list itself remains shrouded in mystery. It reportedly included numbers that were added by governments and national security and law enforcement agencies that were Pegasus operators between 2016 and 2020. By some accounts, researchers and journalists were able to determine which country had added a target's number, while others suggested that there was no such attribution on the list. NSO Group dismissed the resulting reporting as "uncorroborated theories."<sup>26</sup>

The investigations and analysis conducted on the Pegasus list provided insight into secret government surveillance targeting individuals and groups. Reporting by Pegasus Project media partners The Guardian, Le Monde, The Washington Post, Haaretz/TheMarker, Daraj, and PBS Frontline are referenced frequently throughout this

---

<sup>25</sup> Lorenzo Franceschi-Bicchierai, "The Vigilante Who Hacked Hacking Team Explains How He Did It," *Vice* (blog), April 15, 2016, <https://www.vice.com/en/article/3dad3n/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it>.

<sup>26</sup> "About The Pegasus Project | Forbidden Stories," accessed January 21, 2023, <https://forbiddenstories.org/about-the-pegasus-project/>.

thesis, from articles about the use of Pegasus to target Khashoggi's family members and associates<sup>27</sup> to Moroccan journalists.<sup>28</sup> Cumulatively, these articles and reports enable in-depth examination of the use of spyware in the MENA region.

There are many other newspaper articles and reports from human rights groups that document specific types of spyware and its targets. Forbidden Stories analyzed the Pegasus list to produce reporting on targeted journalists.<sup>29</sup> Human Rights Watch, Amnesty International, and other human rights groups have published reports and press statements detailing human rights defenders targeted with spyware. Most of the reporting on political leadership targeted with spyware is sourced from reputable newspapers, such as the Washington Post.<sup>30</sup>

Some journal articles have also lent additional insights into specific spyware use cases. One such article was published shortly after Egypt's revolution and it documented how Egyptian authorities had started experimenting with FinFisher to break Skype's encryption, enabling them to monitor citizens' voice and audio calls during the protests.<sup>31</sup>

The digital forensic analysis of two organizations have provided key insights into the spyware industry, though this reporting is typically not region specific. University of

---

<sup>27</sup> Stephanie Kirchgaessner, "Jeff Bezos Hack: Amazon Boss's Phone 'Hacked by Saudi Crown Prince,'" *The Guardian*, January 22, 2020, <http://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince>.

<sup>28</sup> Amnesty International, "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware," Amnesty International, October 10, 2019, <https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/>.

<sup>29</sup> "Journalists under Surveillance | Forbidden Stories," accessed January 21, 2023, <https://forbiddenstories.org/pegasus-journalists-under-surveillance/>.

<sup>30</sup> Craig Timberg et al., "Heads of State Found on List of Numbers Examined by Pegasus Project - The Washington Post," *Washington Post*, July 20, 2021, <https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/>.

<sup>31</sup> Elizabeth Bryant, "The Iron Fist vs. the Microchip," *Journal of Strategic Security* 5, no. 2 (2012): 1–26, <https://doi.org/10.5038/1944-0472.5.2.1>.

Toronto's Citizen Lab provides some of the most extensive analysis of government-developed and commercial spyware, potential operators, and victims, including technical details. Their reports on NSO Group, Candiru, Hacking Team, FinFisher, Stealth Falcon, Dark Caracal, and Nile Phish are referenced frequently in this thesis.<sup>32</sup> Amnesty International also conducts digital forensics via its Security Lab, and the resulting technical reports, are referenced here as well.<sup>33</sup>

### On the Arab Uprisings

Much of the research in the digital technology domain specific to the MENA region provides an over-simplified, Western view on the role of social media in the Arab uprisings. A few journal articles give a more nuanced accounting of the roles that the internet, mobile phones, satellite TV, and social factors played in mobilizing demonstrations and generating protest waves across the region during the Arab uprisings.<sup>34</sup> In most of the articles from the early 2010s, digital technology is seen as a positive influence on human rights: one that provides citizens the ability to express their opinions and assemble, and that could potentially serve as a liberalizing force.<sup>35</sup> This is important contextual background for analyzing the current use of spyware and digital repression tools.

### On Digital Technology and Human Rights

---

<sup>32</sup> "About the Citizen Lab" (Citizen Lab, University of Toronto), accessed January 21, 2023, <https://citizenlab.ca/about/>.

<sup>33</sup> "Amnesty Tech," Amnesty International, accessed January 21, 2023, <https://www.amnesty.org/en/tech/>.

<sup>34</sup> David Doherty and Peter J. Schraeder, "Social Signals and Participation in the Tunisian Revolution," *The Journal of Politics* 80, no. 2 (2018): 675–91, <https://doi.org/10.1086/696620>.

<sup>35</sup> Szmolka, *Political Change in the Middle East and North Africa*.

Research on the impact of digital technology on human rights exists but is typically not specific to the MENA region. Academics have noted that, in general, as citizens' use of the internet, mobile phones, and other digital devices have increased, governments have increased their surveillance of digital technology to mitigate perceived security and stability concerns. Technology once thought of as liberating has been co-opted by state actors.<sup>36</sup> The UN has provided some analysis on this topic. The secretary general released a report in 2022 that catalogued human rights defenders that had been targeted by their governments for cooperating with the UN.<sup>37</sup> UN special procedures, which include special rapporteurs and independent experts who report on specific countries and themes to the UN Human Rights Council, have also contributed limited reporting on spyware. The most notable of these are the reports by the Special Rapporteur on extrajudicial, summary, or arbitrary executions, Agnes Callamard, who investigated the murder and disappearance of Khashoggi.<sup>38</sup>

### Rationale for Research Questions

Based on the available literature, it is evident that several gaps exist. There currently is no comprehensive analysis detailing how spyware used by MENA governments affects the human rights of the individuals living in the region and beyond.

---

<sup>36</sup> Molly K. Land and Jay D. Aronson, "Human Rights and Technology: New Challenges for Justice and Accountability," *Annual Review of Law and Social Science* 16, no. 1 (2020): 226, <https://doi.org/10.1146/annurev-lawsocsci-060220-081955>.

<sup>37</sup> United Nations Office of the High Commissioner for Human Rights, "OHCHR | A/HRC/51/47: Cooperation with the United Nations, Its Representatives and Mechanisms in the Field of Human Rights - Report of the Secretary-General," OHCHR, accessed December 23, 2022, <https://www.ohchr.org/en/documents/thematic-reports/ahrc5147-cooperation-united-nations-its-representatives-and-mechanisms>.

<sup>38</sup> "OHCHR | Inquiry into the Killing of Mr. Jamal Kashoggi," OHCHR, accessed January 21, 2023, <https://www.ohchr.org/en/special-procedures/sr-executions/inquiry-killing-mr-jamal-kashoggi>.

The literature also does not adequately address whether spyware poses a unique threat or any variances in the use of spyware across countries in the region. This thesis will address these gaps and contribute to broader discussions on these topics.

## Chapter III.

### Research Methods

Government intelligence and law enforcement agencies clandestinely use spyware to target individuals of concern or interest, and information on the identity of these targets is not readily available. Similarly, data describing the human rights impact of spyware targeting is scarce. I will use the Arab uprisings—also commonly called the “Arab Spring”—as a reference point for determining whether human rights have improved or worsened with the increasing adoption of spyware by governments from late 2010 to present. Given limitations in the literature and scant data, I will take a mixed methods approach, and use Freedom House Freedom of the Net and Digital Repression Index scoring alongside interviews, testimony, newspaper articles, reports, and other primary-source information to understand the causal inference of this newer surveillance technology on the human rights of citizens in the region and living abroad.

This analysis is focused on the use of spyware, which is a subcategory of targeted surveillance. I have excluded a second form of targeted surveillance, data-extraction technology, from this thesis since it is used differently. Unlike spyware, data-extraction technology such as Cellebrite accesses information on a phone that has been handed over to authorities.<sup>39</sup>

### Definitions

---

<sup>39</sup> “Cellebrite Provides Facts About Its Business and Solutions,” Cellebrite, accessed January 28, 2023, <https://cellebrite.com/en/cellebrite-facts/>.

*Digital repression.* The use of information and communications technology in parallel to “...surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state.”<sup>40</sup> Throughout this thesis, digital repression refers to the taxonomy in Table 1.

*Exploit.* An exploit is a general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.<sup>41</sup>

*Hack / hacker.* To hack, in the context of computer security, is the action of performing activities on a computer system in an unauthorized manner. Computer hacking is considered an infringement of protected data and property and thus constitutes a malicious act. A hacker is a person who commits this act.<sup>42</sup>

*Malware.* Short for “malicious software,” malware refers to intrusive software developed to steal data and, in some instances, to damage or destroy computers and computer systems. Examples include viruses, worms, Trojan viruses, spyware, adware, and ransomware.<sup>43</sup> Malware that is installed at the network-level is out of scope for this thesis.

*MENA.* This abbreviation stands for the Middle East and North Africa region. Government agencies and academics draw different borders around this region. In my

---

<sup>40</sup> Feldstein, *The Rise of Digital Repression*, 25.

<sup>41</sup> “What Is an Exploit in Computing? - Definition from Techopedia,” Techopedia.com, accessed February 13, 2022, <http://www.techopedia.com/definition/4275/exploit>.

<sup>42</sup> “What Does Hack Mean in Security? - Definition from Techopedia,” Techopedia.com, accessed February 13, 2022, <http://www.techopedia.com/definition/3804/hack-security>.

<sup>43</sup> “What Is Malware? - Definition and Examples,” Cisco, accessed January 22, 2023, <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html>.

thesis, MENA refers to countries defined by the U.S. Department of State: Algeria, Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Palestinian Territories, Qatar, Saudi Arabia, Syria, Tunisia, the UAE, and Yemen.<sup>44</sup>

*Operator.* In this research, operator is the designation for a government or subnational entity that has the license or authorization to use spyware. Using Pegasus as an example, Citizen Lab identified 36 unique operators conducting surveillance in 45 countries in a 2018 report. The spyware operator is typically involved in both targeting and choosing the kinds of information that they want the command and control servers to extract from a target's device once the spyware has been downloaded.<sup>45</sup>

*Spyware.* Software that is installed on a computer device (which includes a mobile phone or smartphone) without the user's knowledge and that transmits information about the user's activities.<sup>46</sup> Spyware is a form of targeted surveillance and is a subcategory of malware.

*Target.* A person selected for spyware surveillance.

*Zero-day.* A flaw in software or hardware that has gone unnoticed by the developer for which there is no existing patch. Spyware takes advantage of such vulnerabilities to gain access to the device.

---

<sup>44</sup> U.S. Department of State, "Bureau of Near Eastern Affairs," United States Department of State, accessed February 13, 2022, <https://www.state.gov/bureaus-offices/under-secretary-for-political-affairs/bureau-of-near-eastern-affairs/>.

<sup>45</sup> Marczak et al., "HIDE AND SEEK."

<sup>46</sup> "Definition of SPYWARE," accessed January 22, 2023, <https://www.merriam-webster.com/dictionary/spyware>.

*Zero-click.* Digital exploits that require no click or affirmative action by the user to silently infect malware onto a computer system, which can enable digital surveillance or remote control of computers, phones, apps, and other digital tools.<sup>47</sup>

## Interviews

The conduct of my thesis involved interviewing human subjects; as such, approval was obtained from the Institutional Review Board whose work is guided by the ethical principles set forth in the Belmont Report. With the approval of my proposal in hand, I conducted interviews with individuals from government, NGOs, international organizations, and the media. I sought their expertise on matters ranging from security themes in the MENA region to the conduct of UN special rapporteur visits to digital repression. Most interviewees agreed to have their names included, while interviews with current U.S. government employees were on background. Several dissidents also approached me to share their experiences; their interviews provided first-hand accounts of the impact of spyware and digital repression on their human rights.

Interviews ranged in duration from 30 minutes to one hour and were conducted via Harvard Zoom, which uses 2-factor authentication to enhance the security of the communications.

## Case Studies

I identified five countries to profile as case studies. These countries are all located in the MENA region, as defined by the U.S. Department of State.<sup>48</sup> The chosen countries

---

<sup>47</sup> Perlroth, *This Is How They Tell Me the World Ends*.

<sup>48</sup> U.S. Department of State, "Bureau of Near Eastern Affairs."

represent variances in governance models according to v-auth scores from the V-Dem Institute. They are (in alphabetical order): Egypt, Lebanon, Morocco, Saudi Arabia, and the UAE. Egypt and Lebanon are electoral autocracies, though Lebanon leans more democratic while Egypt is less. Morocco, Saudi Arabia, and the UAE are closed autocracies and monarchies.

Each country review includes four elements:

1. the country's Freedom of the Net and digital repression index scores from 2010 to 2022 to indicate general internet freedom and digital repression trends;
2. the history of digital repression and general political context since the Arab uprisings, drawing upon the taxonomy in Table 1 to differentiate the various methods and tools observed: mass surveillance, online censorship, social manipulation and disinformation, internet shutdowns, and targeted persecution of online users;<sup>49</sup>
3. the types of Advanced Persistent Threat (government-developed) and commercially licensed spyware believed to be employed by that country's government or its representatives; and
4. the profiles at least five individuals who were targeted by spyware by the case study country, and for whom spyware targeting has been confirmed through digital forensic analysis.

Concerning number four, the intent is to only include the stories of individuals targeted by the country in the chapter they appear, though attribution is imperfect in some

---

<sup>49</sup> Feldstein, *The Rise of Digital Repression*, 27.

instances. Profiling individuals by targeting country, as opposed to nationality, allows a deeper examination of how each case study country uses spyware on targeted individuals and instances of transnational repression.

Lebanon is the exception to number four, as only one individual is profiled in that chapter. She states that it is unlikely that she was the target of Lebanese surveillance. However, at this time, she is reluctant to name the country that she believes targeted her. As her story is compelling and she has been public about the human rights impact to her, I have included her in that chapter.

I included interviews of each profiled individual, drawing from available reporting and, in several cases, interviews by this author. The experiences described by the profiled individuals were categorized into rights as identified in the International Bill of Human Rights, which is an amalgam of two covenants: the International Covenant on Economic, Social, and Cultural Rights, and the International Covenant on Civil and Political Rights.<sup>50</sup>

## Results

In the results section, I categorize comments made by profiled individuals into a list of human rights violations and abuses.

Using information from profiled individuals and Freedom of the Net and Digital Repression Index scores, I make a conclusion about whether human rights have improved or worsened with the increased adoption of spyware since the Arab uprisings.

---

<sup>50</sup> “OHCHR | International Bill of Human Rights,” OHCHR, accessed January 10, 2023, <https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights>.

Also drawing from these two scores, I assess whether there is a difference between the use of spyware in electoral versus closed autocracies. I compare individuals' stories to identify any country-specific trends and compare these trends against other profiled countries.

To isolate whether spyware brings a unique tool to the digital repression toolkit, I outline the opinions of experts.

I also reviewed the instances of transnational repression to identify any common themes.

### Limitations

There are limitations to the conduct of this thesis. Given the clandestine nature of spyware compounded by the lack of transparency in governments in the region, my analysis is at best incomplete.

The sample size of profiled individuals is small, given two factors: few people are aware that they have been targeted and those that know must weigh the risks associated with going public about it. Also, not all who have been targeted want to submit their personal device for digital forensic analysis given the additional risk of exposing personal information; having such analysis conducted was a requirement for inclusion in the case studies to maintain the quality of the sampling. As a result of the above considerations, the number of individuals available to profile is small. Any trends identified are micro-trends.

In addition, individuals are typically targeted using a variety of digital repression tools and methods, making it challenging to isolate the precise impact of spyware on their human rights. It is important to note that the categorization of spyware felt arbitrary at

times. Some mass surveillance also enables targeted surveillance with the same results as spyware, including real-time geolocation. Through interviews, I ask multiple experts what unique attributes spyware adds to the digital repression toolkit.

Despite these limitations, I believe this topic is timely and worthy of close examination to enhance discussions around how to better protect human rights in this digital era.

## Part Two:

### Chapter IV.

#### Digital Repression and the Rise of Spyware

During the Arab uprisings, individuals used the internet to share information and organize outside of traditional, government-operated communication lines, growing optimism that digital technology could democratize the MENA region. Many governments in the region were unprepared for the ways that activists used the internet, and they took quick steps to build their cyber capabilities in order to coerce and silence individuals they perceive as threats. Bruce Schneier describes this phenomenon as “the quick versus the strong”: the first to benefit from new technologies are those outside of traditional power structures who use it to magnify their collective power. Governments that are already powerful are typically slower to adopt new technologies, but when they do, they have “more raw power to magnify.”<sup>51</sup>

Several MENA regimes attempted to impede protest organization during the Arab uprisings by shutting down access to the internet, mobile phone networks, and social media sites. While these blunt techniques are still used today, regimes have gained ground with training and the adoption of new tools and methods, as outlined below.

#### Evolving Forms of Digital Repression

---

<sup>51</sup> Bruce Schneier, “The Quick vs the Strong: Commentary on Cory Doctorow’s Walkaway,” *Crooked Timber* (blog), April 26, 2017, <https://crookedtimber.org/2017/04/26/the-quick-vs-the-strong-commentary-on-cory-doctorows-walkaway/>.

## Internet and ICT Shutdowns

Internet shutdowns were one of the earliest tactics used by regimes to impede protest mobilization during the Arab uprisings. There are six main categories of internet shutdowns: national internet shutdowns, subnational internet shutdowns, national mobile shutdowns, subnational mobile shutdowns, national shutdowns of apps or service, and subnational shutdowns of apps or service.<sup>52</sup> Egypt's infamous shutdown of the internet during its revolution in 2011 was not a simple flip of a "kill switch" as often depicted in the media. Rather, it was the result of former President Hosni Mubarak government's order to two telecommunication companies, Vodafone and Orange, to cut access nationally to the internet, voice, and SMS.<sup>53</sup> A U.S. government official speaking on background said the Egyptian government's shutdown of mobile phone connectivity (both voice and data) had the opposite intended effect – rather than stop the organization of protests, the lack of information due to the information blackout prompted people to go to the streets to see what was happening.<sup>54</sup> Internet and data connectivity were disrupted from January 28, 2011, until Mubarak resigned nearly two weeks later.<sup>55</sup>

Other countries in the region have shut down mobile phone networks to limit the spread of information in a specific area or region. The Bahraini government shut down mobile phone and landline service in Duraz in 2016 during nightly curfews to slow protests from supporters of a Shiite cleric against the Sunni monarchy. Similarly, the

---

<sup>52</sup> Feldstein, *The Rise of Digital Repression*, 34.

<sup>53</sup> Deji Olukotun and Peter Micek, "Five Years Later: The Internet Shutdown That Rocked Egypt," *Access Now* (blog), January 22, 2016, <https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/>.

<sup>54</sup> Interview by author with U.S. government official, December 1, 2022.

<sup>55</sup> Al Jazeera, "Timeline: Egypt's Revolution," Al Jazeera, February 14, 2011, <https://www.aljazeera.com/news/2011/2/14/timeline-egypts-revolution>.

Lebanese government turned off mobile phones in the Lebanese town of Aarsal that borders Syria to stem fighting between the military and extremist militants.<sup>56</sup>

In addition, regimes in the region have also routinely restricted access or throttled traffic to smartphone apps, especially free messaging services using Voice Over Internet Protocol (VoIP) and encrypted messaging apps such as Skype, Viber, Telegram, WhatsApp, or those using Voice Over IP. This author had to use a Virtual Private Network (VPN) set to another country to circumvent Kuwait's blocking of Skype when residing there between 2009-2011. Some countries block use of these services and apps given difficulties intercepting such communication tools.<sup>57</sup> Countries including the UAE, Morocco, Egypt, and Saudi Arabia have also justified blocking these apps and services to protect the telecom industry from the competition.<sup>58</sup>

### Online Censorship

Online censorship is common in the MENA region, as authoritarian governments attempt to control the content their citizens consume and post. Blocking access to social media websites and distributed denial of service (DDOS) attacks are also forms of censorship that shape narratives in each country.<sup>59</sup> The director of London-based NetBlocks that tracks online censorship, Alp Toker, described the concern as follows: "We're starting to head toward a model where each country has its own version of the

---

<sup>56</sup> Sanja Kelly et al., "Freedom on the Net 2017, Manipulating Social Media to Undermine Democracy" (Freedom House, November 2017), 16.

<sup>57</sup> Sanja Kelly et al., "Freedom on the Net 2013, A Global Assessment of Internet and Digital Media," 6.

<sup>58</sup> Sanja Kelly et al., "Freedom on the Net 2016, Silencing the Messenger: Communication Apps under Pressure" (Freedom House, November 2016), 7.

<sup>59</sup> Feldstein, *The Rise of Digital Repression*, 30.

internet.”<sup>60</sup> Egypt provides some of the more egregious examples. In 2017, the Egyptian government blocked access to 21 news websites for allegedly supporting terrorism and spreading fake news. In 2018, Egyptian President al-Sisi ratified the Anti-Cyber and Information Technology Crimes Law, which allows the government to block websites that threaten national security or the national economy.<sup>61</sup>

### Targeted Persecution of Online Users

Freedom House describes this category of digital repression as “reprisal for digital expression,” and it encompasses forms of physical violence and legal action against online users.<sup>62</sup> Saudi Arabia began counterrevolutions to stifle regime threats, including by mobilizing Saudi citizens to engage in online surveillance. In 2017, the Saudi government incentivized their citizens to report on any “account on social networks publishing terrorist or extremist ideas’ under the hashtag banner ‘#we’re\_all\_security’.”<sup>63</sup>

### Social Manipulation and Disinformation

Social manipulation and disinformation are government tactics intended to shape narratives and beliefs in an effort to mislead and manipulate users. Rather than censor information, these tactics aim to weaponize communication.<sup>64</sup> While authoritarian

---

<sup>60</sup> Jared Malsin, “Throughout Middle East, the Web Is Being Walled Off,” *WSJ*, accessed January 8, 2023, <https://www.wsj.com/articles/throughout-middle-east-the-web-is-being-walled-off-1531915200>.

<sup>61</sup> Reema Hibrawi, “Egypt Leads the Pack in Internet Censorship across the Middle East,” *Atlantic Council* (blog), August 28, 2018, <https://www.atlanticcouncil.org/blogs/menasource/egypt-leads-the-pack-in-internet-censorship-across-the-middle-east/>.

<sup>62</sup> Feldstein, *The Rise of Digital Repression*, 35.

<sup>63</sup> Robert Uniacke, “Authoritarianism in the Information Age: State Branding, Depoliticizing and ‘de-Civilizing’ of Online Civil Society in Saudi Arabia and the United Arab Emirates,” *British Journal of Middle Eastern Studies* ahead-of-print, no. ahead-of-print (n.d.): 1–21, <https://doi.org/10.1080/13530194.2020.1737916>.

<sup>64</sup> Feldstein, *The Rise of Digital Repression*, 32.

governments have long histories of propaganda and disinformation, these newer tools and techniques have led to what Marc Owens Jones refers to as a “post-truth ‘moment’,” led primarily by Gulf Cooperation Council states. He argues that the central tenet of digital repression is deception to preserve the authoritarian status quo and minimize perceived ‘Islamist’ and Iranian threats.<sup>65</sup> Saudi Arabia is the leader in this area. Saudi Arabia outsourced some of this work to CTF Partners, an Australian PR firm located next door to the Saudi Embassy in London, to enhance the reputation of Saudi Crown Prince Mohammed bin Salman. The firm created websites promoting content aligned with Saudi foreign policy that gave the illusion of grassroots support for the crown prince’s reforms. They also used microtargeting on Facebook to further the reform narrative at a time when the crown prince was in the headlines for Khashoggi’s murder.<sup>66</sup>

## Surveillance

### Passive Surveillance

There are many kinds of passive surveillance. Common varieties include mobile phone tapping, location monitoring, network interception, and deep packet inspection, which are common throughout the MENA region.<sup>67</sup> Algeria, Bahrain, Israel, Kuwait, Lebanon, Qatar, Tunisia, and the UAE all deployed contact-tracing apps to track COVID-19 cases. Amnesty International flagged Bahrain and Kuwait’s apps, along with a third country’s, “as among the most alarming mass surveillance tools assessed...with all three

---

<sup>65</sup> Jones, *Digital Authoritarianism in the Middle East*, 31.

<sup>66</sup> Jones, 72.

<sup>67</sup> Feldstein, *The Rise of Digital Repression*, 28.

carrying out live or near-live tracking of users' locations by frequently uploading GPS coordinates to a central server.”<sup>68</sup>

Egypt and Turkey are among countries that use deep packet inspection (DPI) devices to redirect users to spyware, with implications for neighboring countries. A DPI middlebox installed in Türk Telekom's network redirected hundreds of Syrian users to spyware when they attempted to download certain Windows applications. It is believed that one of the IP addresses in Syria served the YPG (Kurdish militia), which the Turkish government has targeted militarily. Similar DPI middleboxes were identified in Telecom Egypt's network. They hijacked Egyptian internet users' unencrypted web connections and redirected them to revenue-generating content that featured affiliate ads and cryptocurrency mining. DPI devices in both countries were sold by Sandvine/Procera Networks, which is currently owned by the US-based private equity firm Francisco Partners.<sup>69</sup>

In recent years, there have been reports of the use of a sophisticated version of quasi-passive-targeted surveillance. Candiru, an Israeli product sold exclusively to governments, employs a “watering hole” technique: the spyware compromises select websites with an exploit that infects the iPhones, Androids, Macs, PCs, and cloud accounts of the people who visit the website. Compromised websites included the independent news organization Middle East Eye in 2020, and others focused on the

---

<sup>68</sup> “Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy,” Amnesty International, June 16, 2020, <https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/>.

<sup>69</sup> The Citizen Lab, “BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?,” The Citizen Lab, March 9, 2018, <https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/>.

Middle East, Yemen, Hezbollah, the Houthis, and Saudi dissidents.<sup>70</sup> In 2021, Citizen Lab identified at least 750 websites linked to Candiru globally, some of which impersonated human rights NGOs, social movements, international health organizations such as Amnesty International, Black Lives Matter, and WHO. The estimated 100 victims of Candiru were observed in Palestine, Israel, Iran, Lebanon, Yemen, Spain, United Kingdom, Turkey, Armenia, and Singapore. This type of surveillance serves to target individuals with specific interests and political leanings, such as human rights defenders, dissidents, journalists, and others. It is unknown what countries are responsible for the above websites compromised in 2020-2021, but Saudi Arabia, the UAE, and Qatar are among the countries believed to have purchased Candiru. The company offers an additional attack vector called Sherlock that may be a browser-based zero-click exploit.<sup>71</sup>

### AI and Big Data Surveillance

This category of surveillance serves to classify, store, and predict through automation. It is used primarily for understanding data at scale, whether social media surveillance, facial recognition systems, or smart cities. AI and big data allow Egypt's Ministry of Interior to analyze social media for surveillance on all citizens. Its "Social Networks Security Hazard Monitoring Operation," announced in 2014, would serve as a "public opinion measurement system" that would allow the monitoring of Islamists and people involved in "debauchery" and "homosexual acts."<sup>72</sup> In Dubai, security forces use

---

<sup>70</sup> Marc Owen Jones, "Israeli Spyware: What You Read Could Make You a Target," Middle East Eye, November 18, 2021, <http://www.middleeasteye.net/opinion/candiru-israel-spyware-surveillance-imperialism>.

<sup>71</sup> Bill Marczak et al., "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus" (University of Toronto, July 15, 2021), <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>.

<sup>72</sup> Herrera, "Citizenship under Surveillance."

facial recognition technology to track suspected criminals live across the city, leading to the arrest of 318 persons in 2018.<sup>73</sup> Forms of passive surveillance such as geo-location services can also be parsed by AI and big data to lend automated analysis to data and allow security services and law enforcement to identify issues and individuals of concern.<sup>74</sup> Big data and AI technology are especially powerful when paired with surveillance laws that retain individuals' metadata so that they could better track individual's online activities. Many MENA regimes have adopted such data retention laws in recent years.<sup>75</sup>

China is a formidable developer of passive surveillance and big data and AI technologies. As part of its Belt and Road Initiative, the "digital Silk Road" seeks to sell Chinese-built fiber-optic networks around the globe and to set the standard for how traffic is transmitted and coded. China regularly organizes forums with authoritarian governments for norm-sharing, such as the 2017 World Internet Conference in Wuzhen and intensive social media training. Officials from Egypt, Jordan, Lebanon, Libya, Morocco, Saudi Arabia, and the UAE have participated in such training.<sup>76</sup> In the MENA region, Bahrain, Egypt, Iran, Lebanon, Libya, Morocco, Saudi Arabia, and Tunisia have internet and mobile networking equipment installed by Chinese companies, and the UAE uses intelligent monitoring systems and facial recognition technology developed by Chinese companies.<sup>77</sup>

---

<sup>73</sup> "How Dubai's AI Cameras Helped Arrest 319 Suspects Last Year," accessed September 13, 2021, <https://gulfnews.com/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675>.

<sup>74</sup> Feldstein, *The Rise of Digital Repression*, 29–30.

<sup>75</sup> Sanja Kelly et al., "Freedom on the Net 2015, Privatizing Censorship, Eroding Privacy" (Freedom House, October 2015), 8.

<sup>76</sup> Adrian Shahbaz, "Freedom on the Net 2018, The Rise of Digital Authoritarianism" (Freedom House, November 2018), 8.

<sup>77</sup> Adrian Shahbaz, 9.

## Targeted Surveillance

Governments deploy targeted surveillance to monitor individuals deemed threatening to national security and—as often seen with authoritarian regimes—to leadership survival. This form of surveillance deploys intrusion operations (commonly malware or spyware) that manipulate software, data, computer systems, or networks to gain unauthorized access to user information and devices.<sup>78</sup> Citizen Lab has identified at least three models that demonstrate the capacities and tactics of actors involved in targeted surveillance. First, well-resourced states with strong technical capabilities may run their own national in-house development and operations, also known as “Advanced Persistent Threat” (APT) within the security industry. APT can also be created by cyber groups with direct or tacit government support. A second form of targeted surveillance uses repurposed crimeware, primarily Remote Access Trojans, and is mainly seen with groups involved in the Syrian civil war. A third form of targeted spyware is produced by private companies for sale to (mostly) government buyers and is called commercial spyware. Such spyware is also described as “lawful intercept” products and services that provide governments, law enforcement, and intelligence agencies with bespoke surveillance options.<sup>79</sup>

In this research we focus primarily on commercial spyware used by MENA regimes to target smartphones and highlight some of the in-house developed spyware as well. Malware that is installed at the network-level and digital-extraction technology that

---

<sup>78</sup> Feldstein, *The Rise of Digital Repression*, 27.

<sup>79</sup> Citizen Lab, “Communities @ Risk: Targeted Digital Threats Against Civil Society” (University of Toronto, November 11, 2014), <https://targetedthreats.net/media/1-ExecutiveSummary.pdf>.

is primarily used for forensic analysis are out of scope, as they are employed differently than spyware.

The emphasis on spyware targeting smartphones derives from how individuals access the internet in the region. In 2010, prior to the Arab Uprisings, over 50% of citizens in GCC countries had access to the internet via smartphones (mobile broadband), while less than 10% had fixed broadband at home. Fixed and mobile broadband penetration was lower in non-GCC countries, but mobile broadband still predominated over fixed broadband: 10% of Moroccans and 6.4% of Egyptians had access to mobile broadband, while less than 2% of the population that had access to fixed broadband in both countries.<sup>80</sup> By 2020, the average mobile phone subscription was just over one per person, most of which provided access to mobile broadband. The rate is higher in some countries, with 1.6 mobile phone subscriptions per person in Kuwait and nearly two mobile phone subscriptions per person in the UAE.<sup>81</sup>

### Spyware

There are at many reasons why governments in the MENA region and globally use spyware that go beyond the ubiquity of the smartphone and the vulnerability of its connection to the internet. First is high impact. Regimes can obtain myriad details from smartphone exfiltration that would be time-consuming or impossible to obtain otherwise. Spyware such as Pegasus can provide behavioral information such as schedules and

---

<sup>80</sup> PRB, “In Arab Countries, Mobile Internet and Social Media Are Dominant, but Disparities in Access Remain,” PRB, accessed December 11, 2022, <https://www.prb.org/resources/in-arab-countries-mobile-internet-and-social-media-are-dominant-but-disparities-in-access-remain/>.

<sup>81</sup> International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database, “Mobile Cellular Subscriptions (per 100 People) - Middle East & North Africa | Data,” accessed March 19, 2022, <https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2020&locations=ZQ&start=1960&view=chart>.

habits and potentially incriminating information about an individual's activities and connections. Second, knowledge of its use not only causes targeted individuals to self-censor, but one of the more chilling effects is that it also shapes their future self-expression to align with socially accepted norms more closely.<sup>82</sup> Third, digital surveillance is discrete and can reduce the risk of backlash seen with conventional coercive methods. The most recent versions of Pegasus require no action by the targeted individual to install, such as a phony link that when clicked delivers the spyware, and therefore can operate undetected. Fourth, the geopolitical risks of using unattributable spyware on targets abroad is lower than using human agents to conduct physical surveillance who, if caught, could raise bilateral tensions. Fifth, spyware operators typically store the data locally, which enables ongoing data collection and retention. Data localization is a particular concern with other surveillance methods where there may be legal hurdles to data sources outside of a country's jurisdiction. Sixth, the risk of litigation for transnational use is relatively low, as it is difficult to attribute spyware to a specific government operator and there may be additional legal hurdles such as jurisdiction and sovereign immunity laws that make it more difficult to hold spyware operator countries to account.

Who makes it

NSO Group

---

<sup>82</sup> Jonathon Penney, "Understanding Chilling Effects," *SSRN Electronic Journal*, 2021, 1455, <https://doi.org/10.2139/ssrn.3855619>.

Spyware like Pegasus is the ultimate tool in the security and intelligence community toolkit.<sup>83</sup> Once Pegasus is installed, the remote operator can enable digital surveillance of a targeted smartphone, capturing emails, texts, photos, passwords, messages on end-to-end encrypted apps, contacts, and calendar entries, Pegasus can also turn on the phone's camera, microphone, and geo-location for live capture.<sup>84</sup> This powerful tool is designed to help law enforcement and national security agencies thwart criminals and terrorists planning to harm innocent civilians.<sup>85</sup>

NSO Group sells its products to licensed government intelligence law enforcement agencies but does not disclose its clients.<sup>86</sup> The company maintains that there are over 55 countries that it will not sell its technology to, including if it believes a nation-state customer has "...inadequate country-level protections in place to confidently prevent product misuse, or where the rule of law creates an unduly high risk of misuse."<sup>87</sup> Prior to sale, potential customers undergo an internal human rights due diligence process by NSO Group, governmental export authority reviews, and a review by the Israeli Ministry of Defense through a process similar to an arms sale.<sup>88</sup>

Given the secretive nature in which surveillance technology is sold and operated, it is difficult to confirm how Pegasus has been deployed. NSO Group claims that its

---

<sup>83</sup> Perlroth, *This Is How They Tell Me the World Ends*, 7.

<sup>84</sup> Marczak et al., "HIDE AND SEEK."

<sup>85</sup> "CYBER INTELLIGENCE SECTOR LEADER NSO GROUP UNVEILS THE INDUSTRY'S FIRST 'TRANSPARENCY AND RESPONSIBILITY REPORT,'" *NSO Group* (blog), accessed October 17, 2021, <https://www.nso.group.com/News/cyber-intelligence-sector-leader-nso-group-unveils-the-industrys-first-transparency-and-responsibility-report/>.

<sup>86</sup> "NSO GROUP - About Us," *NSO Group* (blog), accessed April 18, 2022, <https://www.nso.group.com/about-us/>.

<sup>87</sup> NSO Group, "NSO Group Transparency and Responsibility Report" (Tel Aviv, Israel, June 30, 2021), 8, <https://www.nso.group.com/wp-content/uploads/2021/06/ReportBooklet.pdf>.

<sup>88</sup> *Watch 60 Minutes: The Tool Meant to Hack Any Smartphone - Full Show on Paramount Plus*, accessed October 17, 2021, [https://www.paramountplus.com/shows/60\\_minutes/video/PAw6rD\\_p57euS0hC9\\_6gtKM8AWYXMhCO/ceo-of-israeli-spyware-maker-nso-on-fighting-terror-khashoggi-murder-and-saudi-arabia/](https://www.paramountplus.com/shows/60_minutes/video/PAw6rD_p57euS0hC9_6gtKM8AWYXMhCO/ceo-of-israeli-spyware-maker-nso-on-fighting-terror-khashoggi-murder-and-saudi-arabia/).

technology has prevented terrorist shooting sprees, car bombs and suicide bombings in heavily populated public areas; broken up pedophilia, and sex and drug-trafficking rings; found and rescued kidnapped children; located survivors trapped under collapsed buildings during natural disasters; and stopped the spread of specific COVID-19 outbreaks, though this cannot be independently verified.<sup>89</sup> The head of a western European intelligence agency told 60 Minutes correspondent Leslie Stahl off camera that Pegasus is a “gamechanger for foiling European jihadists as well as shutting down drug and human trafficking rings.”<sup>90</sup>

In the hands of one government, the license to operate Pegasus might be legitimate, yet in another, this dual-use technology can be used in ways that flout international humanitarian law. Despite NSO Group’s reported commitment to respect human rights,<sup>91</sup> leaks have confirmed that countries that have purchased Pegasus<sup>92</sup> include several that have used it to target civil society in the MENA region. These include Bahrain, Egypt, Jordan, Lebanon, Morocco, Saudi Arabia, and the UAE—countries known to have abused surveillance tools to track dissidents.<sup>93</sup> Israel also uses Pegasus technology on Israeli and Palestinian targets, bringing the total to at least eight known Pegasus operators in the region.<sup>94</sup>

NSO Group has come under scrutiny for its controversial sale of Pegasus to Saudi Arabia, which used Pegasus spyware to collect information on Jamal Khashoggi from the

---

<sup>89</sup> NSO Group, “NSO Group Transparency and Responsibility Report,” 7.

<sup>90</sup> *Watch 60 Minutes*.

<sup>91</sup> NSO Group, “NSO Group Transparency and Responsibility Report,” 10.

<sup>92</sup> “WikiLeaks - The Hackingteam Archives.”

<sup>93</sup> Marczak et al., “HIDE AND SEEK.”

<sup>94</sup> Steven Feldstein and Brian Kot, “Democracy, Conflict, and Governance Program: Global Inventory of Commercial Spyware and Digital Forensics,” Carnegie Endowment for International Peace, accessed January 9, 2023, <https://carnegieendowment.org/programs/democracy/commercialspyware>.

phones of family and friends. Khashoggi was brutally murdered by Saudi officials in October 2018 at the Saudi consulate in Istanbul, Turkey.<sup>95</sup> Khashoggi was once considered a Saudi insider, but prior to his death, had become increasingly vocal about Saudi Arabia's repression, which led him to flee and live in exile in the United States.<sup>96</sup> Former NSO Group CEO Shalev Hulio denies that Pegasus was used in the murder of Khashoggi.<sup>97</sup>

#### Other spyware manufacturers

NSO Group is not the only company in the spyware industry that is marketing dual-use products to countries with poor human rights records. Some of the earliest reports of spyware in the MENA region come from Bahrain, where the government used FinFisher to target 77 electronic devices of prominent lawyers, activists, and politicians domestically from 2010-2012. These activists suspected that they had been targeted when they were presented with their e-mail, text messages, or other communications during interrogations or when authorities used them as evidence in trials.<sup>98</sup> The targeting arrived in the form of important information about political developments or planned protests that concealed malware. Once the malware downloaded, it enabled attackers to monitor their targets' keystrokes and personal communications.<sup>99</sup> Although FinFisher denied that

---

<sup>95</sup> United Nations Human Rights Council, "Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi\*," Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development, June 19, 2019, [https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session41/Documents/A\\_HRC\\_41\\_CRP.1.docx](https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_CRP.1.docx).

<sup>96</sup> Jamal Khashoggi, "Opinion | Read Jamal Khashoggi's Columns for The Washington Post," *Washington Post*, accessed October 29, 2022, <https://www.washingtonpost.com/news/global-opinions/wp/2018/10/06/read-jamal-khashoggis-columns-for-the-washington-post/>.

<sup>97</sup> *Watch 60 Minutes*.

<sup>98</sup> Sanja Kelly et al., "Freedom on the Net 2013, A Global Assessment of Internet and Digital Media," 8.

<sup>99</sup> Sanja Kelly et al., 4.

it has sold a copy of to the Bahraini government, documents hacked and leaked from the company confirmed that Bahrain had purchased a license to use it.<sup>100</sup>

Many of the more well-known companies creating spyware in this space are based in democratic countries: Germany's FinFisher, Amesys/Nexa in France; Italy's now-defunct Hacking Team;<sup>101</sup> Candiru, Quadream, and Cytrox in Israel; and the hack-for-hire company BellTroX located in India that has both government and private clients.<sup>102</sup>

China is also active in the digital surveillance market, though is more well-known for its mass surveillance, big data, and AI products. Chinese telecom companies Huawei<sup>103</sup> and ZTE<sup>104</sup> are important players in the targeted surveillance industry, along with cyber companies Knowlesys and Sempitan.<sup>105</sup> Private Chinese companies, some of which are subsidized by the Chinese state, have supplied surveillance tools to 63 countries.<sup>106</sup>

---

<sup>100</sup> Fahad Desmukh, "Bahrain Government Hacked Lawyers and Activists with UK Spyware," *Bahrain Watch* (blog), accessed August 15, 2014, <https://web.archive.org/web/20140815233325/https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/>.

<sup>101</sup> Winnona Desombre, Lars Gjesvik, and Johann Ole Willers, "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets," #ACCyber, November 2021, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/>.

<sup>102</sup> Ronald Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy," *Foreign Affairs*, December 12, 2022, <https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert>.

<sup>103</sup> Joe Parkinson Chin Nicholas Bariyo and Josh, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, sec. Tech, <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>.

<sup>104</sup> "Analysis | The Cybersecurity 202: Trump's ZTE Reversal Flouts Warnings from Top National Security Officials," *Washington Post*, accessed October 29, 2022, <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/14/the-cybersecurity-202-trump-s-zte-reversal-flouts-warnings-from-top-national-security-officials/5af87ab030fb0425887994ca/>.

<sup>105</sup> Freedom House, "Freedom on the Net 2019: The Crisis of Social Media" (Freedom House, 2019), 13, <https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>.

<sup>106</sup> Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 2019), 8, [https://carnegieendowment.org/files/WP-Feldstein-AISurveillance\\_final1.pdf](https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf).

Governments in the MENA region have purchased from many of these companies and more, as indicated in Table 2. Steven Feldstein and Brian Kot compiled this information from multiple sources including Citizen Lab, Freedom House, Privacy International, the Council on Foreign Relations' Cyber Operations Tracker, the Electronic Frontier Foundation, Article 19, Access Now, related research organizations, and data from major print and news media outlets (e.g., The New York Times, Reuters, Haaretz, Financial Times, The Wall Street Journal).<sup>107</sup>

Table 2. MENA Region Spyware Inventory

|         | Dates Used            | Commercial Entity | Entity Country of Origin | Description                                                                                                                                                                                  |
|---------|-----------------------|-------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Algeria | --                    | --                | --                       | --                                                                                                                                                                                           |
| Bahrain | 2010-2012             | FinFisher         | Germany                  | Arab Spring activists hacked                                                                                                                                                                 |
|         | 2016-2018, 2020, 2021 | NSO Group         | Israel                   | Activists hacked                                                                                                                                                                             |
| Egypt   |                       | Cytrox            | Israel, Hungary          |                                                                                                                                                                                              |
|         |                       | FinFisher         | Germany                  |                                                                                                                                                                                              |
|         | 2013                  | Hacking Team      | Italy                    | Malware campaigns against civil society                                                                                                                                                      |
| Iran    | --                    | --                | --                       | --                                                                                                                                                                                           |
| Iraq    | --                    | --                | --                       | --                                                                                                                                                                                           |
| Israel  |                       | NSO Group         | Israel                   | Police reportedly used Pegasus against antigovernment protests, senior politician, mayors & employees of government-owned companies; Pegasus also found on Palestinian activists' cellphones |
| Jordan  |                       | FinFisher         | Germany                  | Malware to spy on journalists, human rights defenders, and opposition                                                                                                                        |

<sup>107</sup> Steven Feldstein and Brian Kot, "Democracy, Conflict, and Governance Program."

|                         |           |              |                 |                                                                                                      |
|-------------------------|-----------|--------------|-----------------|------------------------------------------------------------------------------------------------------|
|                         | 2019-2021 | NSO Group    | Israel          | Mobile phones of four Jordanian human rights activists were hacked over a two-year period            |
| Kuwait                  | --        | --           | --              | --                                                                                                   |
| Lebanon                 |           | Dark Caracal | Lebanon         | Developed unique mobile surveillance tool, Dark Caracal/Pallas, to extract data from Android devices |
|                         | 2014      | FinFisher    | Germany         | Linked to General Directorate of General Security & Internal Security Forces                         |
|                         |           | Hacking Team | Italy           | --                                                                                                   |
| Libya                   | --        | --           | --              | --                                                                                                   |
| Morocco                 | 2012-2015 | FinFisher    | Germany         | Allegedly used by Supreme Council of National Defense                                                |
|                         | 2012-2014 | Hacking Team | Italy           | Remote Control Systems (RCS) used against award-winning Moroccan media outlet Mamfakinch             |
|                         | 2017-2021 | NSO Group    | Israel          | Spyware targeted civil society and French government officials                                       |
| Oman                    |           | Hacking Team | Italy           | Targeted surveillance linked to Oman's Ministry of Interior                                          |
|                         |           | FinFisher    | Germany         | Targeted surveillance linked to Oman's Ministry of Interior                                          |
|                         |           | Cytrox       | Israel, Hungary | Targeted surveillance linked to Oman's Ministry of Interior                                          |
| Palestinian Territories | --        | --           | --              | --                                                                                                   |
| Qatar                   | --        | --           | --              | --                                                                                                   |
| Saudi Arabia            |           | Hacking Team | Italy           | Extensive documented abuse of spyware to target political opponents & civil society                  |
|                         | 2017-2018 | NSO Group    | Israel          | --                                                                                                   |
|                         |           | FinFisher    | Germany         | --                                                                                                   |
|                         | 2018-2021 | Candiru      | Israel          | --                                                                                                   |
|                         |           | Cytrox       | Israel, Hungary | --                                                                                                   |
|                         | 2019-2021 | Quadream     | Israel          | --                                                                                                   |
| Syria                   | --        | --           | --              | --                                                                                                   |
| Tunisia                 | --        | --           | --              | --                                                                                                   |

|                            |      |              |         |                                                       |
|----------------------------|------|--------------|---------|-------------------------------------------------------|
| United Arab Emirates (UAE) | 2012 | Hacking Team | Italy   | Surveilled newspaper editor; tracked regime opponents |
|                            | 2021 | Candiru      | Israel  | --                                                    |
|                            | 2011 | FinFisher    | Germany | --                                                    |
|                            | 2016 | NSO Group    | Israel  | --                                                    |
| Yemen                      | --   | --           | --      | --                                                    |

*Inventory of countries using spyware, dates of use, spyware used and country of spyware maker, and details of targeting, where available. Cells marked with "--" indicate that information is not available.<sup>108</sup>*

---

<sup>108</sup> Steven Feldstein and Brian Kot.

## Chapter V.

### Legitimacy of Spyware

Revelations regarding the apparent widespread use of the Pegasus software to spy on journalists, human rights defenders, politicians and others in a variety of countries are extremely alarming, and seem to confirm some of the worst fears about the potential misuse of surveillance technology to illegally undermine people's human rights.

—Michelle Bachelet, UN High  
Commissioner for Human Rights<sup>109</sup>

States often engage in activities seen as invasive, unethical, and illegal if private companies or individuals were to conduct them. Whether democracy or dictatorship, the tools of state surveillance are often the same, but a key difference is motive. “Is espionage necessary to defend the freedoms and values of a democratic State and protect its citizens, or to protect a regime from domestic challenge, including by suppressing internal dissent?” asks David Omand, author and former UK Director of the Government Communications Headquarters (GCHQ). If the former, it may be possible to form an ethical boundary around surveillance activities that supports the values of liberal democracy and creates a democratically backed “license to operate.” If the latter, the regime may move unhindered by such considerations.<sup>110</sup>

For many governments in the MENA region, spyware and other forms of digital repression provide an option that supports their form of autocracy. Some governments have substituted physical surveillance and coercive tactics such as detentions, torture,

---

<sup>109</sup> “Use of Spyware to Surveil Journalists and Human Rights Defenders, Statement by UN High Commissioner for Human Rights Michelle Bachelet,” OHCHR, July 19, 2021, <https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner>.

<sup>110</sup> “The Morality of Espionage,” *Engelsberg Ideas* (blog), February 9, 2021, <https://engelsbergideas.com/essays/the-morality-of-espionage/>.

beatings, and extrajudicial killings with spyware and other forms of digital repression.<sup>111</sup> They may view digital repression as more effective and less obtrusive than violent tactics. Additionally, digital repression may pose a lower risk of undermining regime legitimacy that keeps the ruler or ruling party in power. For other regimes, spyware has reinforced traditional tactics, to strengthen control where it is already applied.<sup>112</sup>

Spyware is one of several digital surveillance methods that achieves a similar result as the others: the collection of personal information. Such collection can be accomplished via targeted surveillance, passive surveillance, big data and AI methods, or all three, depending on a country's means and methods. Examples include Pegasus, which is a targeted surveillance product that exploits the smartphone of an individual, or Cerebro, a tool that is installed in internet networks to conduct passive surveillance (see Egypt case study for more details).

### Legitimacy and human rights

State surveillance can be legitimate when it meets certain criteria. According to international human rights law, domestic surveillance laws should be publicly available, clear, and precise; surveillance actions must meet the “necessity and proportionality” international legal standard; and the interests defining the surveillance action must be legitimate.<sup>113</sup> In the aftermath of 9/11, governments justified the use of digital

---

<sup>111</sup> Weidmann, *The Internet and Political Protest in Autocracies*, 130.

<sup>112</sup> Feldstein, *The Rise of Digital Repression*, 11–13.

<sup>113</sup> Steven Feldstein, “The Global Expansion of AI Surveillance,” *Carnegie Endowment for International Peace - Papers*, 2019, <https://search.proquest.com/docview/2299099093?pq-origsite=primo>.

surveillance to prevent and fight crime stemming from terrorism, global crises, organized crime, and natural disasters.<sup>114</sup>

To minimize the negative effects of surveillance, democracies employ safeguards to varying degrees, and they draw upon democratic institutions to initiate public consultation and correct mistakes.<sup>115</sup> A Belgian federal police spokesperson speaking about their agency's use of spyware says that it respects "a legal framework as to the use of intrusive methods in private life." Pegasus provides law enforcement agencies with limited cyber-intelligence capacity the ability to know where criminals "...store the gas, to go to the place, to put the explosive..." according to another senior European law enforcement official. Former NSO Group CEO Shalev Hulio claims that "Almost all governments in Europe are using our tools." Several European authorities, including in Germany, Poland, and Hungary, have admitted to using Pegasus. Law enforcement in Belgium reportedly uses it though will not admit it.<sup>116</sup> The FBI also reportedly purchased Pegasus in 2019 but deny using it.<sup>117</sup> Irrespective of democratic guardrails, the use of such technology is contentious even in liberal countries. This is evidenced by the domestic and international outcry over the Edward Snowden leaks concerning highly

---

<sup>114</sup> Elvira Santiago Gomez and Carmen Rodriguez Rodriguez, "Surveillance Technologies: A review of legitimate State violence in security and control contexts," *Encrucijadas (Salamanca, Spain)* 16 (2018), <http://gateway.webofknowledge.com/gateway/Gateway.cgi?GWVersion=2&SrcApp=Summon&SrcAuth=ProQuest&DestApp=WOS&DestLinkType=FullRecord&UT=000455807000011>.

<sup>115</sup> Sanja Kelly et al., "Freedom on the Net 2014, Tightening the Net: Governments Expand Online Controls" (Freedom House, 2014), 5.

<sup>116</sup> Ronan Farrow, "How Democracies Spy on Their Citizens," *The New Yorker*, April 18, 2022, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.

<sup>117</sup> Michael Levenson, "F.B.I. Secretly Bought Israeli Spyware and Explored Hacking U.S. Phones," *The New York Times*, January 28, 2022, sec. World, <https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html>.

classified NSA programs that stored the metadata of Americans and non-Americans for the mining of information as part of the U.S.'s antiterrorism efforts.<sup>118</sup>

### Human rights in the MENA region

In authoritarian regimes, executive decrees and unilateral decisions can bypass judicial or legislative oversight.<sup>119</sup> This creates the conditions for reduced accountability and increased unlawful surveillance in the MENA region, despite safeguards provided by international human rights law<sup>120</sup> and the ratification of human rights treaties by some MENA governments. It is instructive to examine the structural impediments that create the conditions for illegitimate surveillance.

Within the Gulf Cooperation Council (GCC), a regional body comprising six Arabian Gulf countries, over half of the states have ratified the ten core UN human rights treaties. All six GCC states have ratified The Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW), The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), The Convention on the Rights of the Child (CRC), and The Convention on the Rights of Persons with Disabilities (CRPD). Despite this, human rights monitors, international organizations, NGOs, and governments accuse GCC members of failing to live up to their obligations.<sup>121</sup> Upon closer scrutiny, many of these countries cited reservations when

---

<sup>118</sup> Sanja Kelly et al., "Freedom on the Net 2013, A Global Assessment of Internet and Digital Media," 7.

<sup>119</sup> Sanja Kelly et al., "Freedom on the Net 2014, Tightening the Net: Governments Expand Online Controls," 5.

<sup>120</sup> Steven Feldstein, "The Global Expansion of AI Surveillance," 2019.

<sup>121</sup> Rachel A. George, "Dialogue as Progress?: Islam and UN Human Rights Treaty Ratification in the Gulf Cooperation Council States," in *The Arab Gulf States and the West*, 1st ed. (Routledge, 2019), 289, <https://doi.org/10.4324/9780429505300-15>.

ratifying the treaties, namely Islamic incompatibility due to Sharia law.<sup>122</sup> As a result, UN human rights treaties do not have extensive effects on institutions, legislative changes, and judicial decisions in the GCC region post ratification.<sup>123</sup>

Beyond the GCC, other MENA governments have ratified key human rights treaties, though again, structural impediments have contributed to conditions for illegitimate surveillance. Of the previously mentioned human rights treaties, the International Covenant on Civil and Political Rights (ICCPR) is one of the most relevant to surveillance legitimacy, as it seeks to target the necessary conditions for a domestic legal environment that protects civil and political rights. The core aims of the ICCPR address emergency and counterterrorism legislation, the administration of justice, the death penalty, democratic rights, the protection of minorities and indigenous peoples, and equality and non-discrimination.<sup>124</sup> The ICCPR has been widely accepted within the MENA region, boasting ratification by 16 of 19 countries: Bahrain, Egypt, Iraq, Iran, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Palestine, Qatar, Syria, Tunisia, and Yemen.<sup>125</sup> The three missing are Algeria, Saudi Arabia, and the UAE. Like the treaties signed by GCC countries, structural impediments such as state reservations on the covenant (often owing to Sharia law differences) and strained relationships between the UN Human Rights Council and MENA governments have limited the ICCPR's legal

---

<sup>122</sup> George, 301.

<sup>123</sup> Başak Çali, Nazila Ghanca, and Benjamin Jones, "Big Promises, Small Gains: Domestic Effects of Human Rights Treaty Ratification in the Member States of the Gulf Cooperation Council," *Human Rights Quarterly* 38, no. 1 (2016): 21–57, <https://doi.org/10.1353/hrq.2016.0017>.

<sup>124</sup> Daniel Moeckli, Helen Keller, and Corina Heri, *The Human Rights Covenants at 50: Their Past, Present, and Future*, First edition. (Oxford: University Press, 2018), 124.

<sup>125</sup> "UN Treaty Body Database," United Nations Human Rights Treaty Bodies, accessed October 10, 2022, [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/treaty.aspx?treaty=cescr&lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/treaty.aspx?treaty=cescr&lang=en).

influence in the region. These states often posit that their constitutional arrangements and laws offer sufficient civil and political protections for their people.<sup>126</sup>

With limited local laws, regulations, and incomplete adoption of international treaties, citizens in the MENA region enjoy fewer protections from illegitimate surveillance. Such illegitimate surveillance can profoundly affect an individual's right to privacy and lead to what Office of the UN High Commissioner for Human Rights (OHCHR) has called "arbitrary or unlawful interference with his or her privacy, family, home or correspondence." Surveillance can infringe upon an individual's right to freedom of association, opinion, and expression,<sup>127</sup> and can also influence changes in behavior.<sup>128</sup>

#### Transnational questions of legitimacy

In countries outside of the MENA region with stronger national human rights protections, citizens have also been targeted and victimized by surveillance technology deployed by MENA regimes. Here, the applicability of human rights laws and domestic cybersecurity laws is being tested via lawsuits. In the United Kingdom, the smartphones of Princess Haya, former wife of the Ruler of Dubai Sheikh Mohammed al Makhtoom; two of her solicitors; her personal assistant; and two members of her security detail were hacked by Pegasus technology. The NSO reportedly informed Princess Haya's lawyers of the targeting in an effort to enforce the company's terms of use, which are limited to

---

<sup>126</sup> Moeckli, Keller, and Heri, *The Human Rights Covenants at 50*, 125.

<sup>127</sup> Steven Feldstein, "The Global Expansion of AI Surveillance," 2019.

<sup>128</sup> Santiago Gomez and Rodriguez Rodriguez, "Surveillance Technologies."

“combatting terrorism and violent crime.”<sup>129</sup> In this child protection battle between Princess Haya and her former husband, the High Court judgments called the hacking "serial breaches of [UK] domestic criminal law" that were "in violation of fundamental common law and [European Court of Human Rights] ECHR rights." They were described as "interference with the process of this court and the mother's access to justice" and an "abuse of power" by a head of government.<sup>130</sup> Also in the United Kingdom, a judge gave satirist Ghanem Almasarir the green light to sue Saudi Arabia for hacking his phone using Pegasus and for a physical attack on him by Saudi agents in London in 2018.<sup>131</sup> It is believed to be one of the first cases in which an exception to the sovereign immunity clause has been granted, allowing a foreign government to be sued for using spyware against individuals in the UK.<sup>132</sup> The case is proceeding in a UK court at the time of publishing.

Other lawsuits from countries with more safeguards for individuals' rights have targeted spyware and mass surveillance companies, instead of the country operating the technology. In France, four executives of Amesys and Nexa Technologies were indicted by the crimes against humanity and war crimes unit of the Paris Judicial Court. They were found to be complicit in cases of torture in Libya and torture and forced

---

<sup>129</sup> Eytan Avriel, "Two UAE Princes Each Got Their Own Personal NSO Spyware," *Haaretz*, November 17, 2021, <https://www.haaretz.com/israel-news/tech-news/2021-11-17/ty-article/.premium/two-uae-princes-each-got-their-own-personal-nso-spyware/0000017f-e395-d9aa-afff-fbdd23c30000>.

<sup>130</sup> "Princess Haya: Dubai Ruler Had Ex-Wife's Phone Hacked - UK Court," *BBC News*, October 6, 2021, sec. Middle East, <https://www.bbc.com/news/world-middle-east-58814978>.

<sup>131</sup> "Digital Nightmare: The Arab Dissidents Ruined by Phone Hacking," *Middle East Eye*, accessed September 26, 2022, <http://www.middleeasteye.net/big-story/digital-nightmare-arab-dissidents-lives-torn-apart-hacking>.

<sup>132</sup> Stephanie Kirchgaessner, "British Judge Rules Dissident Can Sue Saudi Arabia for Pegasus Hacking," *The Guardian*, August 19, 2022, sec. World news, <https://www.theguardian.com/world/2022/aug/19/british-judge-rules-dissident-ghanem-almasarir-can-sue-saudi-arabia-for-pegasus-hacking>.

disappearance in Egypt following sale of their spyware to the Libyan and Egyptian governments.<sup>133</sup> In the United States, lawsuits filed by Meta, Google, and Apple are proceeding. The Meta lawsuit alleges that NSO Group illegally targeted 1,400 WhatsApp users, including lawyers, journalists, and human rights defenders.<sup>134</sup> Apple's lawsuit seeks a permanent injunction to ban NSO Group from using Apple software, services, or devices in the delivery of its targeted surveillance, in addition to redress for the NSO's violations of U.S. federal and state laws.<sup>135</sup>

Governments have begun to examine their relationship with NSO Group and other surveillance technology companies. In 2021, the United States added NSO Group and several other companies, including Israel-based Candiru, Russian company Positive Technologies, and Computer Security Initiative Consultancy in Singapore, to the Department of Commerce's Entity List for malicious cyber activities. The Entity List restricts these companies from purchasing technology from American companies because they pose a risk to the national security or foreign policy interests of the United States.<sup>136</sup> This action prohibits entity-list companies from purchasing business-critical software such as Microsoft and Amazon cloud services, for example. In a similar move, the European Parliament established a committee of inquiry in 2022 to investigate Pegasus

---

<sup>133</sup> International Federation for Human Rights, "Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies Executives Indicted," Press release, June 22, 2021, <https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa>.

<sup>134</sup> "NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware," accessed October 13, 2022, <https://news.bloomberglaw.com/privacy-and-data-security/nso-loses-latest-challenge-to-meta-lawsuit-over-whatsapp-spyware>.

<sup>135</sup> "Apple Sues NSO Group to Curb the Abuse of State-Sponsored Spyware," Apple Newsroom, accessed October 13, 2022, <https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/>.

<sup>136</sup> "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," U.S. Department of Commerce, accessed November 6, 2022, <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>.

and other surveillance technology to assess whether they have breached EU law and fundamental rights. The committee's report is expected in April 2024.<sup>137</sup>

---

<sup>137</sup> “EP Inquiry Committee for Pegasus and Other Spyware Launched | News | European Parliament,” April 19, 2022, <https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched>.

Part Three:

Chapter VI.

MENA Case Studies

As long as we store our lives on devices that have vulnerabilities, and surveillance companies can earn millions of dollars selling ways to exploit them, our defenses are limited, especially if a government decides it wants our data.

– Ben Hubbard<sup>138</sup>

Egypt, Lebanon, Morocco, Saudi Arabia, and the UAE represent five countries in the MENA region with distinct governance styles, constituencies, economies, and regional and international dynamics. They were selected given their historical use of spyware and because they represent two varieties of autocracies: Egypt and Lebanon are electoral autocracies, though at opposite ends of the scoring, and Morocco, Saudi Arabia, and UAE are closed autocracies. These factors facilitate a deeper analysis of the impact of spyware on human rights and any difference between more and less restrictive forms of governance since the Arab uprisings. Targeted individuals are listed under the country that allegedly targeted them. When the surveillance operator is unknown, this is noted, and they are listed under their country of origin.

---

<sup>138</sup> Ben Hubbard, “I Was Hacked. The Spyware Used Against Me Makes Us All Vulnerable.,” *The New York Times*, October 24, 2021, sec. Times Insider, <https://www.nytimes.com/2021/10/24/insider/hacking-nso-surveillance.html>.

## Chapter VII.

### Egypt

Before the Arab uprisings and the Egyptian revolution, the government of former Egyptian President Hosni Mubarak saw the internet as an engine of economic growth, while at the same time, its security services worked to curtail its use for sharing sensitive information. In 2009, this curtailment manifested as intimidation, legal procedures, and the physical surveillance of online users of interest.<sup>139</sup> Digital repression began to pick up in 2010 in response to internet-based activism before the November parliamentary elections in the form of online censorship: the websites of individuals who demanded political and democratic reforms were shut down and two popular Facebook groups that organized political protests were temporarily removed. The legal environment created a hostile environment for bloggers, some of whom were detained and tried before a military tribunal according to the Emergency Law. In 2010, Egypt also had its first court case in which a cybercafé owner was found liable for defamatory information posted online by someone visiting his café.<sup>140</sup>

Egypt's revolution in 2011 brought much hope as protests increased pressure until Mubarak, who had served as leader of Egypt of three decades, stepped down. That optimism was short-lived. Egypt's democracy score is worse today than it was in 2011, according to V-Dem analysis. Former army chief Abdul Fattah al-Sisi overthrew Muslim

---

<sup>139</sup> Freedom House, "Freedom on the Net, A Global Assessment of Internet and Digital Media" (Freedom House, April 1, 2009), [https://freedomhouse.org/sites/default/files/2020-02/FOTN\\_Freedom\\_OnThe%20Net\\_Full%20Report\\_2009.pdf](https://freedomhouse.org/sites/default/files/2020-02/FOTN_Freedom_OnThe%20Net_Full%20Report_2009.pdf).

<sup>140</sup> Sanja Kelly and Sarah Cook, "Freedom on the Net 2011, A Global Assessment of Internet and Digital Media" (Freedom House, April 18, 2011), 24, [https://freedomhouse.org/sites/default/files/2020-02/FOTN\\_2011\\_Summary\\_Findings.pdf](https://freedomhouse.org/sites/default/files/2020-02/FOTN_2011_Summary_Findings.pdf).

Brotherhood-affiliated Mohamed Morsi in 2013, the year after Morsi's election to the presidency. Egypt's 2014 constitution, which is more democratic than the previous one, has failed to prevent widespread torture by security forces and increased use of the death penalty. In 2018, the al-Sisi government began an internet crackdown that punished prominent figures for digital activism, blocked over 500 websites via internet censorship, and jailed online users for describing cases of sexual harassment online.<sup>141</sup> It is possible that one of the tools responsible for the identification of individuals of interest was surveillance technology sold by a company in Western Europe.

UAE purchased the surveillance product Cerebro from the French company Nexa/Advanced Middle East Systems, previously named Amesys, for Egypt to help it combat the Muslim Brotherhood. The company underwent a name change given revelations that Amesys had sold deep packet inspection technology to Muammar Qaddafi.<sup>142</sup> After the contract was signed in March 2014, Egypt's Ministry of Defense received the surveillance technology and regular training from Nexa technicians. While the technology permitted the real-time surveillance of targets, it is largely considered passive surveillance as it intercepts internet traffic. In 2018, one of the technicians noted in a report that "With hundreds of Muslim Brotherhood members condemned to death, [they didn't] feel comfortable" with how the technology was being used.<sup>143</sup> Four Amesys/Nexa executives were indicted in a Parisian court in 2021 for "complicity in torture in the Libyan portion of the investigation and complicity in torture and enforced

---

<sup>141</sup> Adrian Shahbaz, "Freedom on the Net 2018, The Rise of Digital Authoritarianism," 23.

<sup>142</sup> Paul Sonne And Margaret Coker, "Foreign Firms Helped Gadhafi Spy on Libyans," *The Wall Street Journal*, August 30, 2011, sec. World News, <http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html>.

<sup>143</sup> Olivier Tesquet, "Amesys: Egyptian trials and tribulations of a French digital arms dealer," July 5, 2017, <https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php>.

disappearance in the Egyptian portion. The two companies are accused of having supplied surveillance technology to authoritarian regimes in Libya and Egypt."<sup>144</sup>

Egypt's Freedom on the Net and Digital Repression Index scores corroborate the worsening human rights trends described above, as seen in Table 3.

Table 3. Egypt's Freedom on the Net and Digital Repression Index Scores

|                          | 2011 | 2021 | Trend |
|--------------------------|------|------|-------|
| Freedom on the Net       | 54   | 74   | ↑     |
| Digital Repression Index | 1.36 | 1.49 | ↑     |

*Freedom on the Net scores on a scale of 0-100, with 100=least free. The Digital Repression Index (DRI) scale is -5 to 5, with 0 representing the country-mean across variables for the year assessed. A positive score indicates that a country is performing above the mean across all DRI variables.*

During the interceding years from the revolution to present, Egypt's leaders also began using targeted smartphone surveillance. Egypt is known to have used at least three commercial spyware products sold by FinFisher, Cytrox, and Hacking Team. Two Egyptian human rights activists who broke into the headquarters of the State Security Investigations service in March 2011 found a proposal from FinFisher to sell its FinSpy product to the agency. It is unknown whether the agency proceeded with the purchase at that time, but eventual purchase was confirmed in 2015. FinSpy was confirmed to be used in the expansive civil society targeting operation known as Nile Phish in 2019 by Amnesty International,<sup>145</sup> though it is unknown whether FinSpy was used in the earlier

<sup>144</sup> International Federation for Human Rights, "Surveillance and Torture in Egypt and Libya," June 22, 2021.

<sup>145</sup> "German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed," Amnesty International, September 25, 2020, <https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/>.

stages of the phishing operation in which 43 individuals working for NGOs in Egypt were sentenced. Several NGOs spoke with Citizen Lab about the phishing campaign, including the Association for Freedom of Thought and Expression, Cairo Institute for Human Rights Studies, Egyptian Commission for Rights and Freedoms, Egyptian Initiative for Personal Rights, Nadeem Center for Rehabilitation of Victims of Violence, and Nazra for Feminist Studies, of which Mozn Hassan (listed below) is founder.<sup>146</sup>

Digital forensic analysis suggests that Egypt used another product, Cytrox's Predator spyware, in 2021 against two targets: former presidential candidate and opposition leader Ayman Nour (more below) and an unnamed journalist who is host of a popular news program. The spyware was installed via a single-click link sent via WhatsApp. Nour was also targeted at the same time with Pegasus spyware. While Citizen Lab attributes the Predator infiltration to Egypt, it was unable to determine who infected Nour's phone with Pegasus.<sup>147</sup>

Information from the Hacking Team leak in 2015 suggests that Egypt (potentially the Ministry of Defense) purchased RCS spyware from the Hacking Team for 58,000 Euro in January 2012<sup>148</sup> via a ministry-affiliated intermediary company called GNSE which was created to "enable e-business."<sup>149</sup> Citizen Lab lists Egypt as one of 21

---

<sup>146</sup> John Scott-Railton et al., "Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society" (University of Toronto, February 2, 2017), <https://citizenlab.ca/2017/02/nilephish-report/>.

<sup>147</sup> Bill Marczak et al., "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cyrox Mercenary Spyware" (University of Toronto, December 16, 2021), <https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/>.

<sup>148</sup> Ramy Raoof [@RamyRaoof], "From the #HackingTeam Leaks: Invoice to #Egypt - 58,000 EURO - January 2012. <http://T.Co/PgSJOWUwQq>," Tweet, *Twitter*, July 6, 2015, <https://twitter.com/RamyRaoof/status/618011320496050176>.

<sup>149</sup> Abir Ghattas, "For Arab Human Rights Defenders, Hacking Team Files Confirm Suspicions of State Surveillance," *Global Voices Advox* (blog), July 8, 2015, <https://advox.globalvoices.org/2015/07/08/for-arab-human-rights-defenders-hacking-team-files-confirm-suspicions-of-state-surveillance/>.

suspected RCS operators, and digital forensic analysis uncovered signals indicative of Hacking Team activity in Egypt from March to October 2013.<sup>150</sup>

Egypt also appears to have developed in-house spyware according to a report by Amnesty International and Check Point Software Technologies, a cybersecurity company. The spyware installed software enabling operators to read a target's files, emails, contacts, and to track their location using a sophisticated technique known as "OAuth Phishing" via third-party apps. The spyware's developers left artifacts in the code that led researchers to discover that sites affiliated with the spyware are connected to a server registered to Egypt's Ministry of Communications and Information Technology, and geographic coordinates in one of the third-party apps belonged to Egypt's spy agency, the General Intelligence Service. Check Point identified 33 victims in the attack that began in 2016.<sup>151</sup>

Victims of Egypt's targeted surveillance using Cytrox, NSO Group, phishing, and the in-house spyware are described below. Where possible, the surveillance tool used in the targeting is identified.

#### Ayman Nour

Ayman Nour is a leading Egyptian opposition figure living in exile in Turkey. He attempted to run for president twice: once against Mubarak in 2005, during which he was accused of forging signatures on petitions and jailed for five years; and again in 2012

---

<sup>150</sup> Bill Marczak et al., "Mapping Hacking Team's 'Untraceable' Spyware" (University of Toronto, February 17, 2014), <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>.

<sup>151</sup> Ronen Bergman and Declan Walsh, "Egypt Is Using Apps to Track and Target Its Citizens, Report Says," *The New York Times*, October 3, 2019, sec. World, <https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html>.

after the Arab uprisings, though the military council banned his candidature. He previously served in the Egyptian Parliament, founded the Ghad al-Thawra party, currently leads the Union of the Egyptian National Forces as its president, and owns an opposition satellite channel. Nour fled Egypt in 2013 after opposing al-Sisi's military coup and remains critical of the "oppressive military regime."<sup>152</sup>

In 2021, Nour became suspicious that he had been targeted with spyware when he observed that his iPhone was "running hot"<sup>153</sup> and "was being jammed or stopped working." At the time, he was actively hosting meetings with his political opposition group.<sup>154</sup> His smartphone's behavior was familiar, as he believed he had been hacked "long ago" after telephone calls from his office and a private picture of him cuddling a puppy on his bed were leaked online.<sup>155</sup> A Citizen Lab investigation confirmed the presence of both Predator and Pegasus spyware on his iPhone, with infections in March and June 2021, respectively.<sup>156</sup> The Predator infection was traced to Egypt, while the Pegasus infection is believed to be a result of Saudi Arabian or Emirati targeting;<sup>157</sup> The Israeli newspaper Haaretz maintains a continuously updated list of confirmed Pegasus victims and suggests that Nour was targeted by the latter.<sup>158</sup>

---

<sup>152</sup> Marczak et al., "Pegasus vs. Predator."

<sup>153</sup> Ronald Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy."

<sup>154</sup> Thomas Brewster, "Two Spyware, One iPhone: A Khashoggi Murder Trial Witness Fears He Was Hacked By Rival Surveillance Tools," *Forbes*, accessed December 23, 2022, <https://www.forbes.com/sites/thomasbrewster/2021/12/16/nso-and-cytrox-spyware-allegedly-hacks-iphone-of-egypt-opposition-politician-in-exile/>.

<sup>155</sup> Brewster.

<sup>156</sup> Marczak et al., "Pegasus vs. Predator."

<sup>157</sup> Ronald Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy."

<sup>158</sup> Omer Benjakob, "The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware - Tech News - Haaretz.Com," *Haaretz*, April 5, 2022, <https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000>.

Nour fears that the targeting of his smartphone means that governments want him dead. He also points to a television commenter in Egypt who has called for his assassination. As a longtime friend of Saudi dissident Khashoggi who was murdered in 2019, Nour appeared as a witness in a Turkish trial against Khashoggi's killers in 2020. When asked by Forbes whether their relationship was the reason he was targeted, Nour demurred but said "...there is clear evidence that was published about our friendship" which lasted 35 years. In the trial, he gave evidence that Khashoggi had told him that Saud al-Qahtani, Crown Prince Mohammed bin Salman's aide, had personally threatened him.<sup>159</sup>

Nour currently lives in Turkey and faces travel restrictions given his expired Egyptian passport. He filed a lawsuit to compel the Ministry of Foreign Affairs to renew his passport but lost the case in June 2021, as the Supreme Administrative Court ruled that the ministry did not have to renew it.<sup>160</sup>

### Mozn Hassan

Mozn Hassan is a feminist and a human rights defender. She founded the NGO Nazra for Feminist Studies in 2007. Nazra supports women engaged in the political sphere, especially women human rights defenders, who are targeted with violence and discrimination due to their activities. One of the organization's top priorities is to end sexual violence against women since this violence threatens women's right to

---

<sup>159</sup> Brewster, "Two Spyware, One iPhone."

<sup>160</sup> Bureau of Democracy, Human Rights, and Labor, "2021 Country Reports on Human Rights Practices: Egypt" (U.S. Department of State, 2021), <https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/egypt/>.

participate.<sup>161</sup> Nazra took an active role in documenting the sexual assaults of women participating in the Egyptian revolution of 2011, and it ensured that these victims had access to medical, psychological, and legal support.<sup>162</sup> In addition to Nazra's initiatives, Hassan successfully added women's rights to the 2014 Constitution of Egypt and helped introduce new and expand existing sex crime laws to safeguard women. In recognition of her achievements, she was awarded the Global Fund for Women's inaugural Charlotte Bunch Human Rights Award in 2013 and the Right Livelihood Award in 2016.<sup>163</sup>

In March 2016, Hassan was in speaking at the UN Commission on the Status of Women in New York when she received a summons from the Egyptian police. She returned to Egypt and was charged with violating the law banning foreign funding or aid to Egyptian NGOs as part of case 173/2011. Case 173 is often referred to as the "case on foreign funding of civil society." In July 2011, the Minister of Justice set up a fact-finding committee at the behest of the cabinet. The committee produced a report used by the prosecution.<sup>164</sup> The first wave of criminal cases resulted in 43 convictions of Egyptian and foreign NGO staffers in 2013. A second wave of criminal proceedings began in 2014. According to a copy of the fact-finding committee's report, which was leaked in 2015, the prosecution was targeting a list of 37 Egyptian NGOs.<sup>165</sup>

---

<sup>161</sup> "About Us | Nazra for Feminist Studies," accessed December 27, 2022, <https://nazra.org/en/about-us>.

<sup>162</sup> "Mozn Hassan/ Nazra for Feminist Studies Biography" (The Right Livelihood Award), accessed December 27, 2022, <https://rightlivelihood.org/app/uploads/2016/09/MoznHassanNazra.pdf>.

<sup>163</sup> "Mozn Hassan/ Nazra for Feminist Studies Biography."

<sup>164</sup> "Background on Case No. 173 - the 'Foreign Funding Case' | Egyptian Initiative for Personal Rights," accessed December 27, 2022, <https://eipr.org/en/press/2016/03/background-case-no-173-%E2%80%9Cforeign-funding-case%E2%80%9D>.

<sup>165</sup> "Background on Case No. 173 - the 'Foreign Funding Case' | Egyptian Initiative for Personal Rights."

Hassan was summoned as part of the second wave and appeared in court in March 2016.<sup>166</sup> In addition to the charge of foreign funding, Hassan was charged with “inciting and calling for the irresponsible liberation of women,” in a direct attack on her activism.<sup>167</sup> The charge was tantamount to being a prostitute, Hassan said, and “[it] made me wonder what [evidence] they have against me.”<sup>168</sup> In January 2017, Hassan’s assets and the assets of Nazra were frozen, and she was released on bail and placed under house arrest. Following an appeal, the charges against Hassan were dropped due to insufficient evidence and her case was closed in October 2021.<sup>169</sup>

Nazra for Feminist Studies was not only a target of prosecution. According to analysis by Citizen Lab, Nazra was one of many Egyptian civil society organizations targeted by a large-scale phishing campaign called Nile Phish. Phishing is a tactic to steal personal information through deception, such as passwords or secret codes. In the initial phase of Nile Phish, messages were sent that referred to the crackdown on Egyptian civil society and case 173. The messages were timely and well targeted. They typically purported to share a Google or Dropbox document with more information that required entering a password on a fake site, where the sensitive data was captured. Phase two of the phishing campaign involved a generic yet personalized message emphasizing account security issues, such as failed login attempts, which also required re-entering a password. Nazra was phished using the phase 2 approach of a compromised Google email account.

---

<sup>166</sup> Liz Ford, “Egyptian Feminist Leader Mozn Hassan Resolute in Face of Official Investigation,” *The Guardian*, March 31, 2016, sec. Global development, <https://www.theguardian.com/global-development/2016/mar/31/egyptian-feminist-leader-mozn-hassan-resolute-investigation>.

<sup>167</sup> “In Welcome Development, Egypt Drops Charges against Mozn Hassan,” Right Livelihood, accessed December 26, 2022, <https://rightlivelihood.org/news/in-welcome-development-egypt-drops-charges-against-mozn-hassan/>.

<sup>168</sup> Mozn Hassan, Interview by author, December 8, 2022.

<sup>169</sup> “Charges against Mozn Hassan Dropped and Case Closed,” Front Line Defenders, October 28, 2021, <https://www.frontlinedefenders.org/en/case/charges-against-mozn-hassan-dropped-and-case-closed>.

By luring targets to share passwords, phishing operators can quickly download troves of data from email and online accounts.<sup>170</sup>

Hassan confirmed to the author that she had been digitally targeted. Prosecutors had predominantly used her organization's Facebook posts or Tweets as evidence in her trial. Even preceding the trial, Hassan said she had good digital hygiene and was careful with her digital footprint. Similarly, her organization's media strategy was "cautious" and did not allow retweeting or the removal of comments on social media posts. She and her team members were also meticulous in the care they took to store data, given the nature of their work helping victims of sexual assault: identities and testimonies were obscured so that even others working in Egypt's small civil society space could not identify the victims. She said that victims were never named online.

At one point, Hassan became aware that she was under digital attack by the Egyptian government, both on her smartphone and a desktop computer, and she changed her account passwords 40 times in one day in an attempt to keep her organization's data safe. The incident caused her to have a panic attack. Among civil society colleagues, "I was considered the activist with the highest number of digital attacks," she said. She believes she was heavily targeted because she does not share much information online, which may lead people to believe that she is hiding a lot of secrets.<sup>171</sup>

Hassan said that as a feminist working in the Middle East, she has always been subjected to surveillance and scrutiny because feminism eschews traditional societal roles and is seen as immoral. She knows colleagues who have spent years in prison for a Facebook status or tweet. As a result of these collective experiences and her own, Hassan

---

<sup>170</sup> Scott-Railton et al., "Nile Phish."

<sup>171</sup> Mozn Hassan, Interview by author.

mainly avoids social media, she self-censors to avoid harassment, and, when outside her home, she constantly scans her surroundings to avoid dangerous situations and locations with cameras. This heightened state of vigilance is “so draining and can make you collapse” Hassan admitted.<sup>172</sup>

Hassan has tried to keep the repercussions of her activism contained with limited success. While she does not share information with her niece for fear that she would be targeted and she kept the focus on herself during the trial to avoid the implication of Nazra colleagues, others in her circle have been affected. Despite her best efforts, a smear campaign in the media created pressure on Hassan’s mother by her peers, who criticized her raising of Hassan. Her mother had always been supportive of Hassan’s beliefs, “even if she doesn’t agree with all of them,” and the pain this caused her mother hurt Mozn deeply. “All of these things change you,” she said.<sup>173</sup>

#### Hassan Nafaa

Hassan Nafaa is a political scientist at Cairo University with a long history of political activism and commentary who was targeted with in-house spyware operated by the General Intelligence Service.<sup>174</sup> He helped a retired general run against al-Sisi in 2018 in an unsuccessful bid and was also a prolific user of Twitter. In personal tweets, he urged Egypt political stakeholders to prepare for a “post-Sisi era”:

I have no doubt that the continuation of Sisi's absolute rule will lead to disaster, and that Egypt's interest requires his departure today before tomorrow, but he will only leave with public pressure from the street. At

---

<sup>172</sup> Mozn Hassan.

<sup>173</sup> Mozn Hassan.

<sup>174</sup> Bergman and Walsh, “Egypt Is Using Apps to Track and Target Its Citizens, Report Says.”

the same time, we should choose the least expensive ways to guarantee the transfer of power to honest hands, and to avoid a scenario of chaos.<sup>175</sup>

Nafaa often provided memorable quotes to the media as well. He told the news site Arabi21 in July 2018 that “al-Sisi’s regime is weak and will not stand up to the accumulated anger.”<sup>176</sup> Days before his arrest on September 25, 2019, he told AFP that “Sisi’s desired image as ‘Egypt’s savior from Muslim Brotherhood rule’ has been completely dismantled.”<sup>177</sup>

Nafaa’s arrest followed rare anti-government protests days prior; he was held with other critics of al-Sisi who had been targeted following a crackdown. In March 2020, the State Security Prosecution released Nafaa along with 14 others.<sup>178</sup> While he has not conducted an interview in English following his detention, evidence from Check Point suggests one of the main purposes of the spyware is to pinpoint a target’s location in real-time via their smartphone. Nafaa was likely arrested because of this targeting, significantly curtailing his human rights.

### Khaled Dawoud

Khaled Dawoud is the assistant editor of Al-Ahram Weekly, former president of the secular Constitution Party, professor of journalism at the American University of Cairo, and a prominent al-Sisi critic. He was targeted with Egyptian spyware and arrested

---

<sup>175</sup> MEE staff, “Egypt Arrests Prominent Critics of Sisi with 1,400 Detained since Friday Protests,” Middle East Eye, September 25, 2019, <http://www.middleeasteye.net/news/egypt-arrests-prominent-political-scientists-critical-sisi>.

<sup>176</sup> Taha Al-Esawi, “‘Al-Sisi’s Regime Is Weak and Will Not Stand up to the Accumulated Anger,’” *Middle East Monitor* (blog), July 12, 2018, <https://www.middleeastmonitor.com/20180712-al-sisi-regime-is-weak-and-will-not-stand-up-to-the-accumulated-anger/>.

<sup>177</sup> Hamza Guessous, “Egyptian Authorities Arrest More than 1,000 Anti-Corruption Protesters,” Morocco World News, <https://www.moroccoworldnews.com/>, September 25, 2019, <https://www.moroccoworldnews.com/2019/09/283389/egyptian-authorities-anti-corruption-protesters>.

<sup>178</sup> Bureau of Democracy, Human Rights, and Labor, “2021 Country Reports on Human Rights Practices: Egypt.”

on September 24, 2019, in the same crackdown as Hassan Nafaa.<sup>179</sup> Dawoud was charged with “assisting a terrorist group in achieving its goals while knowing its targets,” which he called a “cliché” charge used under al-Sisi to keep political prisoners in pre-trial for up to two years. He was held for 19 months and released on April 14, 2021. In an interview with the Center for Strategic and International Studies two weeks after his release, he said that prosecutors never named the terrorist organization that he allegedly assisted. He was also charged with “spreading false news and abuse of social media,” a charge he also dismissed out of hand given his familiarity and disdain for “fake news” as a journalism professor.<sup>180</sup>

Dawoud wrote memoirs about his 19 months in Tora Prison in which he shared a six-by-nine-foot cell with Hassan Nafaa and another political prisoner, described in a Foreign Policy article:

...[T]hey were each allowed only one “dirty prison suit” that made their skin itch and were made to walk barefoot around the prison and to the prosecution hearing session. Dawoud described how they had to eat from plastic bags, in the absence of spoons or utensils, and improvise knives made from tuna can tops. Soap was scarce and hot water almost nonexistent. The cell was poorly ventilated and without sunlight.

There was no laundry, and inmates washed their clothes in primitive ways and hung them inside their cells, which contributed to the prison’s sickening dampness. Exercise was mostly limited to walking in the prison yard for 30 minutes a day and could be denied at the whim of the prison guards.<sup>181</sup>

---

<sup>179</sup> Bergman and Walsh, “Egypt Is Using Apps to Track and Target Its Citizens, Report Says.”

<sup>180</sup> Khaled Dawoud, Journalism and Politics in Egypt, interview by Jon Alterman, May 4, 2021, <https://www.csis.org/analysis/journalism-and-politics-egypt>.

<sup>181</sup> Amr Magdi, “Al-Sisi Is Leaving the Sick to Suffer in Egypt’s Prisons,” *Human Rights Watch*, September 1, 2021, <https://www.hrw.org/news/2021/09/01/al-sisi-leaving-sick-suffer-egypts-prisons>; Amr Magdi, “Sisi Is Leaving the Sick to Suffer in Egypt’s Prisons,” *Foreign Policy*, September 1, 2021, <https://foreignpolicy.com/2021/09/01/sisi-egypt-prisoners-health-human-rights-abu-al-fotouh/>.

Several weeks before he was released, Dawoud said that Egyptian officials visited him in prison to deliver a message: they hoped he had learned from his experience, and that he would "...try to kind of adopt a middle ground...[and] take care of [his] family." Reflecting on whether he would continue to speak out, he said he would continue to do so but might "watch [his] language a little bit...[because] prison is a very tough, very unhappy experience."<sup>182</sup>

### Shady Al-Ghazaly Harb

Dr. Shady Al-Ghazaly Harb is a surgeon and opposition activist who was detained in May 2018 for criticizing the government on Twitter. Like Hassan Nafaa and Khaled Dawoud, he was targeted by Egyptian spyware and spent 19 months in prison ostensibly for terrorism,<sup>183</sup> a charge that allowed authorities to keep him for up to two years in pre-detention, as well as charges for insulting the president and spreading false news. Al-Ghazaly Harb spent part of his detention in solitary confinement, and, similar to the accounts of Nafaa and Dawoud, his questions to prosecutors about which terrorist organization he allegedly supported went unanswered.<sup>184</sup>

Al-Ghazaly Harb attempted to return to Cairo University as assistant professor and faculty member of the Faculty of Medicine in March 2020 after his release, but the university denied him the role. He filed a lawsuit and won the right to return in July 2022

---

<sup>182</sup> Khaled Dawoud, *Journalism and Politics in Egypt*.

<sup>183</sup> Bergman and Walsh, "Egypt Is Using Apps to Track and Target Its Citizens, Report Says."

<sup>184</sup> "As It Happens," *As It Happens* (CBC Radio, January 25, 2021), <https://www.cbc.ca/radio/asithappens/as-it-happens-monday-edition-1.5886768/january-25-2021-episode-transcript-1.5888366>.

as no final verdict had been found in his legal case (No. 621 of 2018 Supreme State Security).<sup>185</sup>

---

<sup>185</sup> “Administrative Judiciary Obliges Cairo University to Return Dr. Shadi Al-Ghazali Harb to His Work as an Assistant Professor of Medicine in Al-Qasr Al-Ainy,” Egyptian Center for Economic & Social Rights, July 20, 2022, <https://ecesr.org/en/2022/07/20/administrative-judiciary-obliges-cairo-university-to-return-dr-shadi-al-ghazali-harb-to-his-work-as-an-assistant-professor-of-medicine-in-al-qasr-al-ainy/>.

## Chapter VIII.

### Lebanon

According to Reporters Without Borders in 2010, Lebanon was considered a “bastion of free speech” with one of the region’s freest press index scores (which factors in internet restrictions). However, there were signs that internet freedom was eroding that same year. A blogger was arrested for writing articles critical of the president and the army in March; he was told to stick to writing poetry instead of politics. Another four online users were arrested for posting comments on Facebook about President Michel Suleiman in June and July.<sup>186</sup>

In the years since the Arab uprisings, the Lebanese government has undertaken various forms of digital repression, though at decidedly lower levels than the other four case study countries. From August 2014 to September 2017, the government cut broadband service in the northeastern town of Arsal to stem clashes between the military and extremist militants. Aarsal is in the Bekaa Valley near Syria and is host to many Syrian refugees.<sup>187</sup> Lebanese mobile service provider Alfa purchased passive surveillance in the form of Sandvine’s deep packet inspection (DPI) software in 2015 and upgraded to a newer DPI system produced by NEXIUS in 2018.<sup>188</sup>

There were 36 violations of freedom of expression online in 2018, compared to just 12 in 2017. The Cybercrime Bureau brought in online users for multiday

---

<sup>186</sup> Josh Wood, “Lebanon Cracks Down on Internet Freedom,” *The New York Times*, November 3, 2010, <https://www.nytimes.com/2010/11/04/world/middleeast/04iht-m04m1leblog.html>.

<sup>187</sup> “Lebanon: Freedom on the Net 2021 Country Report,” Freedom House, accessed January 10, 2023, <https://freedomhouse.org/country/lebanon/freedom-net/2021>.

<sup>188</sup> “Lebanon: Freedom on the Net 2022 Country Report,” Freedom House, accessed January 10, 2023, <https://freedomhouse.org/country/lebanon/freedom-net/2022>.

interrogations where they pressured the social media users to apologize for posts, remove content the bureau considered controversial, and forced them to sign letters confirming that they would curb their behavior. Some cases proceeded to trial though few are publicly known.<sup>189</sup> During the 2019 protests which some call the country’s second “Arab Spring,” Lebanese officials also engaged in the persecution of online users when Internal Security Forces infiltrated WhatsApp groups created by protestors and arrested them.<sup>190</sup>

However, compared to its scores a decade ago, Lebanon’s level of digital repression has decreased while freedom of the internet has increased, according to scores shown in Table 4.

Table 4. Lebanon’s Freedom on the Net and Digital Repression Index Scores

|                          | 2011 | 2013 | 2021 | Trend |
|--------------------------|------|------|------|-------|
| Freedom on the Net       | --*  | 55   | 51   | ↓     |
| Digital Repression Index | 0.88 | --   | 0.65 | ↓     |

*\*Freedom on the Net (FOTN) did not profile Lebanon in 2011; the country was first included in the report in 2013. FOTN scores on a scale of 0-100, with 100=least free. The Digital Repression Index (DRI) scale is -5 to 5, with 0 representing the country-mean across variables for the year assessed. A positive score indicates that a country is performing above the mean across all DRI variables.*

In the domain of targeted surveillance, Lebanon purchased at least two commercial products from private companies: FinFisher and Hacking Team. Citizen Lab found evidence that the Lebanese government used FinFisher in 2014, according to a

<sup>189</sup> “Lebanon: Freedom on the Net 2019 Country Report,” Freedom House, accessed January 11, 2023, <https://freedomhouse.org/country/lebanon/freedom-net/2019>.

<sup>190</sup> “Lebanon.”

report released in 2015. The primary operators were the General Directorate of General Security and Internal Security Forces (ISF).<sup>191</sup>

In the leak of Hacking Team emails in July 2015, documents were discovered that confirmed that the Lebanese Army and the Cybercrime Bureau had purchased Hacking Team's RCS spyware. Leaked documents also indicated that ISF and General Security Directorate were also interested in the spyware and were in email correspondence with the Hacking Team. A demo to the ISF showed that targeted devices were successfully infected through a backdoor in the Angry Birds app. Activists and bloggers who were summoned multiple times to appear before the Cybercrime Bureau suspect that authorities used Hacking Team products to target and monitor them.<sup>192</sup>

Lebanon has also developed its own in-country spyware which digital forensic analysts have named Dark Caracal.<sup>193</sup> This spyware is believed to be administered out of the General Directorate of the General Security headquarters in Beirut, with its first campaign launching in 2012. The spyware, which relies on traditional hacking and phishing techniques, exfiltrated hundreds of gigabytes of data in over 21 countries, with thousands of victims. The data extracted from smartphones (primarily Android) and desktops includes documents, call recordings, audio recordings, secure messaging client content, contact information, text messages, photos, and account data. Artifacts suggest

---

<sup>191</sup> Bill Marczak et al., "Pay No Attention to the Server Behind the Proxy," Citizen Lab (University of Toronto, October 15, 2015), <https://tspace.library.utoronto.ca/bitstream/1807/97784/1/Report%2364---finfisher.pdf>.

<sup>192</sup> Zalfa Quino, "#HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices," *Global Voices Advox* (blog), July 28, 2015, <https://advox.globalvoices.org/2015/07/28/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/>.

<sup>193</sup> "Lebanon."

that Dark Caracal at times used FinFisher and made extensive use of Windows malware. The spyware is believed to still be in operation today.<sup>194</sup>

Lebanon is not believed to be a Pegasus operator, though it has a sizable number of spyware infections within its borders. The Lebanese online magazine Daraj stated that over 300 Lebanese phone numbers were identified on a list of 50,000 numbers as possible Pegasus targets. Daraj is a member of the Pegasus Project connected to the media nonprofit Forbidden Stories based in Paris.

Le Monde, another Pegasus Project partner, attributed the targeting of top Lebanese officials to Saudi Arabia and the UAE. President Michel Aoun was the senior-most Lebanese official on the list and reportedly a Saudi target. Other notable names included former Prime Minister Saad Hariri (targeted by Saudi Arabia); former Minister of Foreign Affairs Gibran Bassil; Abbass Ibrahim, head of General Security; Central Bank Governor Riad Salamé (by Saudi Arabia); and Hezbollah officials Wafik Safa, Ali Fayyad, and Hassan Fadlallah (by the UAE); among many ministers, ambassadors, and journalists.<sup>195</sup> Hariri may have been targeted twice as Emirati officials wanted proof that an update to Pegasus spyware was worth the increased price by requesting that NSO obtain secret recordings of the emir of Qatar, Saudi Prince Mutaib bin Abdullah, and Hariri. This disclosure became known from the leak of emails that were part of two lawsuits filed in 2018.<sup>196</sup> Of note, none of the individuals mentioned above have publicly

---

<sup>194</sup> “Dark Caracal: Cyber-Espionage at a Global Scale” (Lookout, Electronic Frontier Foundation, January 18, 2018), [https://info.lookout.com/rs/051-ESQ-475/images/Lookout\\_Dark-Caracal\\_srr\\_20180118\\_us\\_v.1.0.pdf](https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf).

<sup>195</sup> Benjamin Barthe, “Au Liban, les monarchies du Golfe surveillent autant leurs amis que leurs ennemis,” *Le Monde.fr*, July 19, 2021, [https://www.lemonde.fr/projet-pegasus/article/2021/07/19/au-liban-les-monarchies-du-golfe-surveillent-autant-leurs-amis-que-leurs-ennemis\\_6088812\\_6088648.html](https://www.lemonde.fr/projet-pegasus/article/2021/07/19/au-liban-les-monarchies-du-golfe-surveillent-autant-leurs-amis-que-leurs-ennemis_6088812_6088648.html).

<sup>196</sup> David D. Kirkpatrick and Azam Ahmed, “Hacking a Prince, an Emir and a Journalist to Impress a Client,” *The New York Times*, August 31, 2018, sec. World, <https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html>.

confirmed that they were successfully targeted by Pegasus by submitting to forensic analysis.<sup>197</sup>

Very few victims of confirmed spyware attacks residing in Lebanon have publicly stepped forward. While it is the author's intent to profile victims targeted by Lebanon to illustrate the impact of governmental decisions and actions, the targeting of Lama Fakhri has not been attributed to a specific country. Fakhri said that General Security visited her following news of the attack to check on her wellbeing.<sup>198</sup> Ben Hubbard was based in Beirut when he was targeted, but his attack has been attributed to Saudi Arabia and his story appears in the Saudi chapter. Ghada Oueiss is a Lebanese citizen and maintains a domicile in Lebanon, but her attack has also been attributed to a Gulf state; she is also included in the Saudi chapter.

Fakhri described several potential reasons why victims may be reluctant to publicize their targeting: they may not feel safe stepping forward; they may feel undermined in their work or mission, especially if it involved building trust and the targeting places others at risk; or they may feel that managing the fallout from the targeting is too burdensome. She said that after publicizing her targeting, at least one other victim confided to her that she too had been the victim of spyware and felt very intimidated by the attack. This person has chosen not to publicly disclose it.<sup>199</sup>

Lama Fakhri

---

<sup>197</sup> Benjamin Barthe, "Au Liban, les monarchies du Golfe surveillent autant leurs amis que leurs ennemis."

<sup>198</sup> Lama Fakhri, Interview by author, January 18, 2023.

<sup>199</sup> Lama Fakhri.

Lama Fakih is the director of Human Rights Watch's Crisis and Conflict Division and is based in Lebanon. She has worked in various roles for Human Rights Watch and Amnesty International since after the start of the Arab uprisings in 2011. She was shocked to learn that her iPhone had been targeted with Pegasus. She became aware when Apple sent her an email and an iMessage stating that she was the target of a state-sponsored attack on November 23 and November 24, 2021. Forensic analysis confirmed that Fakih's new and old iPhones had been infected at least five times between April and August 2022 using "zero-click" attacks, meaning that the spyware installed without Fakih's knowledge or any action on her part. Amnesty International's Security Lab agreed with Human Rights Watch's findings.<sup>200</sup> Fakih was not on the Pegasus list of numbers published in 2021.

At the time of targeting, Fakih was working on crises related to hostilities between Israel and armed groups in Gaza and an investigation into the explosion at the Beirut port for which Lebanese officials are culpable. While the targeting occurred on personal phones, Fakih said she always had the phones with her. She declined to name the country that carried out the attack but does not think that the Lebanese government is responsible. She noted that Lebanon has other low-tech options at their disposal, such as wiretapping and human surveillance, and would not need to resort to spyware to surveil targets of interest residing in country.<sup>201</sup>

Human Rights Watch reached out to NSO Group in January 2022 with a complaint and details of the attack on Fakih's phones, and the company promised an

---

<sup>200</sup> Lama Fakih, Interview: Phone of HRW Director Attacked Using Pegasus Spyware, January 26, 2022, <https://www.hrw.org/news/2022/01/26/interview-phone-hrw-director-attacked-using-pegasus-spyware>.

<sup>201</sup> Lama Fakih, Interview by author.

“initial assessment.” In June 2022, NSO’s Vice President for Compliance, Chaim Gelfand, followed up with an ambiguous, perfunctory answer: “This issue has been investigated to the best of our ability based on the information provided to us. We have not seen evidence that Ms. Fakih’s number, provided below, had been targeted using the Pegasus system by our existing customer’s [sic].” The response could be interpreted one of two ways: either the government that targeted her no longer has a contract, or NSO has incomplete information because its investigations rely on client cooperation.<sup>202</sup>

Since the attack, Fakih keeps “barebones” information on her smartphone and does not have it linked to her work account. She is not aware of others being targeted or the use of information gleaned from her phones in the aftermath of the attack. She is therefore one of the few victims targeted solely with spyware without the usual accompaniment of other forms of digital repression.

As a dual U.S.-Lebanese citizen working for a mainstream human rights organization, Fakih decided to publicize the attack to show how common it is; that spyware surveillance is not limited to counterterrorism or criminal targets as companies like NSO state; and that no one is immune. She described the human rights consequences as follows:

It is hard to inventory, or quantify, just how harmful these attacks, and illegal surveillance more broadly, are from a human rights perspective. Yes, they violate our right to privacy, but the harms are much more nefarious and far reaching than that. In addition to stripping us of our privacy, these attacks undermine our freedom of expression and association. They undermine our ability to communicate freely, without fear of being listened in on. They threaten our personal security and that of

---

<sup>202</sup> Deborah Brown, “NSO Fails to Explain Targeting of Human Rights Watch Employee,” *Human Rights Watch* (blog), July 15, 2022, <https://www.hrw.org/news/2022/07/15/nso-fails-explain-targeting-human-rights-watch-employee>.

the people we know. But this is just on the individual level. In the aggregate, these attacks threaten all of our rights.<sup>203</sup>

---

<sup>203</sup> Lama Fakih, Interview.

## Chapter IX.

### Morocco

Heading into the Arab uprisings in late 2010-early 2011, Morocco was a closed autocracy and considered partly-free according to Freedom House, though there was concern that power was concentrating in the hands of King Mohammed VI. There were also concern over increased harassment of opposition critics and the decline of political rights,<sup>204</sup> an ever-increasing gap between the rich and poor, and compounding grievances surrounding governance and human rights. On the heels of Tunisia and Egypt's uprisings, Moroccans took to the streets on February 20, 2011, and Mohamed VI responded quickly by offering early elections, limited constitutional reforms, and a constitutional referendum, though none substantially changed the system.<sup>205</sup> In Western Sahara, which Morocco administers, the situation was tense following the dismantling of a protest camp called Gdeim Izik in October 2010 and the military trial of 21 Sahrawi prisoners, though no new sustained protests materialized in 2011.

Compared to Egypt, Saudi Arabia, and UAE in 2011, digital repression was lower in Morocco and nearly comparable to that of Lebanon. Nevertheless, there were notable events over the past decade. Morocco reportedly purchased internet monitoring technology called "Eagle" in 2011 from the French company Amesys, which sold similar technology to Libya. The UN Secretary General's annual report to the UN Security Council on the UN peacekeeping mission, MINURSO, mentioned in 2012 that "There

---

<sup>204</sup> "Freedom in the World 2010" (Freedom House, 2010), [https://freedomhouse.org/sites/default/files/2020-03/FIW\\_2010\\_Complete\\_Book\\_Scan.pdf](https://freedomhouse.org/sites/default/files/2020-03/FIW_2010_Complete_Book_Scan.pdf).

<sup>205</sup> Deborah Amos, "In Morocco, The Arab Spring's Mixed Bounty," *NPR*, February 7, 2012, sec. Africa, <https://www.npr.org/2012/02/07/146526685/in-morocco-the-arab-springs-mixed-bounty>.

were ... indications that the confidentiality of communications between MINURSO headquarters and New York was, at least on occasion, compromised.”<sup>206</sup> It is unclear whether Eagle was used in this instance. In 2015, the Swiss government revealed that Morocco had purchased technology from a Swiss company in 2013 or 2014 to intercept or jam mobile telecommunication equipment.<sup>207</sup> Additionally, it was also discovered that UK-based BAE Systems also sold mass surveillance technology to Morocco and five other Middle Eastern governments “in recent years,” according to The Guardian. The technology allows Morocco to “...collect, catalogue and analyze millions of people’s electronic communications,” including at a countrywide level, if desired.<sup>208</sup>

The persecution of online users also features in many accounts of Morocco’s digital repression. In 2013, Freedom House began to state in Freedom of the Net annual reports that Moroccan authorities were occasionally disrupting websites and internet platforms, and that bloggers and other online users were being arrested for content considered offensive.<sup>209</sup> The country’s internet freedom score worsened as the state carried out several high-profile arrests of online journalists and activists connected to coverage of the Hirak el-Rif social justice protests in 2016 and 2017.<sup>210</sup> In addition, the online publication of a report about surveillance by Privacy International and Morocco’s Digital Rights Association led the Ministry of Interior to announce a criminal complaint

---

<sup>206</sup> Louis Charbonneau, “Morocco May Have Spied on Western Sahara Mission: UN,” *Reuters*, April 12, 2012, sec. Emerging Markets, <https://www.reuters.com/article/us-sahara-un-idUSBRE83B0IL20120412>.

<sup>207</sup> Privacy International, “State of Privacy Morocco” (Privacy International, January 26, 2019), <http://privacyinternational.org/state-privacy/1007/state-privacy-morocco>.

<sup>208</sup> Rob Evans, “BAE ‘Secretly Sold Mass Surveillance Technology to Repressive Regimes,’” *The Guardian*, June 14, 2017, sec. Business, <https://www.theguardian.com/business/2017/jun/15/bae-mass-surveillance-technology-repressive-regimes>.

<sup>209</sup> Freedom House, *Freedom in the World 2013: The Annual Survey of Political Rights and Civil Liberties*, Freedom in the World (Lanham, MD: Rowman & Littlefield Publishers, 2013), 482.

<sup>210</sup> Freedom House, “Morocco: Freedom on the Net 2018 Country Report,” Freedom on the Net (Freedom House, 2018), <https://freedomhouse.org/country/morocco/freedom-net/2018>.

in 2018 against “persons who distributed a report containing grave accusations about spying practices.”<sup>211</sup> The report details four Moroccans placed under various forms of surveillance and the effect it had on their lives and their families’ lives. Privacy International no longer keeps the report on its website though it is available through web archiving.<sup>212</sup> In late 2020, three Moroccan security agencies issued a joint statement that they would pursue charges against Moroccans living abroad that spread false or defamatory information. It was widely believed to be targeted at YouTube creators and seemingly confirmed with the arrest of Moroccan-American citizen Chafik Omerani for posting “contemptuous” YouTube videos profiling constitutional institutions, bodies, and public officials.<sup>213</sup>

Morocco’s Freedom on the Net and Digital Repression Index scores support the trends identified above, as illustrated in Table 5.

Table 5. Morocco’s Freedom on the Net and Digital Repression Index Scores

|                          | 2011 | 2013 | 2021 | Trend |
|--------------------------|------|------|------|-------|
| Freedom on the Net       | --*  | 42   | 47   | ↑     |
| Digital Repression Index | 0.91 | --   | 0.97 | ↑     |

*\*Freedom on the Net (FOTN) did not profile Morocco in 2011; the country was first included in the report in 2013. FOTN scores on a scale of 0-100, with 100=least free. The Digital Repression Index (DRI) scale is -5 to 5, with 0 representing the country-mean across variables for the year assessed. A positive score indicates that a country is performing above the mean across all DRI variables.*

<sup>211</sup> Freedom House.

<sup>212</sup> “Their Eyes on Me: Stories of Surveillance in Morocco” (Privacy International, 2014), [https://web.archive.org/web/20170417194607/https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English\\_0.pdf](https://web.archive.org/web/20170417194607/https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf).

<sup>213</sup> Freedom House, “Morocco: Freedom in the World 2021 Country Report,” Freedom House, accessed August 7, 2021, <https://freedomhouse.org/country/morocco/freedom-world/2021>.

Morocco is a known consumer of commercially produced targeted surveillance technology. As discussed in the Privacy International report, Morocco is believed to have purchased products from the Hacking Team, in addition to separate reports of the government's use of FinFisher and NSO Group spyware. According to leaked Hacking Team documents, Morocco was Hacking Team's biggest customer,<sup>214</sup> with the High Council for National Defense and Directory of Territorial Surveillance signing contracts for its RCS spyware in 2009 and 2012, respectively.<sup>215</sup> The high-profile targeting of the Moroccan media outlet Mamfakinch has been attributed to this spyware. Described as a "citizen project that grew out of the Arab Spring in early 2011," the media outlet had won awards for defending and promoting free speech on the internet. In 2012, the site's journalists received an email via the website's contact form with a Microsoft Word document labeled "scandale (2).doc," accompanied by a line in French that translated to, "Please do not mention my name or anything else, I don't want any problems." Likely thinking it was a scoop, the document was opened, downloading RCS spyware, which was later confirmed by digital forensic analysis.<sup>216</sup> The Mamfakinch site has been inactive since February 2014, and the team cites security concerns as one of the reasons behind its disbanding.<sup>217</sup>

---

<sup>214</sup> Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," *The New York Times*, May 29, 2016, sec. Technology, <https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html>.

<sup>215</sup> Privacy International, "State of Privacy Morocco."

<sup>216</sup> Ryan Gallagher, "How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists," *Slate*, August 20, 2012, <https://slate.com/technology/2012/08/moroccan-website-mamfakinch-targeted-by-government-grade-spyware-from-hacking-team.html>.

<sup>217</sup> "Their Eyes on Me: Stories of Surveillance in Morocco."

There is evidence to suggest that FinFisher was used in 2014 by the Supreme Council of National Defense, according to signals identified by Citizen Lab, though there are few details concerning how it was deployed.<sup>218</sup>

In contrast, there is extensive evidence concerning Morocco's use of Pegasus. Citizen Lab determined that Morocco has been using NSO Group's spyware from 2017 to target civil society, journalists, and French government officials.<sup>219</sup> Roughly 10,000 phone numbers from the Forbidden Stories list were based in Morocco, including King Mohamed VI who was seemingly a target, in addition to some high-profile names that Morocco targeted outside of the country. Some 1,000 of the numbers Morocco targeted had French country codes, including French President Emmanuel Macron and 14 ministers. Other surprising names targeted by Morocco included U.S. diplomat and 2015 Iran nuclear deal lead negotiator Robert Malley.<sup>220</sup> When asked to comment on its use of Pegasus by the media nonprofit Forbidden Stories, the Moroccan government categorically denied using Pegasus.<sup>221</sup>

Individuals who were targeted by Pegasus and RCS spyware are detailed below.

#### Aminatou Haidar

Aminatou Haidar is a prominent Sahrawi opposition figure and co-founder of the Sahrawi Commission against the Moroccan Occupation. In 1987, she was arrested,

---

<sup>218</sup> Bill Marczak et al., "Mapping FinFisher's Continuing Proliferation" (University of Toronto, October 15, 2015), <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/>.

<sup>219</sup> "Response from NSO and Governments," *The Guardian*, July 20, 2021, sec. News, <https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments>.

<sup>220</sup> Cole Stangler and Abdellatif El Hamamouchi, "Morocco's Surveillance Machine: Morocco's Intelligence Apparatus Fuels a Crackdown on Dissent," *The Intercept* (blog), October 21, 2021, <https://theintercept.com/2021/10/21/morocco-pegasus-surveillance-journalists/>.

<sup>221</sup> "Response from NSO and Governments."

tortured, and forcibly disappeared for participating in a peaceful demonstration against Morocco's occupation of Western Sahara. She spent four years in a secret prison without due process where she was subjected to electrical shocks and having a chemical-soaked cloth forced into her mouth. She was also jailed from 2005 to 2006 for her independence advocacy. Haidar gained national attention for staging a hunger strike when she was denied re-entry into Western Sahara at the Laayoune airport and has won numerous awards for her peaceful activism.<sup>222</sup>

Haidar received security alerts from Apple notifying her that she may be the target of state-sponsored attackers. She then asked Amnesty International's Security Lab to do forensic analysis and it was confirmed that her two phones were successfully infected with Pegasus as early as September 2018 and as recently as November 2021. When asked for comment, Moroccan authorities disputed the findings citing "a lack of material evidence."

Haidar told RightLivelihood, which recognized her with its Right Livelihood Award in 2019, that her private life has been stolen following the revelation that Morocco had targeted her phones. She told the organization in an interview that she had always been careful about her communications and what she shared in public, as Morocco had used such information in the past to limit her freedoms and to perpetrate violations against her. However, the latest news of the Pegasus targeting "has crossed all limits," leading her to change her work as an activist and her private activities. She stated that:

The consequences have been serious also for my family and close circles, who now have to limit their contact with me to avoid being monitored through my devices. If I am far away, I limit my communications with others as I no longer feel safe talking about personal things. I always try to

---

<sup>222</sup> "Aminatou Haidar | RFK Human Rights," ROBERT F. KENNEDY HUMAN RIGHTS, accessed January 12, 2023, <https://rfkhumanrights.org/aminatou-haidar>.

get information in other ways or postpone information sharing when I can be with loved ones physically...Unlike other times when I felt that digital advances had brought me closer to those who were physically far away, now I feel that the same technology is endangering my family and friends.<sup>223</sup>

Haidar was profiled in a 2022 UN report that listed individuals who were subject to intimidation and reprisals for their engagement with the United Nations related to human rights.<sup>224</sup>

### Fouad Abdelmoumni

Human rights activist and economist Fouad Abdelmoumni learned that he had been targeted by Pegasus surveillance in October 2019 when Citizen Lab both reached out to him telling him that his phone had been hacked by Pegasus. WhatsApp separately contacted Abdelmoumni to tell him the same news.<sup>225</sup> He joined seven other Moroccan activists and journalists in co-signing a letter to Morocco's data protection authorities denouncing the surveillance and demanding an official investigation.<sup>226</sup>

Several months later, in February 2020, Abdelmoumni and his partner were secretly filmed having sex inside their own home, seemingly from the air conditioning vents. Friends and relatives alerted him to the videos—of which there were seven—that had been circulated by an unknown number on WhatsApp.<sup>227</sup> The filming was not done

---

<sup>223</sup> “‘My Private Life Has Been Stolen’: Aminatou Haidar Reveals How Her Life Has Changed after Pegasus Hacking,” Right Livelihood, accessed January 12, 2023, <https://rightlivelihood.org/advocacy-updates/my-private-life-has-been-stolen-aminatou-haidar/>.

<sup>224</sup> “OHCHR | A/HRC/51/47: Cooperation with the United Nations, Its Representatives and Mechanisms in the Field of Human Rights - Report of the Secretary-General,” OHCHR, accessed October 13, 2022, <https://www.ohchr.org/en/documents/thematic-reports/ahrc5147-cooperation-united-nations-its-representatives-and-mechanisms>.

<sup>225</sup> Gail Horak to Cole Stangler and Abdellatif El Hamamouchi, “Question about ‘Morocco’s Surveillance Machine,’” January 11, 2023.

<sup>226</sup> Stangler and Hamamouchi, “Morocco’s Surveillance Machine.”

<sup>227</sup> Stangler and Hamamouchi.

by Pegasus but part of a larger plan to digitally repress him. Abdelmoumni believes he was the target of a smear campaign using tactics that the government has used on dozens of other critics:<sup>228</sup>

I was filmed having sexual relations with my partner as a way to silence me...I felt violated and sad for my country...I'm facing immense pressure, but I did not and I will not submit to the political police attempting to blackmail me.<sup>229</sup>

### Hisham Almiraat

Hisham Almiraat cofounded the award-winning online news outlet, Mamfakinch, in 2009. The outlet was instrumental in circumventing the Moroccan media blackout to bring news of the Arab uprising demonstrations to the people. Several days before the website was to be awarded with the Google-Global Voices Breaking Border award, it was targeted by the Moroccan government using the Hacking Team's RCS technology. The spyware allowed the Moroccan government to gain remote access to every computer, monitor contents in real time, and take photos and videos using the computers' webcams. Citizen Lab confirmed the infection, and it is considered one of the first documented digital attacks using European-made technology to repress human rights activism and journalism.<sup>230</sup>

Almiraat said that one of his first emotions was angst following news of the attack. "You fear for the people who trusted you with their personal information and whose careers, and maybe even lives, you may have put in harm's way," he said. This

---

<sup>228</sup> "Morocco's Regime Is Accused of Blackmailing Critics," *The Economist*, accessed January 16, 2023, <https://www.economist.com/middle-east-and-africa/2021/01/28/moroccos-regime-is-accused-of-blackmailing-critics>.

<sup>229</sup> Stangler and Hamamouchi, "Morocco's Surveillance Machine."

<sup>230</sup> Hisham Almiraat, How a hacking campaign helped shut down an award-winning news site, December 9, 2016, <https://www.amnesty.org/en/latest/research/2016/12/how-a-hacking-campaign-helped-shut-down-an-award-winning-news-site/>.

feeling was quickly replaced by anger – anger for loss of a unique project built on trust that had received a “deadly blow.” He believes that the government may have targeted Mamfakinch to learn who was behind the project in order to intimidate, attack, or discredit them.<sup>231</sup> However, fear of government naming and shaming became irrelevant as people came to another realization: “If the government was ready to invest such vast amounts of money on discovering who was doing what, those who had a career to protect felt that it was time to leave.”<sup>232</sup> He told Freedom House that, ultimately, the state’s ability to rewrite a person’s story based on surveillances allows authorities to “assassinate your character and use your own information to hurt you.”<sup>233</sup>

Almiraat also founded the digital rights organization, Association des Droits Numerique. He is one of the individuals charged with destabilizing state security because of his co-authoring of a report with Privacy International on the use of unlawful spyware used against Moroccan journalists, academics, and human rights activists.<sup>234</sup> While scant information is publicly available, it appears that the criminal prosecution proceedings against him continue at the time of writing.

### Omar Radi

Omar Radi is an award-winning investigative journalist and human rights activist. He was arrested in December 2019 for a tweet posted in April that same year criticizing the judicial system’s decision to uphold the verdict against the 2016-2017 Hirak el-Rif

---

<sup>231</sup> Hisham Almiraat.

<sup>232</sup> “Their Eyes on Me: Stories of Surveillance in Morocco.”

<sup>233</sup> Freedom House, “Morocco,” 2018.

<sup>234</sup> Hisham Almiraat, How a hacking campaign helped shut down an award-winning news site.

protestors. He was granted a provisional release a few days later but received a four-month suspended sentence in March 2020.

Amnesty International examined Radi's phone and determined that it had been subject to network injections from January 2019 to the end of January 2020 that were ultimately successful. Network injections allow operators to redirect a targets' browsers and apps invisibly and automatically to malicious sites under the operator's control. They ultimately leverage software vulnerabilities to infect the device. The same kinds of attacks were used against human rights defender Maati Monjib.<sup>235</sup> Both Radi and Monjib's targeting have been attributed to NSO Group, and the government of Morocco is believed to be the operator.<sup>236</sup>

Radi's trial began in 2020 within days of the Amnesty International issuing a report about Morocco targeting Radi using Pegasus spyware. He was sentenced in July 2021 to six years in prison for espionage and sexual assault charges that Freedom House, Human Rights Watch, and other human rights groups have criticized as politically motivated.<sup>237</sup> His subsequent appeal was denied. Human Rights Watch noted that "all sexual assault complaints merit serious investigation...however, there are precedents in

---

<sup>235</sup> Amnesty International, "Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools" (Amnesty International, June 22, 2020), <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/>.

<sup>236</sup> David Pegg et al., "FT Editor among 180 Journalists Identified by Clients of Spyware Firm," *The Guardian*, July 20, 2021, sec. World news, <https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware>.

<sup>237</sup> Adrian Shahbaz and Allie Funk, "Freedom on the Net 2020, The Pandemic's Digital Shadow" (Freedom House, November 2020), 9, [https://freedomhouse.org/sites/default/files/2020-10/10122020\\_FOTN2020\\_Complete\\_Report\\_FINAL.pdf](https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf).

Morocco of arresting, trying, or imprisoning independent journalists, activists, or politicians on questionable charges of sexual misconduct.”<sup>238</sup>

### Maati Monjib

Maati Monjib is a historian, journalist, and co-founder of the NGO Freedom Now that protects the rights of journalists and writers. He also co-founded and is a leading member of the Moroccan Association for Investigative Journalism.<sup>239</sup> He was accused of “threatening the internal security of the state” in 2015 for promoting a mobile app called StoryMaker that would allow individuals to publish stories anonymously. In 2021, he was jailed for three months on money laundering charges.<sup>240</sup>

Monjib believes he has been under constant digital surveillance since 2015, which caused psychological distress:

I need to constantly analyze the consequences of what I say and the risk that this may lead to defamatory accusations against me. This even applies to very practical things like arranging meetings or a dinner downtown.<sup>241</sup>

Forensic analysis by Amnesty International confirmed that Monjib had been targeted with Pegasus spyware via malicious links in SMS messages.<sup>242</sup>

### Abdessadak El Bouchattaoui

---

<sup>238</sup> “Morocco: Espionage Case Against Outspoken Journalist,” *Human Rights Watch* (blog), September 21, 2020, <https://www.hrw.org/news/2020/09/21/morocco-espionage-case-against-outspoken-journalist>.

<sup>239</sup> Amnesty International, “Morocco: Human Rights Defenders Targeted with NSO Group’s Spyware,” Amnesty International, October 10, 2019, <https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/>.

<sup>240</sup> Human Rights Watch, “‘They’ll Get You No Matter What’: Morocco’s Playbook to Crush Dissent” (Human Rights Watch, July 28, 2022), <https://www.hrw.org/report/2022/07/28/theyll-get-you-no-matter-what/moroccos-playbook-crush-dissent>.

<sup>241</sup> Amnesty International, “Morocco,” October 10, 2019.

<sup>242</sup> Amnesty International.

Abdessadak El Bouchattaoui is a human rights defender and lawyer that served on the legal defense team for individuals imprisoned for participating in the Hirak el-Rif social justice protests in 2016 and 2017. He criticized the authorities' excessive use of force in the protests in several online posts and was sentenced in 2017 to 20 months in prison, though he not served time since his asylum request was accepted in France.<sup>243</sup>

Like Monjib, Bouchattaoui believed he was being surveilled when he began defending the Hirak protestors. He said the physical harassment and intimidation that his family has faced have affected his psychological wellbeing and ability to work. He described it in this manner:

Surveillance in Morocco is carried out in an open and brazen way...  
Surveillance is a type of punishment. You can't behave freely. It is part of their strategy to make you suspect you're being watched so you feel like you're under pressure all the time.<sup>244</sup>

Amnesty International confirmed that his phone was targeted by Pegasus spyware. In Bouchattaoui's targeting, the SMS messages were intended to seem like spam and were accompanied by malicious links disguised as stop message commands.<sup>245</sup>

---

<sup>243</sup> Amnesty International, "Morocco," October 10, 2019.

<sup>244</sup> Amnesty International.

<sup>245</sup> Amnesty International.

## Chapter X.

### Saudi Arabia

Seeing the fall of the Egyptian and Tunisian governments, Saudi Arabia responded to the Arab uprisings in its own, unique way: it used its oil rent to pay \$134 billion to increase salaries, build housing, finance religious organizations, and support other projects in an effort to neutralize most opposition. It also responded to protests in the mostly Shiite eastern provinces with arrests.<sup>246</sup>

By 2011, Freedom House was already tracking digital repression concerns in the kingdom. These included online censorship, the persecution of online users, the blocking of certain websites, internet throttling to slow the dissemination of photos and news, and state ownership of the country's internet infrastructure.<sup>247</sup> Over the next decade, these concerns continued to grow, with a marked decline from 2017-2018 when there was "[an] escalating intolerance for all forms of political, social, and religious dissent."<sup>248</sup> This period correlates with Mohamed bin Salman's first year as Crown Prince.

From 2011 to 2012, the kingdom started to use pro-government commentators to manipulate online discussions.<sup>249</sup> By 2015, Freedom House noted that the number of

---

<sup>246</sup> Neil MacFarquhar, "In Saudi Arabia, Royal Funds Buy Peace for Now," *The New York Times*, June 9, 2011, sec. World, <https://www.nytimes.com/2011/06/09/world/middleeast/09saudi.html>.

<sup>247</sup> Sanja Kelly and Sarah Cook, "Freedom on the Net 2011, A Global Assessment of Internet and Digital Media."

<sup>248</sup> Freedom House, "Saudi Arabia: Freedom on the Net 2018 Country Report" (Freedom House, 2018), <https://freedomhouse.org/country/saudi-arabia/freedom-net/2018>.

<sup>249</sup> Sanja Kelly, Sarah Cook, and Mai Truong, "Freedom on the Net 2012, A Global Assessment of Internet and Digital Media."

progovernment Twitter accounts had increased and intensified their disinformation and misinformation campaigns.<sup>250</sup>

In 2012 some of the first reports emerged stating that the Saudi government was recruiting experts to intercept encrypted data from Twitter, Viber, Vine, and WhatsApp.<sup>251</sup> This included recruiting two Twitter employees to clandestinely provide personal user information of Saudi dissidents posting anonymously. One employee, Ahmad Abouammo, was convicted in 2022, while the other, Ali Alzabarah, fled the United States before he could be arrested.<sup>252</sup>

During the past decade, the persecution of online users grew, with social media users frequently detained and sentenced with up to 10 years of jail for posting content on taboo topics.<sup>253</sup> Saudi Arabia's purchase of passive surveillance from BAE systems came to light in 2017, expanding the capacity of operators to monitor "any" traffic and drill down to details around specific targets, according to an anonymous individual who worked for the firm.<sup>254</sup>

Saudi internet filtering has long been noted by human rights activists and organizations. In 2013, Manal al-Sharif was one of the first women to post videos of herself driving in Saudi Arabia. She encouraged other women to create videos of themselves driving and post them online as an act of defiance to Saudi custom.<sup>255</sup> Al-

---

<sup>250</sup> Freedom House, "Saudi Arabia: Freedom on the Net 2016 Country Report" (Freedom House, 2016), <https://freedomhouse.org/country/saudi-arabia/freedom-net/2016>.

<sup>251</sup> Sanja Kelly et al., "Freedom on the Net 2013, A Global Assessment of Internet and Digital Media."

<sup>252</sup> Kalley Huang and Kate Conger, "Former Twitter Employee Convicted of Charges Related to Spying for Saudis," *The New York Times*, August 9, 2022, sec. Technology, <https://www.nytimes.com/2022/08/09/technology/twitter-saudi-arabia-spying-ahmad-abouammo.html>.

<sup>253</sup> Sanja Kelly et al., "Freedom on the Net 2014, Tightening the Net: Governments Expand Online Controls."

<sup>254</sup> Evans, "BAE 'Secretly Sold Mass Surveillance Technology to Repressive Regimes.'"

<sup>255</sup> Sanja Kelly et al., "Freedom on the Net 2014, Tightening the Net: Governments Expand Online Controls."

Sharif was taken by the secret police and held for nine days. It was only after her father made a personal appeal to the king that she was released.<sup>256</sup> The Saudi government blocked the campaign website #Women2Drive as the protest movement continued to grow in 2014.<sup>257</sup> In May 2018, Loujain al-Hathloul and several other activists were arrested for their role in a renewed push to lift the driving ban, despite the initiative succeeding several weeks later. Al-Hathloul’s imprisonment served as a reminder that the crown prince’s modernizing reforms were shallow, as she was released in February 2021 after serving three years in prison.<sup>258</sup>

Saudi Arabia boasts the second highest digital repression score globally; it is also one of the best-known countries for targeting its citizens abroad.<sup>259</sup> Table 6 corroborates trends identified above.

Table 6. Saudi’s Freedom on the Net and Digital Repression Index Scores

|                          | 2011 | 2021 | Trend |
|--------------------------|------|------|-------|
| Freedom on the Net       | 70   | 76   | ↑     |
| Digital Repression Index | 1.68 | 1.69 | ↑     |

*Freedom on the Net scores on a scale of 0-100, with 100=least free. The Digital Repression Index (DRI) scale is -5 to 5, with 0 representing the country-mean across variables for the year assessed. A positive score indicates that a country is performing above the mean across all DRI variables.*

<sup>256</sup> Manal Sharif, *Daring to Drive: A Saudi Woman’s Awakening*, First Simon&Schuster hardcover edition. (New York: Simon & Schuster, 2017).

<sup>257</sup> Sanja Kelly et al., “Freedom on the Net 2015, Privatizing Censorship, Eroding Privacy.”

<sup>258</sup> Fatma Tanis, “Saudi Activist Who Led Campaign To Legalize Driving For Women Is Released From Jail,” *NPR*, February 10, 2021, sec. Middle East, <https://www.npr.org/2021/02/10/966258281/loujain-al-hathloul-saudi-activist-jailed-for-driving-has-been-released>.

<sup>259</sup> “Saudi Arabia Case Study | Understanding Transnational Repression,” Freedom House, accessed December 30, 2022, <https://freedomhouse.org/report/transnational-repression/saudi-arabia>.

Saudi Arabia has reportedly purchased the products and services of at least six private spyware companies over the past decade: Hacking Team, NSO Group, FinFisher, Candiru, Cytrox, and Quadream. In June 2014, Citizen Lab detected Hacking Team's RCS spyware for the first time in Saudi Arabia and, working with Human Rights Watch, determined that it was being used to monitor activists in the eastern province of Qatif, where most minority Shia Muslims live in the kingdom. The spyware was disguised as a copy of the mobile phone news app Qatif Today that, once downloaded, installed the spyware.<sup>260</sup> It is believed that the Saudi government acquired a stake in the Hacking Team through intermediaries in 2018,<sup>261</sup> though the founder and former CEO of Hacking Team, David Vincenzetti, posted a curious note on his LinkedIn profile in May 2020 stating that "Hacking Team is dead. Definitely dead."<sup>262</sup>

NSO Group and its Pegasus spyware have a long and complicated history with Saudi Arabia that has been punctuated with egregious reports of abuse. NSO first signed a contract with the kingdom in 2017. On the Israeli side, the relationship was handled by a few senior members of Prime Minister Netanyahu's inner circle who operated under secrecy. Following revelations of Jamal Khashoggi's brutal murder and dismemberment by a Saudi Tiger Team at the Saudi Consulate in Istanbul on October 2, 2018, the company's ethics committee decided to turn Pegasus off in the kingdom. The committee advised the company to resist anticipated pressure from the Israeli government to turn it back on, even though NSO reported that its after-action review found no evidence that

---

<sup>260</sup> Morgan Marquis-Boire et al., "Hacking Team's Tradecraft and Android Implant" (University of Toronto, June 24, 2014), <https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/>.

<sup>261</sup> Freedom House, "Saudi Arabia," 2018.

<sup>262</sup> "Hacking Team Founder: 'Hacking Team Is Dead,'" accessed October 17, 2021, <https://www.vice.com/en/article/n7wbnd/hacking-team-is-dead>.

Khashoggi had been targeted using its product. Independent forensic analysis has since disproved NSO's assertions: Pegasus infections were confirmed on the phones of Khashoggi's friend, Omar Abdulaziz,<sup>263</sup> and his fiancée, Hatice Cengiz, which were attributed to Saudi Arabia. UAE is believed to be behind the targeting of Khashoggi's wife, Hanan Elatr, using Pegasus.<sup>264</sup> In addition, an unnamed close associate and two associates of Khashoggi's were also found on the Forbidden Stories Pegasus list, in addition to two senior Turkish officials involved in the homicide investigation.<sup>265</sup>

In 2019, the decision was taken to turn Pegasus back on following UK-based private equity firm Novalpina's purchase of U.S.-based Francisco Partners' NSO shares, but it was short-lived.<sup>266</sup> While Pegasus was turned back on, former Tunisian minister and UN lead investigator into possible war crimes in Yemen Kamel Jendoubi was targeted by Saudi Arabia using the spyware in August 2019.<sup>267</sup> This occurred several weeks before Jendoubi and experts released a report concluding that the Saudi-led coalition had committed "serious violations of international humanitarian law" that could constitute "criminal responsibility for war crimes" in the Yemen war.<sup>268</sup> In late 2020,

---

<sup>263</sup> Bill Marczak et al., "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil" (University of Toronto, October 1, 2018), <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>.

<sup>264</sup> Stephanie Kirchgaessner, "Saudis behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian*, July 18, 2021, sec. World news, <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.

<sup>265</sup> Dana Priest, Souad Mekhennet, and Arthur Bouvart, "Jamal Khashoggi's Wife Targeted with Spyware before His Death," *Washington Post*, July 18, 2021, <https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/>.

<sup>266</sup> Ronen Bergman and Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon," *The New York Times*, January 28, 2022, sec. Magazine, <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>.

<sup>267</sup> "Pegasus: Saudi Arabia 'targeted Phone' of UN Investigator into Yemen War Crimes," *Middle East Eye*, December 20, 2021, <http://www.middleeasteye.net/news/pegasus-spyware-saudi-arabia-targeted-phone-un-investigator-yemen>.

<sup>268</sup> Stephanie Kirchgaessner, "UN-Backed Investigator into Possible Yemen War Crimes Targeted by Spyware," *The Guardian*, December 20, 2021, sec. World news,

NSO's export license to Saudi Arabia ran out, and Pegasus was turned off again. NSO had been concerned about allegations of abuse and did not request re-licensing from Israeli authorities. The crown prince allegedly called Netanyahu, who was unaware of the licensing issue. That night, at Netanyahu's direction and with a written request from the Ministry of Defense, Pegasus was turned back on.<sup>269</sup>

In mid-2020, 34 Al Jazeera journalists, producers, anchors, and executives and their 36 phones were targeted using Pegasus, and the attack was attributed to Saudi Arabia and the UAE in a Citizen Lab report issued in December that year.<sup>270</sup> This revelation prompted another shutdown of the system before the end of 2020, and in July 2021, the company's board reportedly declared any new deals with Saudi Arabia off limits.<sup>271</sup> An additional victim has been identified that calls Saudi's current Pegasus status into doubt: either Saudi Arabia or UAE may have been behind the targeting of former Egyptian presidential candidate and opposition leader Ayman Nour's phone with Pegasus in 2021, which had been simultaneously targeted with Cytox by Egypt.<sup>272</sup>

Saudi Arabia is also a likely operator of FinFisher spyware. Citizen Lab scanned the internet for signals related to the spyware's command and control server, FinSpy Master, and found evidence. Unlike the other case study examples, no fingerprints pointing to a specific Saudi agency were identified.<sup>273</sup>

---

<https://www.theguardian.com/world/2021/dec/20/un-backed-investigator-into-possible-yemen-war-crimes-targeted-by-spyware>.

<sup>269</sup> Bergman and Mazzetti, "The Battle for the World's Most Powerful Cyberweapon."

<sup>270</sup> Bill Marczak et al., "The Great IPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit" (University of Toronto, December 20, 2020), <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/>.

<sup>271</sup> Ronen Bergman and Mark Mazzetti, "Israeli Companies Aided Saudi Spying Despite Khashoggi Killing," *The New York Times*, July 17, 2021, sec. World, <https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html>.

<sup>272</sup> Ronald Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy."

<sup>273</sup> Marczak et al., "Mapping FinFisher's Continuing Proliferation."

Saudi Arabia is believed to have a contract with Candiru since 2018.<sup>274</sup> There is little documentation on the purchase and use of the spyware. Candiru is an Israeli company founded in 2015 that is considered an NSO Group competitor. Though it has changed names many times and is now called Saito Tech, Ltd., it is best known by the name Candiru. The company originally focused on computer spyware but added smartphone targeting capabilities in 2017, according to a lawsuit filed by a former Candiru employee.<sup>275</sup> Brian Bartholomew, a researcher for Kaspersky Labs, identified a lapse in an Uzbekistan intelligence agency's operational system that enabled him to connect Windows vulnerabilities in the Uzbek attacks back to Candiru and two of its other customers, Saudi Arabia and the UAE.<sup>276</sup> After Khashoggi's murder, Israel allegedly encouraged NSO Group to continue working with Saudi Arabia, in addition to two other companies, Candiru and Verint (about which even less is known).<sup>277</sup>

Saudi Arabia has also been linked with Cytrox, another little-known spyware company that began as a Macedonian startup. Two Cytrox companies were formed in Israel and Hungary in 2017, which have subsequently undergone renaming. The company's spyware, Predator, is connected to Egypt's targeting of Nour. Analysis of Nour's phone led Citizen Lab to discover signals indicating that Saudi Arabia was another Cytrox operator.<sup>278</sup> Meta reported that it had removed 300 accounts on Facebook

---

<sup>274</sup> Bergman and Mazzetti, "Israeli Companies Aided Saudi Spying Despite Khashoggi Killing."

<sup>275</sup> Amitai Ziv, "Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed," *Haaretz*, September 7, 2020, <https://www.haaretz.com/israel-news/tech-news/2020-09-07/ty-article/.premium/mobile-spytech-millions-in-gulf-deals-top-secret-israeli-cyberattack-firm-reve/0000017f-e1eb-d568-ad7f-f3eb36390000>.

<sup>276</sup> Thomas Brewster, "Meet Candiru — The Mysterious Mercenaries Hacking Apple And Microsoft PCs For Profit," *Forbes*, October 3, 2019, <https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/>.

<sup>277</sup> Bergman and Mazzetti, "Israeli Companies Aided Saudi Spying Despite Khashoggi Killing."

<sup>278</sup> Marczak et al., "Pegasus vs. Predator."

and Instagram linked to the spyware. The social media company observed that Cytox had a vast domain infrastructure to spoof legitimate news entities in countries of interest, and its analysis also pointed to Saudi Arabia as an operator.<sup>279</sup>

Quadream is another Israeli company that began working with Saudi Arabia in 2019 after the Khashoggi murder.<sup>280</sup> There is scant information about the company which targets smartphones using a virus called Reign. Reign reportedly belongs to one of Quadream's shareholders, InReach, which is based in Cyprus. As a result of this arrangement, Quadream is not subject to the same Israeli oversight as NSO Group's Pegasus, which has similar smartphone-targeting capabilities. Reign also reportedly cannot be turned off remotely, which may be why the kingdom purchased a product similar to Pegasus.<sup>281</sup>

### Manal al-Sharif

The May 2011 video of Manal al-Sharif driving around the Saudi town of al-Khobar several years before the country's ban on female drivers was lifted is still visible on YouTube. In it, Al-Sharif described the absurdity of relying on men, oftentimes strangers, to drive women when they are capable of driving themselves. She then encouraged fellow women to join her in a campaign challenging what was not a law but a custom stating that women could not drive in Saudi Arabia. For her act of defiance, al-

---

<sup>279</sup> Mike Dvilyanski, David Agranaovich, and Nathaniel Gleichder, "Threat Report on the Surveillance-for-Hire Industry" (Meta, December 16, 2021), <https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf>.

<sup>280</sup> Bergman and Mazzetti, "Israeli Companies Aided Saudi Spying Despite Khashoggi Killing."

<sup>281</sup> Gur Megiddo, "Secretive Israeli Cyber Firm Selling Spy-Tech to Saudi Arabia," *Haaretz*, June 8, 2021, <https://www.proquest.com/docview/2538079950/citation/5128B78F82A54D99PQ/1>.

Sharif was subject of a smear campaign and jailed for nine days until her father made a personal plea to the king to forgive his daughter's transgression.

Al-Sharif's employer put her on notice that it did not want the attention from her activism, and she soon after lost her job. She was targeted twice by spyware, which Citizen Lab confirmed. Al-Sharif has not publicly named which spyware product was used. As a result of immense pressure, she moved to the UAE, and eventually to Australia, where she started a new life. As a divorced Saudi woman, she was unable to take her son with her because her ex-husband (who is also Saudi) exercises full custody, as is the custom. Al-Sharif remarried a non-Saudi, and the Saudi government has declined recognition of that marriage. As a result, her son from her second marriage who lives in Australia has never met her son from her first marriage.<sup>282</sup>

Despite these challenges, al-Sharif has remained vocal. She returned to her cyber security background and now writes articles and speaks out about the dangers of tech. She meets people face to face instead of by phone whenever possible. She has deleted all of her social media accounts. This includes the Twitter account that once notified international media when she was arbitrarily detained in 2011 so that Saudi officials could not "disappear" her.<sup>283</sup>

There is no doubt in al-Sharif's mind that human rights have deteriorated since the Arab uprisings. However, she does not point to spyware as the cause; rather, she points to the internet. She notes that Saudi efforts to supply citizens with fast, cheap

---

<sup>282</sup> Sharif, *Daring to Drive*.

<sup>283</sup> "How Western Spyware Helps Dictators with Phillip Adams," *ABC Radio National* (Australian Broadcasting Corporation, August 3, 2021), <https://www.abc.net.au/radionational/programs/latenightlive/pegasus-israeli-spyware-manal-alsharif/13482000>.

internet preceded 2011 and has resulted in an environment where there is very high internet penetration and nearly every Saudi has two phones. The Saudi government has moved many services online and digitized the national identification card. This infrastructure allows the connection of disparate data systems. The danger, al-Sharif explains, is that the government can locate you at all times and, if you are a woman, can send a text message to your male guardian to alert him that you are exiting the kingdom.<sup>284</sup> This digital government project is driven by Saudi Arabia's Digital Government Authority with the stated objective of establishing "...a foundation that enables the digital government ecosystem to innovate, without being limited by doing 'business as usual.'"<sup>285</sup>

#### Saad al-Jabri

Saad al-Jabri is a former Saudi official living in exile in North America. He was a senior intelligence and counter-intelligence official in Saudi's Ministry of Interior, a Minister of State, and a longtime advisor to deposed Crown Prince Mohamed bin Nayef. Former Acting Director of the CIA, Mike Morrell, credits al-Jabri with saving many U.S. lives for his work thwarting specific terrorist threats against the United States. Al-Jabri was dismissed from his government positions in 2015 after a visit to Washington, DC that included CIA headquarters, and he continued to advise Crown Prince Mohammed

---

<sup>284</sup> Manal al-Sharif, Interview by author, January 19, 2023.

<sup>285</sup> "Saudi Arabia's Digital Government Stays Ahead of the Curve," Deloitte Insights, accessed January 24, 2023, <https://www2.deloitte.com/us/en/insights/focus/tech-trends/2023/saudi-arabia-government-digital-transformation-and-innovation.html>.

bin Nayef until departing Saudi Arabia in May 2017.<sup>286</sup> Bin Nayef was deposed in June 2017 when King Salman named Crown Prince Mohammed bin Salman as his successor.

Al-Jabri and his family have been the target of harassment, physical attacks, and spyware. Crown Prince Mohammed bin Salman sent threatening WhatsApp messages directly to al-Jabri, demanding that al-Jabri return to Saudi Arabia.<sup>287</sup> He then began to collectively punish al-Jabri's family members.

Saudi officials prevented al-Jabri's youngest children, Omar and Sarah, born in 1998 and 2000, respectively, from returning to the United States for school in June 2017. In March 2020, more than 50 armed men dressed in civilian clothes entered the al-Jabri residence in Riyadh and took Omar and Sarah without an arrest warrant or documentation authorizing the arrest. They are being held incommunicado at an undisclosed location.

Al-Jabri's son-in-law, Salem Almuzaini, has also been subject to threats and torture due to his connection to al-Jabri. While attempting to leave Dubai to visit his father-in-law in Turkey in 2017, Almuzaini was forcibly returned from the UAE (where he is a permanent resident) to Saudi Arabia. He was imprisoned at a maximum-security prison in Jeddah and another in Riyadh for 45 days, where he was physically and psychologically tortured, including beatings and 300 lashes. The torture was intended to extract information about al-Jabri and to compel his return to Saudi Arabia. Almuzaini was then transferred to the Ritz Carlton Hotel in Riyadh with others that the crown prince had detained; he was released in January 2018 with an ankle bracelet for tracking. In

---

<sup>286</sup> "Former Saudi Official Calls Mohammed Bin Salman a 'Psychopath,' Says Saudi Crown Prince Fears What He Knows," News (CBS, July 10, 2022), <https://www.cbsnews.com/news/mohammed-bin-salman-alleged-plot-saad-aljabri-60-minutes-2021-10-24/>.

<sup>287</sup> "Former Saudi Official Calls Mohammed Bin Salman a 'Psychopath,' Says Saudi Crown Prince Fears What He Knows."

August 2020, Almuzaini was asked to meet with Saudi State Security and has not been heard from since. Approximately 20 family members and associates have been arrested and are currently being held incommunicado to exert pressure on al-Jabri.<sup>288</sup>

Al-Jabri alleges that the crown prince has tried to track him down to kill him. In a lawsuit al-Jabri filed in the United States against Saudi Crown Prince Mohammed bin Salman, he said the Saudi government first attempted to determine his whereabouts using Saudi students in U.S. universities, and then a Saudi contact visited his son in Boston and made several trips to Toronto to learn where the Saudi exile lived. A friendly intelligence agency informed al-Jabri that the Saudi regime had also targeted him with spyware (which kind is unknown) via a video file sent by a Saudi journalist on WhatsApp to assist in hunting him down. Once his location was determined, there were attempts on his life.<sup>289</sup>

The crown prince dispatched a Tiger Team hit squad to find al-Jabri less than two weeks after Khashoggi's murder in October 2018, drawing from the same team of mercenaries sent to kill Khashoggi. They carried two bags of forensic tools with them and were stopped by Canada Border Services Agency officials at Ottawa International Airport. During inspection, officials noted inconsistencies in the group's stories and found evidence that the team members knew each other, which they had previously denied. The team was deported and the attack was thwarted. Canadian security agencies also told al-Jabri in July 2020 that there was a "credible and imminent threat to his life," a

---

<sup>288</sup> Human Rights Council Working Group on Arbitrary Detention, "Opinions Adopted by the Working Group on Arbitrary Detention at Its Ninety-Third Session, 30 March–8 April 2022" (United Nations Human Rights Council, May 12, 2022), <https://www.ohchr.org/sites/default/files/2022-06/A-HRC-WGAD-2022-29-ARE-SAU-AEV.pdf>.

<sup>289</sup> Dr. Saad Al-Jabri v. Mohammed bin Salman bin Abdulaziz al Saud, No. Civil Action 20-2146 (TJK) (U.S. District Court for the District of Columbia September 30, 2022).

warning that was echoed by other sources in November 2020.<sup>290</sup> Al-Jabri is convinced that the crown prince wants to kill him because of what he knows, and he has made a video revealing secrets that is to be publicized if the crown prince is successful.<sup>291</sup>

Al-Jabri has had mixed success in North American courts. The judge in the U.S. District Court dismissed his case, stating that al-Jabri failed to prove that the court had jurisdiction in the case.<sup>292</sup> He was partially successful in other legal cases. Sakab Saudi Holding Company filed a complaint in Canada stating that al-Jabri conspired with former Crown Prince Mohammed bin Nayef to defraud the company of \$1.2 billion, from which al-Jabri allegedly took \$500 million. Al-Jabri used to control the company with bin Nayef, and it was used to facilitate several front companies for intelligence operations with the CIA and other foreign intelligence agencies. The Canadian case has not yet been heard, but the judge there thought the company's evidence was compelling enough to put a global freeze on al-Jabri and his family's assets. The company also filed a lawsuit in Massachusetts stating that al-Jabri's eight condos in Boston should be included as part of the Canadian asset freeze, which al-Jabri's lawyers had escalated to a federal court.<sup>293</sup> In December 2021, the U.S. suit was dismissed citing a U.S. government intervention by Director of National Intelligence Avril Haines to prevent the release of classified information.<sup>294</sup> Canadian government lawyers acting at the request of the Canadian

---

<sup>290</sup> *AlJabri*.

<sup>291</sup> "Former Saudi Official Calls Mohammed Bin Salman a 'Psychopath,' Says Saudi Crown Prince Fears What He Knows."

<sup>292</sup> Danna Akkad and Umar Farooq, "US Judge Throws out Former Saudi Spy Chief's Case against Crown Prince," *Middle East Eye*, October 3, 2022, <http://www.middleeasteye.net/news/us-saudi-arabia-former-spy-chief-crown-prince-case-thrown>.

<sup>293</sup> "Former Saudi Official Calls Mohammed Bin Salman a 'Psychopath,' Says Saudi Crown Prince Fears What He Knows."

<sup>294</sup> Reuters, "U.S. Court Tosses Saudi Suit against Former Top Saudi Intelligence Officer," *Reuters*, December 30, 2021, sec. United States, <https://www.reuters.com/world/us/us-court-tosses-saudi-suit-against-former-top-saudi-intelligence-officer-2021-12-30/>.

Security Intelligence Service took cues from the United States and have filed a motion preventing al-Jabri and his lawyers from using classified material in the Canadian court case, which could result in case dismissal.<sup>295</sup>

### Omar Abdulaziz

Saudi Arabia also targeted Saudi human rights activist and influential Twitter user Omar Abdulaziz using Pegasus in 2018. Abdulaziz alleges that 30 other Saudi influencers had their smartphones hacked and were blackmailed to support Saudi propaganda on Twitter or else the personal information extracted from their smartphones would be released online. Twitter is seen as shaping public opinion in Saudi Arabia,<sup>296</sup> where eight out of ten Saudis use it. With his half a million Twitter followers, he is one of the kingdom's top three Twitter influencers. The second has been arrested and the third disappeared. Saudi expert Guido Steinberg of the German Institute for International and Security Affairs described why Abdulaziz's voice is important:

He is so prominent because all opposition, liberal and liberal-Islamic voices in Saudi Arabia have fallen silent. Either they are in prison or they have been forced by other means to cease their activities. Abdulaziz is considered an opposition and liberal voice, without having a clear political profile.<sup>297</sup>

---

<sup>295</sup> "Former Saudi Official Calls Mohammed Bin Salman a 'Psychopath,' Says Saudi Crown Prince Fears What He Knows."

<sup>296</sup> Omar Abdulaziz, "Opinion | Saudi Spies Hacked My Phone and Tried to Stop My Activism. I Won't Stop Fighting.," *Washington Post*, November 15, 2019, <https://www.washingtonpost.com/opinions/2019/11/14/saudi-spies-hacked-my-phone-tried-stop-my-activism-i-wont-stop-fighting/>.

<sup>297</sup> Diana Hodali, "Omar Abdulaziz: A Critic of Saudi Arabia Becomes a Target – DW – 06/24/2020," *Dw.Com*, June 24, 2020, <https://www.dw.com/en/omar-abdulaziz-a-critic-of-saudi-arabia-becomes-a-target/a-53924977>.

Abdulaziz claimed asylum in Canada while studying there.<sup>298</sup> He had been working with Khashoggi on a project to identify Saudi trolls and to counter them using a volunteer army of “electronic bees” prior to Khashoggi’s murder by Saudi officials.<sup>299</sup> The two had planned and purchased – with Khashoggi’s financial support – untraceable U.S. and Canadian sim cards that volunteers could use to counter Saudi trolls on Twitter.<sup>300</sup>

To help track him down, the Saudi government paid two Twitter employees to spy for them and obtain information about dissidents using the platform; Abdulaziz was one of the individuals who was targeted.<sup>301</sup> In 2018, he was approached by two Saudi emissaries who suggested that he could return to Saudi Arabia and become the “voice of the youth,” but he said the offer had overtones: either return home or go to jail. He was also told that he should get his passport renewed at the Saudi embassy. He did not go, and several months later, Khashoggi was murdered at the Saudi Consulate in Istanbul. He says he is haunted by what might have happened.

It was after the emissaries’ visit that Abdulaziz’s phone was infected with Pegasus in 2018. Saudi officials also imprisoned the activist’s two younger brothers and dozens of friends and made them tell Abdulaziz to stop his work. “They want to hurt me as a critic, ok. But what does my family have to do with it? Why are my parents and siblings not

---

<sup>298</sup> Tim Adams, “Khashoggi Confidant Omar Abdulaziz: ‘I’m Worried about the Safety of the People of Saudi Arabia’ | Documentary Films | The Guardian,” *The Guardian*, February 20, 2021, <https://www.theguardian.com/film/2021/feb/20/me-jamal-khashoggi-mohammed-bin-salman-omar-abdulaziz-the-dissident-netflix>.

<sup>299</sup> Omar Abdulaziz, “Opinion | Saudi Spies Hacked My Phone and Tried to Stop My Activism. I Won’t Stop Fighting.”

<sup>300</sup> Tim Adams, “Khashoggi Confidant Omar Abdulaziz: ‘I’m Worried about the Safety of the People of Saudi Arabia’ | Documentary Films | The Guardian.”

<sup>301</sup> Omar Abdulaziz, “Opinion | Saudi Spies Hacked My Phone and Tried to Stop My Activism. I Won’t Stop Fighting.”

allowed to travel, not allowed to contact me anymore?" he said in a video on Twitter. In 2020, Royal Canadian Mounted Police notified Abdulaziz that there was a credible threat against his life from Saudi Arabia. He told the Guardian:

I can't announce where I'm going. I'm using a code to interact with others. I'm worried about my safety, but to be honest I'm more worried about the safety of the people of Saudi Arabia. I want to talk about my brothers and my friends, but really we're talking about thousands of people who are threatened.<sup>302</sup>

#### Ghanem al-Masarir

Al-Masarir is a Saudi dissident living in the United Kingdom who creates satirical YouTube videos about the Saudi royal family, including Saudi Crown Prince Mohammad bin Salman. In mid-2018, al-Masarir noticed that his smartphones had become sluggish. He sent them to Citizen Lab, and they were confirmed to be infected with Pegasus spyware. In August that year, he was tracked down and physically assaulted by Saudi agents in London, who asked who gave him the right to talk about the Saudi royal family.<sup>303</sup> In October, Metropolitan Police visited his home to issue him an "Osman warning," which police give when they receive information of a threat against a person's life that lacks evidence for an arrest, and they installed a panic button linked to his landline. Al-Masarir filed a lawsuit against the Saudi government in November 2018 seeking damages and an apology. In 2020, the British High Court decided that the lawsuit could proceed.

---

<sup>302</sup> Tim Adams, "Khashoggi Confidant Omar Abdulaziz: 'I'm Worried about the Safety of the People of Saudi Arabia,'" *The Guardian*, February 20, 2021, sec. Film, <https://www.theguardian.com/film/2021/feb/20/me-jamal-khashoggi-mohammed-bin-salman-omar-abdulaziz-the-dissident-netflix>.

<sup>303</sup> *Ghanem Almasarir Political Satirist Attacked in London for Mocking Saudi Royals*, 2018, <https://www.youtube.com/watch?v=vKyTBrvWdP4>.

“Knowing that the Saudis have been spying on me and had complete access to my private life has had a huge impact on me personally,” al-Masarir wrote in an op-ed in the *Washington Post*. The invasion of privacy has led him to live in constant fear for his life both at home and abroad, where he could be kidnapped and returned to Saudi Arabia. He also worries about the safety of anyone associated with him.<sup>304</sup>

### Ghada Oueiss

Pegasus spyware was used to target a Lebanese journalist for Al Jazeera, Ghada Oueiss, who anchors political programs covering current affairs. In 2020, Oueiss started to suspect that her smartphone was compromised. She discovered personal information on Twitter detailing where she lived in Beirut and information about her brother that she had not shared publicly. A private photo with colleagues was also posted online, which colleagues denied sharing. Next, hundreds of copies of a screenshot of Oueiss in a swimsuit from a video her husband had taken was published all over the internet.<sup>305</sup> The photo was accompanied by misogynistic messages and false claims that it was taken at the private residence of Al Jazeera Media Network’s Qatari chairman, Sheikh Hamad Bin Thamer Al-Thani. Hours later, another photo surfaced with her in a hot tub; it had been pixelated to make it appear that she was nude. It was tweeted more than 40,000 times.<sup>306</sup>

---

<sup>304</sup> Ghanem al-Masarir, “Opinion | Saudi Arabia Has Had Complete Access to My Private Life. So Now I’m Suing,” *Washington Post*, January 26, 2020, [https://www.washingtonpost.com/opinions/saudi-arabia-has-been-spying-on-me-for-years-so-im-suing/2020/01/25/0fa55462-3f00-11ea-8872-5df698785a4e\\_story.html](https://www.washingtonpost.com/opinions/saudi-arabia-has-been-spying-on-me-for-years-so-im-suing/2020/01/25/0fa55462-3f00-11ea-8872-5df698785a4e_story.html).

<sup>305</sup> Madeline Earp, “Al-Jazeera’s Ghada Oueiss on Hacking, Harassment, and Jamal Khashoggi,” *Committee to Protect Journalists* (blog), February 11, 2021, <https://cpj.org/2021/02/ghada-oueiss-hacking-harassment-jamal-khashoggi/>.

<sup>306</sup> Ghada Oueiss, “Opinion | I’m a Female Journalist in the Middle East. I Won’t Be Silenced by Online Attacks,” *Washington Post*, July 9, 2020, <https://www.washingtonpost.com/opinions/2020/07/08/im-female-journalist-middle-east-i-wont-be-silenced-by-online-attacks/>.

A falsified financial document was also posted online purportedly showing that Oueiss had taken cash bonuses from the Qatari government.<sup>307</sup> Throughout, bots attacked her online, calling her a prostitute, often from accounts with pictures of Saudi Crown Prince Mohammed bin Salman, his father, the Saudi flag, or Abu Dhabi's Crown Prince Mohammed bin Zayed.<sup>308</sup>

Oueiss described the psychological effects of the online attacks and her fear of them leading to a physical attack. As a woman, a journalist, and as a Christian, Oueiss felt uniquely vulnerable. She had also been in touch with Khashoggi before his murder. "I was afraid for my life," she told The Committee to Protect Journalists. "I saw what happened to Jamal. I kept looking at the direct messages [he sent me] and thinking, 'Will I be able to go back home, to travel? Will they kill my family, kidnap me?' In the end, I felt I needed professional help."<sup>309</sup>

Oueiss told the Middle East Monitor that it is "...hard to describe how one's life can change overnight for simply doing your job and reporting the truth. Mine and my husband's life will never be the same again, we live in fear and feel we are constantly attacked and watched. We hardly leave the house and almost never talk about personal issues on the phone anymore." Oueiss also said that her mother, who was widowed a few months after the online attack, fears for her and her siblings' lives. "My family's life will never be the same again."<sup>310</sup>

---

<sup>307</sup> "US Court Issues Summons for MBS and MBZ over Hacking of Al Jazeera Anchor," Middle East Eye, accessed November 16, 2022, <http://www.middleeasteye.net/news/us-court-issues-summons-mbs-and-mbz-over-hacking-al-jazeera-anchor>.

<sup>308</sup> Ghada Oueiss, "Opinion | I'm a Female Journalist in the Middle East. I Won't Be Silenced by Online Attacks."

<sup>309</sup> Earp, "Al-Jazeera's Ghada Oueiss on Hacking, Harassment, and Jamal Khashoggi."

<sup>310</sup> "Ghada Oueiss: 'Saudi Has Based Its Rule on the Suppression of Women' – Middle East Monitor," accessed November 16, 2022, <https://www.middleeastmonitor.com/20210210-ghada-oueiss-saudi-has-based-its-rule-on-the-suppression-of-women/>.

Oueiss ultimately hired a lawyer to help her collect evidence and file a lawsuit in 2021 in the state of Florida, which she credits for helping her maintain her mental health.<sup>311</sup> According to the court filing, Oueiss says she was targeted by the Saudi and Emirati leaders because of her reporting on human rights violations.<sup>312</sup> The lawsuit names Saudi Crown Prince Mohammed bin Salman, Abu Dhabi Crown Prince Mohammed bin Zayed, and the UAE-based cybersecurity firm DarkMatter as co-conspirator, among others, for involvement in the hack and subsequent leak.<sup>313</sup>

### Ben Hubbard

Ben Hubbard is a New York Times correspondent and Beirut bureau chief who covers the Middle East. He has lived for over a dozen years in the Middle East, including in Egypt, Iraq, Lebanon, Syria, and Yemen. He has written extensively about Saudi Arabia and authored a biography about the crown prince that was published in 2020.

Hubbard has been targeted at least four times with Pegasus spyware. He was sent two suspicious-looking text messages with links in 2018, one in iMessage, and the other in WhatsApp. Since he did not click on the links, his phone was not infected. However, his phone was successfully infected twice via “zero-click” exploits in 2020 and 2021, as confirmed by Citizen Lab. In the case of the second infection, the operator attempted to delete fingerprints from the first infection.

Citizen Lab has “high confidence” that Pegasus was used all four times. Saudi Arabia likely orchestrated the first two attacks because they used servers that had

---

<sup>311</sup> Earp, “Al-Jazeera’s Ghada Oueiss on Hacking, Harassment, and Jamal Khashoggi.”

<sup>312</sup> “US Court Issues Summons for MBS and MBZ over Hacking of Al Jazeera Anchor.”

<sup>313</sup> Earp, “Al-Jazeera’s Ghada Oueiss on Hacking, Harassment, and Jamal Khashoggi.”

previously targeted several Saudi activists. It is less clear which country was responsible for the 2020 and 2021 attacks, though the second one used an account that had also targeted a Saudi activist. NSO Group denied that Hubbard was the target of Pegasus by any of NSO's customers and cited two additional reasons that it was not involved: it did not have the technology described in the 2018 attempts and Hubbard could not be the target due to unspecified "technical and contractual reasons and restrictions."

Hubbard was not surprised to be targeted but noted that it had caused him to lose sleep thinking about what was compromised. He is not aware of his targeting affecting any of his contacts. He said that he now limits the amount of information he keeps on his phone, uses Signal to limit what a hacker can find, uses a U.S. number (which NSO Group is prevented from targeting), and reboots his phone often to kick out some spy programs. He also leaves his phone behind when meeting people face to face.<sup>314</sup>

---

<sup>314</sup> Hubbard, "I Was Hacked. The Spyware Used Against Me Makes Us All Vulnerable."

## Chapter XI.

### United Arab Emirates

The UAE experienced very limited unrest during the Arab uprisings owing to wealth that shielded it from economic pressures and a one-time monetary concession in the amount of \$1.6 billion for infrastructure projects in the poorer northern emirates.<sup>315</sup> The one notable protest movement – a petition calling for universal suffrage that accumulated 133 signatures – was handled quickly and quietly. The UAE dissolved the elected boards of the Jurists’ and Teachers’ Associations, and police arrested five dissidents associated with the petition in April and blocked their website, UAE Hewan.<sup>316</sup>

The “UAE five,” as they were known, were charged with defamation of Emirati heads of state and for running an “anti-government” website that expressed anti-government views. Their arrests received widespread media coverage and attention from human rights groups. While in detention, the five went on hunger strike for two weeks to protest their treatment. In November, the court reached a decision: as the supposed mastermind, Ahmed Mansour was sentenced to three years in prison, while Nasser bin Ghaith, Fahad Salim Dalk, Hassan Ali al-Khamis, and Ahmed Abdul Khaleq received two years each. In a welcome move, the five men received a presidential pardon from Sheikh Khalifa bin Zayed the day after sentencing and were released.<sup>317</sup> As demonstrated

---

<sup>315</sup> Yasmina Abouzzohour, “Heavy Lies the Crown: The Survival of Arab Monarchies, 10 Years after the Arab Spring,” *Brookings* (blog), March 8, 2021, <https://www.brookings.edu/blog/order-from-chaos/2021/03/08/heavy-lies-the-crown-the-survival-of-arab-monarchies-10-years-after-the-arab-spring/>.

<sup>316</sup> Angela Shah, “Why the Arab Spring Never Came to the UAE,” *Time*, July 18, 2011, <https://content.time.com/time/world/article/0,8599,2083768,00.html>.

<sup>317</sup> “Five Jailed UAE Activists ‘Receive Presidential Pardon,’” *BBC News*, November 28, 2011, sec. Middle East, <https://www.bbc.com/news/world-middle-east-15922492>.

in the case of the UAE five, the UAE was already engaging in digital repression in 2011, and as of 2021, it surpassed Saudi Arabia according to the Digital Repression Index.

The persecution of online users has been a persistent feature since the Arab uprisings, with laws that enabled steep penalties and jail sentences.<sup>318</sup> In 2011, the UAE passed legislation criminalizing the criticism of authorities online or calls for a different ruling system. Statements that offend the state, its rulers, or state symbols were also banned. The law was expanded in 2017 to criminalize sympathy or support for Qatar. The penal code is also used to justify the punishment of public “insults” against leadership. The UAE also passed a law in 2015 prohibiting hate speech, including steep fines of \$14,000-550,000 and jail terms of six months to over 10 years for insulting protected religious symbols.<sup>319</sup> In 2021, a data protection law took effect that raises additional concerns for user privacy.<sup>320</sup>

One of the members of the UAE five, Ghaith, has been charged with breaking several of these laws and regulations. He was arrested again and held incommunicado from August 2015 until April 2016 for “committing hostile acts against a foreign state” because of tweets criticizing Egypt’s treatment of political prisoners.<sup>321</sup> He was found guilty of this charge, in addition to charges for tweets concerning religious tolerance and unjust treatment during a previous trial that, respectively, violated the cybercrime law and damaged the state’s reputation. He was sentenced to 10 years in prison in 2017, which he

---

<sup>318</sup> Sanja Kelly et al., “Freedom on the Net 2014, Tightening the Net: Governments Expand Online Controls.”

<sup>319</sup> Freedom House, “United Arab Emirates: Freedom on the Net 2016 Country Report” (Freedom House, 2016), <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2016>.

<sup>320</sup> Freedom House, “United Arab Emirates: Freedom on the Net 2022 Country Report” (Freedom House, 2022), <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2022>.

<sup>321</sup> Freedom House, “United Arab Emirates,” 2016.

is presently serving.<sup>322</sup> Another member of the UAE five targeted for online activism, Ahmed Mansour, is profiled below.

The UAE actively blocks websites and engages in disinformation and misinformation campaigns. Prohibited content includes terrorism, pornography, and gambling, but political speech is also blocked, including on sites that criticize the government or discuss social taboos. The government also blocks Voice Over Internet Protocol (VoIP) apps in part as a protectionist measure for the state-supported telecommunications infrastructure.<sup>323</sup> From 2019-2021, Freedom House documented how the UAE government used automated and pro-government social media accounts to manipulate information around themes including the coronavirus, Tunisia, Sudan, and the Russia-Ukraine conflict.<sup>324</sup>

The UAE has been using passive surveillance for well over a decade. Abu Dhabi commissioned a safe city surveillance project in the 2000's using Israeli technology called "Falcon Eye;" the project launched in 2013 using facial and license plate recognition technology that means that "every person is monitored from the moment they leave their doorstep to the moment they return to it."<sup>325</sup> In 2015, the UAE's Telecommunications Regulatory Authority announced that it had started monitoring social media for inappropriate and abusive behavior. The monitoring includes an alert system for certain keywords which, if triggered, will initiate an investigation and efforts

---

<sup>322</sup> Freedom House, "United Arab Emirates: Freedom on the Net 2018 Country Report" (Freedom House, 2018), <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2018>.

<sup>323</sup> Freedom House, "United Arab Emirates: Freedom on the Net 2017 Country Report" (Freedom House, 2017), <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2017>.

<sup>324</sup> Freedom House, "United Arab Emirates," 2022.

<sup>325</sup> Rori Donaghy, "Falcon Eye: The Israeli-Installed Mass Civil Surveillance System of Abu Dhabi," *Middle East Eye*, July 15, 2015, <http://www.middleeasteye.net/news/falcon-eye-israeli-installed-mass-civil-surveillance-system-abu-dhabi>.

to remove the content.<sup>326</sup> In 2016 it was revealed that BAE Systems sold deep packet inspection equipment to the UAE dating back to at least 2014, as it had to Saudi Arabia.<sup>327</sup>

Table 7. The UAE's Freedom on the Net and Digital Repression Index Scores

|                          | 2011 | 2013 | 2021 | Trend |
|--------------------------|------|------|------|-------|
| Freedom on the Net       | --*  | 66   | 73   | ↑     |
| Digital Repression Index | 1.62 | --   | 1.84 | ↑     |

*\*Freedom on the Net (FOTN) did not profile the UAE in 2011; the country was first included in the report in 2013. FOTN scores on a scale of 0-100, with 100=least free. The Digital Repression Index (DRI) scale is -5 to 5, with 0 representing the country-mean across variables for the year assessed. A positive score indicates that a country is performing above the mean across all DRI variables.*

The UAE was also one of the early adopters of targeted surveillance technology in the MENA region. Evidence has emerged that the UAE purchased spyware from FinFisher, Hacking Team, NSO Group, and Candiru. Citizen Lab analysis on the UAE dissident Ahmed Mansour concluded that he was targeted by three different brands of spyware. These findings give examples of the earliest uses of the spyware in the UAE and the broader region.<sup>328</sup>

FinFisher was the first commercial spyware that the UAE used to target Ahmed Mansour in March 2011. He received a message containing an attachment that was an

<sup>326</sup> "UAE in Crackdown on Social Media Abuse - Arabian Business," *Arabian Business*, March 10, 2015, <https://www.arabianbusiness.com/industries/technology/uae-in-crackdown-on-social-media-abuse-585044>.

<sup>327</sup> Jenna McLaughlin, "BAE Systems Sells Internet Surveillance Gear to United Arab Emirates," *The Intercept*, August 26, 2016, <https://theintercept.com/2016/08/26/bae-systems-sells-internet-surveillance-gear-to-united-arab-emirates/>.

<sup>328</sup> Freedom House, "United Arab Emirates," 2016.

EXE file disguised as a PDF of a pro-democracy petition that he had already signed. He did not open it but instead submitted it for forensic analysis.

The UAE also used Hacking Team spyware again against Mansour in July 2012, using a Microsoft Word document that hid an exploit that allowed UAE intelligence to break into Mansour's email account.<sup>329</sup> Two years later, in 2014, Citizen Lab found digital evidence that the UAE was a Hacking Team operator.<sup>330</sup> A Hacking Team document leaked in 2015 confirmed what human rights groups and defenders already knew: that UAE was a big customer. The UAE paid the company over \$634,500 for the use of spyware to target 1,100 devices since 2011. The purchase was facilitated by U.S.-based CyberPoint,<sup>331</sup> which had previously received a license from the State Department to provide advice on cyber defense and policy to the Emirates.<sup>332</sup> In 2016, it was reported that the Hacking Team no longer sold to the Emirates because the company's global license was revoked by the Italian Ministry of Economic Development.<sup>333</sup> It is unknown whether a new export license was obtained and cooperation continued.

Mansour was also targeted with Pegasus in August 2016. The UAE has used Pegasus in some high-profile instances beyond Mansour, including the UK Prime Minister's Office at 10 Downing,<sup>334</sup> and the family of Sheikh Mohammed bin Rashid Al

---

<sup>329</sup> Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender" (University of Toronto, August 24, 2016), <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>.

<sup>330</sup> Marczak et al., "Mapping Hacking Team's 'Untraceable' Spyware."

<sup>331</sup> Lee Fang, "Why Did the Firm That Sold Spyware to the UAE Win a Special Export License From State Department?," *The Intercept*, July 7, 2015, <https://theintercept.com/2015/07/07/baltimore-firm-supplying-united-arab-emirates-surveillance-software-won-special-export-license-state-department/>.

<sup>332</sup> Ellen Nakashima, "As Cyberwarfare Heats up, Allies Turn to U.S. Companies for Expertise," *Washington Post*, November 22, 2012, sec. National Security, [https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c\\_story.html](https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c_story.html).

<sup>333</sup> Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents."

<sup>334</sup> Ron Deibert, "UK Government Officials Infected with Pegasus" (Citizen Lab, University of Toronto, April 18, 2022), <https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/>.

Maktoum, which the sheikh himself authorized. The UAE has also targeted individuals seemingly in coordination with Saudi Arabia, such as the 34 Al Jazeera employees and Khashoggi's wife, Hanan Elatr.

As the chapter on Saudi Arabia showed, Israeli leadership had a bias for keeping Pegasus running in the kingdom, as it was seemingly important to the relationship between Riyadh and Jerusalem. The same can be said for the role of the spyware in the Israeli-Emirati relationship. Israel authorized the sale of Pegasus to the UAE in 2013 following the poisoning of a senior Hamas operative in a Dubai hotel room in 2010 as a peace offering. Crown Prince Mohammed bin Zayed, the de facto Emirati leader, was incensed that the assassination took place on Emirati soil, and he readily accepted the Israeli technology.<sup>335</sup> In September 2020, the UAE, Bahrain, and Israel signed the U.S.-sponsored Abraham Accords to normalize relations between the Arab states and Israel, which Morocco later joined.<sup>336</sup> The use of the spyware to foster the rapprochement has been dubbed “Pegasus diplomacy” by some who criticize the use of arms sales for foreign policy gains.<sup>337</sup>

The UAE has two contracts with NSO Group: one sold to Abu Dhabi ruler Mohammed bin Zayed in 2013, and the other to Dubai ruler Sheikh Mohammed bin Rashid al-Maktoum. Haaretz offers two theories to explain why a country with a joint federal military, police and security force need to separate systems: either the need arose because of internal politics and rivalries between the seven emirates, or because one of

---

<sup>336</sup> Bergman and Mazzetti, “The Battle for the World’s Most Powerful Cyberweapon.”

<sup>337</sup> Ben Lynfield, “Israel’s Rewarding Road to Normalization,” *Foreign Policy*, January 31, 2021, <https://foreignpolicy.com/2022/01/31/israel-abraham-accords-normalization-middle-east/>.

the rulers wanted to use the spyware for personal means.<sup>338</sup> The latter has credence given the stories of Princess Haya, whose phone was hacked 11 times with her estranged husband bin Rashid al-Makhtoum's direction or knowledge (more in chapter V), and Princess Latifa, profiled below. Sources told the Guardian and Washington Post that NSO cancelled its contract with Dubai between 2020-2021 in part because of an investigation that the technology had been used to monitor the sheikh's family.<sup>339</sup>

In contrast to Pegasus, few details are available concerning the UAE's use of Candiru. Citizen Lab has identified the UAE as a Candiru operator, and Kaspersky has observed an overlap between a Candiru exploit and Emirati malware called "Stealth Falcon,"<sup>340</sup> which is described in more detail below.

In addition to commercially purchased spyware, the UAE has developed of its own in-house surveillance capabilities. In addition to the passive surveillance used in the Abu Dhabi Safe City project, it also developed a malware exploit that Citizen Lab dubbed "Stealth Falcon." In its report, Citizen Lab described how the spyware targeted Rori Donaghy, a journalist and founder of the Emirates Center for Human Rights who is based in the UK. Donaghy received a bogus invitation to speak on a panel of human rights experts, which he forwarded for analysis. By analyzing the exploit, Citizen Lab was able to identify other Emirati journalists, activists, and dissidents who had been

---

<sup>338</sup> Eytan Avriel, "Two UAE Princes Each Got Their Own Personal NSO Spyware."

<sup>339</sup> Dan Sabbagh, "Data Leak Raises New Questions over Capture of Princess Latifa," *The Guardian*, July 21, 2021, sec. World news, <https://www.theguardian.com/world/2021/jul/21/data-leak-raises-new-questions-over-capture-of-princess-latifa>.

<sup>340</sup> Marczak et al., "Hooking Candiru."

targeted. Stealth Falcon is believed to have led to the arrests and convictions of at least five targets from 2012-2015.<sup>341</sup>

Stealth Falcon might actually be Project Raven, which became known in recent years. Maryland-based contractor CyberPoint set up a clandestine surveillance team to run Project Raven in Abu Dhabi in 2009. (You may recall that CyberPoint also facilitated the UAE's purchase of Hacking Team spyware.) The premise of the project was that Americans would develop and run the program that hacked into phones and computers for five to ten years until Emirati intelligence officials developed the skills and experience to take over. By 2013, there were between 12-20 American team members at any time with expertise gained from previous work within the U.S. intelligence community, including many from NSA.<sup>342</sup>

Originally, the work focused on helping the UAE's version of the NSA, the Signals Intelligence Agency, track and break up ISIS terror cells in the Emirates. Tracking ISIS proved tricky, and CyberPoint often had to buy different zero-day exploits for the team to keep up with the militants' use of burner phones and different technology platforms.<sup>343</sup> The initial stages in the surveillance cycle – targeting and attack – were handled by separate parts of the team. The Americans would identify vulnerabilities in the targets, and the Emiratis would launch the attack. Targets also included militants in Yemen; foreign adversaries in Iran, Qatar, and Turkey; individuals who insulted the monarchy on social media; and dissidents and human rights activists that the Emiratis

---

<sup>341</sup> Bill Marczak and John Scott-Railton, "Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents" (University of Toronto, May 29, 2016), <https://citizenlab.ca/2016/05/stealth-falcon/>.

<sup>342</sup> Christopher Bing and Joel Schectman, "Special Report: Inside the UAE's Secret Hacking Team of U.S. Mercenaries," *Reuters*, January 30, 2019, sec. Special Reports, <https://www.reuters.com/article/us-usa-spying-raven-specialreport-idUSKCN1PO190>.

<sup>343</sup> Perlroth, *This Is How They Tell Me the World Ends*, 159.

categorized as national security targets.<sup>344</sup> Former CyberPoint employee David Evenden said he was asked to hack into Qatari systems to determine whether Qatar was funding the Muslim Brotherhood or if Qatar had bribed FIFA officials to win hosting the 2022 tournament, though he noted that his Emirati bosses showed no interest in shutting down the infiltration when no evidence was found.<sup>345</sup>

Evenden also told New York Times journalist and author Nicole Perlroth that his Emirati bosses had asked him to create a template for determining whether a target had terrorist connections. Evenden created such a message containing an exploit, and later became aware that his draft, which was never supposed to be sent, had been emailed to Donaghy. As a result, he said that “CyberPoint’s digital fingerprints were all over the hacks of some four hundred people around the world, including several Emiratis, who were picked up, jailed, and thrown into solitary confinement for daring to insult the state on social media or even so much as questioning the ruling monarch in their most intimate personal correspondence.” Evenden dismissed the red flags until he saw that the project’s targeting had produced correspondence concerning First Lady Michelle Obama’s trip to Qatar in 2015.<sup>346</sup>

By 2015, UAE officials had become increasingly uncomfortable with having foreigners at the core of their surveillance project, and the project transitioned from CyberPoint to DarkMatter, a UAE LLC. Project members were told to either join DarkMatter or go home. In early 2016, DarkMatter purchased a zero-day exploit and an operating system for \$1.3 million from two U.S. companies according to a court report.

---

<sup>344</sup> Christopher Bing and Joel Schectman, “Special Report.”

<sup>345</sup> Perlroth, *This Is How They Tell Me the World Ends*, 159–60.

<sup>346</sup> Perlroth, 161.

Project Raven employees came to call the new technology Karma.<sup>347</sup> Karma is no-click spyware that breaks into iPhones. Between 2016-2017, it was used to target hundreds of individuals across the MENA region, including the iPhone of the Emir of Qatar, Sheikh Tamim bin Hamad al-Thani, along with the phones of his close associates and his brother.<sup>348</sup>

At least eight team members left Project Raven after Emiratis took the reins, some citing concern over vague responses about the targeting of Americans.<sup>349</sup> At least two have commented publicly that they filed tips with the FBI about the project. In September 2021, three former U.S. intelligence community and military personnel that decided to continue their employment with DarkMatter were tried in the United States; they entered into a deferred prosecution agreement with the Justice Department that restricts future activities and employment and requires that they pay more than \$1.68 million in penalties for violating U.S. export control, computer fraud, and access device fraud laws.<sup>350</sup>

Five spyware victims are highlighted below. They were targeted by FinFisher, Hacking Team, NSO, and Project Raven surveillance.

#### Ahmed Mansour

Ahmed Mansour is an Emirati engineer, poet, and human rights defender that Citizen Lab has described as the “million-dollar dissident” given the cost of targeting him

---

<sup>347</sup> Joseph Cox, “U.S. Company Sold Zero-Click Hacking Tool to UAE Spy Operation,” *Vice* (blog), September 14, 2021, <https://www.vice.com/en/article/3aq9a5/us-company-sold-zero-click-exploit-project-raven-uae>.

<sup>348</sup> Christopher Bing and Joel Schectman, “Special Report.”

<sup>349</sup> Christopher Bing and Joel Schectman.

<sup>350</sup> Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than \$1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government (U.S. Department of Justice September 14, 2021).

with at least three different types of spyware. He campaigned from 2006 to 2007 for the release of two people jailed for making critical social comments, and regularly raised concerns about arbitrary detention, torture, and due process. In 2011, he was detained for eight months for organizing a petition that called for a constitutional monarchy and was pardoned the day after receiving a three-year prison sentence.<sup>351</sup>

Mansour was targeted by the Emiratis using FinFisher spyware in 2011, Hacking Team spyware in 2012, and Pegasus in 2016.<sup>352</sup> Each time that he suspected being targeted, he reached out to Citizen Lab for analysis. Following the Pegasus infection, which was made public and prompted Apple to push a security patch to all users, Mansour's car was stolen, his email account was hacked, his passport was confiscated, and \$140,000 was stolen from his bank account. He lost his job and faced physical attacks from strangers. He was the subject of repeated smear campaigns in the media and was called an Iranian agent or terrorist, "despite the fact that you don't even know how to put a bullet in a gun." He was besieged: "You start to believe your every move is watched...[and] your family starts to panic. I have to live with that."<sup>353</sup>

Mansour told New York Times author and journalist Nicole Perlroth in 2015 that the surveillance "...is as bad as someone encroaching in your living room, a total invasion of privacy, and you begin to learn that maybe you shouldn't trust anyone anymore." Years later, she learned that CyberPoint had not only attacked Mansour's

---

<sup>351</sup> "Ahmed Mansoor Selected as the 2015 Laureate Martin Ennals Award for Human Rights Defenders," Amnesty International, October 6, 2015, <https://www.amnesty.org/en/latest/press-release/2015/10/ahmed-mansoor-selected-as-the-2015-laureate-martin-ennals-award-for-human-rights-defenders/>.

<sup>352</sup> Marczak and Scott-Railton, "The Million Dollar Dissident."

<sup>353</sup> Bergman and Mazzetti, "The Battle for the World's Most Powerful Cyberweapon."

phones but had also targeted his wife's devices and implanted themselves into their child's baby monitor. They also listened to Mansour and Perlroth's interview.<sup>354</sup>

In March 2017, Mansour was arrested for "spreading sectarianism and hatred on social media" after his tweet calling for the release of activist Osama al-Najjar. He remained in detention for more than a year and, following a secret trial in which he had no access to a lawyer, received a sentence of 10 years' imprisonment in May 2018 for cybercrimes. He has been held in solitary confinement without a bed or mattress, and the latest reports state that his health is declining.<sup>355</sup>

#### Latifa al Makhtoum

Princess Latifa bint Mohammed al Maktoum is the daughter of Sheikh Mohammed bin Rashid al Maktoum, the ruler of Dubai and Prime Minister and Vice President of the UAE. She has reportedly been prevented from traveling abroad since 2000 and her requests to travel, study, or "do anything normal" were denied.<sup>356</sup> According to the website #FreeLatifa, the princess first tried to flee Dubai in 2002 at the age of 16. She was caught at the border with Oman and returned to Dubai where she spent three and a half years in arbitrary detention at the Nad Al-Sheba prison.<sup>357</sup> In a video released in 2018, she said that she had been beaten and tortured during those years and was also forcibly injected with sedatives. One of her captors reportedly told her, "Your father told us to beat you until we kill you."<sup>358</sup>

---

<sup>354</sup> Perlroth, *This Is How They Tell Me the World Ends*, 184–85.

<sup>355</sup> Perlroth, 185.

<sup>356</sup> Jane McMullen, "Princess Latifa: The Dubai Ruler's Daughter Who Vanished," *BBC News*, February 16, 2021, sec. Middle East, <https://www.bbc.com/news/world-middle-east-56085369>.

<sup>357</sup> "Learn More About Princess Latifa Of Dubai - Missing Since March 2018," #FreeLatifa (blog), accessed January 16, 2023, <https://freelatifa.com/about-latiifa/>.

<sup>358</sup> Sabbagh, "Data Leak Raises New Questions over Capture of Princess Latifa."

Princess Latifa again attempted to flee Dubai in March 2018 in an elaborate escape that garnered international attention. Since she had no passport, she slipped out of Dubai and drove with a friend to the coast of Oman, where they took a dinghy and a jet ski 13 miles to reach international waters where a yacht was waiting for them. Her goal was to cross the Indian ocean and fly to the United States to request asylum.<sup>359</sup>

The day after she went missing from Dubai, the princess's number was added to the Pegasus target list, though she had left it behind on a table in a cafe. As she was traveling toward India on a yacht, she was texting two friends, Lynda Bouchiki and Sioned Taylor; it was later discovered that her friends' numbers had also been added to the Pegasus list. The dates and times they were added led journalist Paul Lewis of The Guardian to conclude, "You have something more than a coincidence." Eight days after Latifa's escape, Indian forces authorized by Indian Prime Minister Modi who were acting on Dubai's request boarded the yacht just off the Indian coast.<sup>360</sup> They used smoke grenades to force the princess and her friends from their hiding places below deck. Princess Latifa asked them to kill her instead of taking her back, and she was tranquilized and transferred to an Indian military ship and to Emirati special forces who took her by private jet back to Dubai.<sup>361</sup>

The Guardian was unable to check Bouchiki and Taylor's phones but was able to confirm that her friend David Haigh's phone had been infected with Pegasus. Haigh had

---

<sup>359</sup> Jane McMullen, "Princess Latifa."

<sup>360</sup> "Global Spyware Scandal: Exposing Pegasus," *FRONTLINE* (PBS, January 3, 2023), <https://www.pbs.org/wgbh/frontline/documentary/global-spyware-scandal-exposing-pegasus/>.

<sup>361</sup> Jane McMullen, "Princess Latifa."

been in daily conversations with Latifa and was alarmed when she went dark following her capture on the yacht.<sup>362</sup>

A year after her capture, she sent videos to her friends describing her capture and return to Dubai where she was being held in a secret, boarded up villa that was guarded by police. The princess said that she did not have access to medical or legal help. Over the course of several months, she sent these videos via a secret phone from the bathroom of the villa, which was the only room with a lock on the door. Then the contact stopped. Her friends released the videos to the BBC, and Panorama broadcast them in February 2021 citing concern that the princess was in grave danger.<sup>363</sup>

A few photos of Princess Latifa emerged in May 2021 on social media in locations around Dubai. Her blank expressions led her friends and former Foreign Office Minister Peter Hain to renew calls for proof of life and for her freedom. There was precedent for concern: the princess had previously appeared in a staged photo with former UN High Commissioner for Human Rights and Irish president Mary Robinson in December 2018; Robinson later said she had made the “worst mistake of her life” and had been “horribly tricked” to appear in the photo cover-up at a time when the princess was being arbitrarily detained.<sup>364</sup>

New photos emerged again in August 2021 of the princess in Iceland and Spain, and the #FreeLatifa campaign has reportedly disbanded.<sup>365</sup> Princess Latifa also met with UN High Commissioner Michelle Bachelet in November 2021 to convey that she is well,

---

<sup>362</sup> “Global Spyware Scandal.”

<sup>363</sup> “Princess Latifa: ‘Hostage’ Ordeal of Dubai Ruler’s Daughter Revealed,” *Panorama* (BBC, February 16, 2021), <https://www.bbc.com/news/world-middle-east-56075528>.

<sup>364</sup> Samuel Osborne, “Princess Latifa: New Photo Emerges of Dubai Royal in Iceland as Campaign to Free Her Is Disbanded,” *Sky News*, August 10, 2021, <https://news.sky.com/story/princess-latifa-new-photo-emerges-of-dubai-royal-in-iceland-as-campaign-to-free-her-is-disbanded-12377367>.

<sup>365</sup> Samuel Osborne.

is free to travel, and wants respect for her privacy. She also sent a statement to Sky News confirming that the meeting with Bachelet was intended “to assert her right to a private life, following persistent media speculation about her.” It is believed that she must have reached some sort of accommodation with her father that facilitated her release.<sup>366</sup>

#### Hanan Elatr

Hanan Elatr is the widow of Jamal Khashoggi, who was murdered at the hands of a Saudi paramilitary team in the Saudi Consulate in Istanbul in October 2018. Earlier that year, in April, Elatr was returning on a work trip from Toronto to the Dubai as a flight attendant on Emirates Airlines. Upon arrival, she was met by an Emirati intelligence officer and a woman who confiscated her bags, her two Android phones, her laptop, and passwords. She was interrogated for the better part of a day about her fiancé at the time, Khashoggi, and then driven blindfolded and handcuffed to her home where she was placed under house arrest. “In Middle East [sic], you have no choice. Either you comply with them, or they beat you and torture you,” she said. The ordeal made her feel “very ill” and “panicked,” and she was uncomfortable with the idea of them seeing the love letters that she and her fiancé had shared with one another.<sup>367</sup>

Forensic analysis by Citizen Lab showed that someone opened the Chrome browser on one of her phones in April 2018 while it was still in official custody and proceeded to type an address – making two typos along the way – that downloaded

---

<sup>366</sup> Adela Suliman, “Dubai’s Princess Latifa Tells U.N. She Is ‘Well’ during Meeting with Human Rights Chief in Europe,” *Washington Post*, February 19, 2022, <https://www.washingtonpost.com/world/2022/02/19/princess-latifa-michelle-bachelet-human-rights-dubai/>.

<sup>367</sup> Dana Priest, “UAE Agency Put Pegasus Spyware on the Phone of Hanan Elatr, Jamal Khashoggi’s Wife,” *Washington Post*, December 21, 2021, <https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/>.

Pegasus on her phone. Her phones were returned to her several days after her release. Bill Marczak of Citizen Lab hailed the Pegasus proof as a “smoking gun” that challenges NSO Group’s claims that Khashoggi, his family, and his friends were not targeted as part of the heinous crime. NSO continues to deny its involvement. The company’s attorney, Thomas Clare, said “The Post’s continued efforts to falsely connect NSO Group to the heinous murder of Mr. Khashoggi are baffling.”<sup>368</sup>

Elatr and Khashoggi married in June 2018. He tried to call her the day before he was killed in Istanbul. Now aware of the presence of spyware on her devices, she feels terrible about how they used her to extract information that ultimately helped trap and kill her fiancé in Istanbul. Both Elatr and Turkish fiancée Cengiz, who did not know about each other before his murder, had full lives before their romantic relationships with Khashoggi. However, now both live in hiding.<sup>369</sup> “Every day I see the sunlight, I don’t know why I’m still alive... because I’m the second victim after Jamal in this tragedy. I’ve lost my life,” Elatr said.<sup>370</sup>

#### Rori Donaghy

Rori Donaghy is based in London and is a former director and founder of the Emirates Centre for Human Rights from 2012-2014 and a news editor at Middle East Eye from 2014-2016. He has published several articles critical of the UAE government, including a series for Middle East Eye based on leaked emails involving UAE government members and an opinion piece for the Guardian in 2012.

---

<sup>368</sup> Dana Priest.

<sup>369</sup> Priest, Mekhennet, and Bouvart, “Jamal Khashoggi’s Wife Targeted with Spyware before His Death.”

<sup>370</sup> Dana Priest, “UAE Agency Put Pegasus Spyware on the Phone of Hanan Elatr, Jamal Khashoggi’s Wife.”

Donaghy became a key target of Project Raven in 2012, when it was under CyberPoint leadership. Using social engineering, a project team member sought to “ingratiate himself to the target by espousing similar beliefs... [that Donaghy] would be unable to resist.” Donaghy was convinced to download software that would make his messages “difficult to trace” that was actually malware that facilitated the monitoring of Donaghy’s email account and internet browsing. The monitoring was confirmed from 2012-2015 per Citizen Lab, whom Donaghy reached out to when he received another suspicious email in 2015.<sup>371</sup>

Donaghy was not surprised to learn of the spyware: “Once you dig beneath the surface, you find an autocratic state, with power centralized among a handful of people who have increasingly used their wealth for surveillance in sophisticated ways.”<sup>372</sup> He posted the following on LinkedIn in 2021:

I was a bit freaked out when the FBI and US Dept of Justice contacted me out of the blue a couple weeks back.

But when I found out that they were contacting me to say that three Americans were being charged with hacking me - among many far more vulnerable people - on behalf of the UAE Government, I was delighted.

I’m happy to see the wheels of justice moving - but there’s so much more to do on preventing governments from abusing the power that comes with cyber surveillance tools.<sup>373</sup>

#### Alaa al-Siddiq

Alaa al-Siddiq was a human rights defender and Executive Director of ALQST, a nonprofit that highlighted human rights violations in the Gulf. She was also the daughter

---

<sup>371</sup> Christopher Bing and Joel Schectman, “Special Report.”

<sup>372</sup> Perlroth, “Governments Turn to Commercial Spyware to Intimidate Dissidents.”

<sup>373</sup> Rori Donaghy, “Post | Feed | LinkedIn,” Social media, LinkedIn, accessed January 16, 2023, <https://www.linkedin.com/feed/update/urn:li:activity:6843634248063164417/>.

of Mohamed al-Siddiq, who was arrested in late 2011, held in detention, and sentenced to 10 years in prison in July 2013 for plotting to overthrow the UAE government. He was one of 56 lawyers, judges, and activists convicted for signing a petition that called for a representative parliament in the UAE. Police questioned Alaa al-Siddiq about her father in the months after his arrest, and she fled the UAE for Qatar several months later where she requested asylum with her husband.<sup>374</sup>

Emirati officials sought to forcibly return Alaa al-Siddiq to the UAE, and she became a central figure in their diplomatic dispute. In 2015, Sheikh Mohammed bin Abdulrahman bin Jassim Al Thani, Qatar's Deputy Prime Minister and Minister of Foreign Affairs, said Abu Dhabi had sent an envoy to meet him to request that she be handed over to Emirati authorities. The request was denied, as was another formal request in 2017,<sup>375</sup> adding to the growing rift between the two countries. The Emiratis stripped her of her passport, she was subjected to smear campaigns in which she was called a terrorist, and she ultimately fled to the UK in 2020.

Al-Siddiq initiated contact with Citizen Lab and learned in 2020 that she had been targeted multiple times with Pegasus in 2015, with forensic fingerprints pointing to the UAE. Her new UK phone numbers were also successfully targeted several times in 2020. Brian Dooley, Senior Advisor to the UN Special Rapporteur on Human Rights Defenders, noted that these successful infections happened despite her excellent "digital hygiene." Her daily routine involved three phones: a regular phone, one for work, and a

---

<sup>374</sup> "Prominent UAE Activist Alaa Al-Siddiq Dies in UK Car Crash," *Aljazeera*, June 20, 2021, <https://www.aljazeera.com/news/2021/6/20/prominent-emirati-activist-dies-in-london-car-crash>.

<sup>375</sup> *An Exclusive Interview with His Excellency the Deputy Prime Minister and Minister of Foreign Affairs - #Al-Haqiqa # 10/1/2018*, Al Haqiqa (Qatar Television, 2018), <https://www.youtube.com/watch?v=IP908poMGIE>.

burner phone for very sensitive outreach when she felt her devices were compromised. He said that Al-Siddiq fretted about whether to save new people she met as contacts in her phone.<sup>376</sup>

Contacts and friends described al-Siddiq as changed but resilient after learning of the hack. She gave an interview to the UK-based research group Forensic Architecture soon after she learned of the surveillance, and she described how her research had likely made her a target. She worried that the spyware might expose people that trusted her and supported her research: “In this case, this kind of violation is not changeable, and I cannot protect them. It is a sad thing to feel,” she said. She also told Citizen Lab’s Bill Marczak that she was worried that the UAE government would leak her family photos.

Al-Siddiq died in a car crash in June 2021. No foul play is suspected, as it was a two-car collision and there were injuries in both cars. One of her friends who was riding with her and survived the crash told the Guardian that al-Siddiq changed her habits after learning of the hack, including not standing too close to the edge of the tube platform in case someone tried to push her onto the tracks. Worrying about her devices “...was part of her daily life...[but] she did not surrender to this fear...she was really fierce.”<sup>377</sup>

---

<sup>376</sup> Brian Dooley, Interview by author, January 16, 2023.

<sup>377</sup> Stephanie Kirchgaessner, “New Evidence Suggests Spyware Used to Surveil Emirati Activist Alaa Al-Siddiq,” *The Guardian*, September 24, 2021, sec. World news, <https://www.theguardian.com/world/2021/sep/24/new-evidence-suggests-spyware-used-to-surveil-emirati-activist-alaa-al-siddiq>.

## Chapter XII.

### Results

Each time you looked at how the client of NSO Group used the technology, it tells you something about that government.

-- Paul Lewis, *The Guardian*<sup>378</sup>

How has spyware used by governments in the MENA region affected the human rights of those living in the region and beyond since the Arab uprisings? Except in Lebanon, profiled individuals described worsening human rights, though it is difficult to blame spyware by itself. Individuals were typically subjected to spyware and other forms of digital and physical repression in parallel, such as smear campaigns and government-sponsored trolling, harassment by security forces, arbitrary detention, travel bans, asset freezes, and loss of employment.

Many individuals in the MENA region described the chilling effects of spyware: they were more likely to self-censor as a result and choose their words more carefully. Similar to Penney's findings, these individuals changed their behavior "...out of concern for potential future harms due to privacy violations, embarrassing public disclosures, risks of fraud or identity theft, or being labeled a criminal, deviant, or non-conformist by state authorities."<sup>379</sup> They were also more hesitant to circulate outside their homes and make new social connections that may result in surveillance by association. Spyware made it more difficult for individuals to live lives that are true to themselves, a core

---

<sup>378</sup> "Global Spyware Scandal."

<sup>379</sup> Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," SSRN Scholarly Paper (Rochester, NY, 2016), 164, <https://papers.ssrn.com/abstract=2769645>.

desire expressed by Mozn Hassan. In the most horrific cases, as seen with the murder of Jamal Khashoggi, this targeting resulted in the arbitrary deprivation of life, and in cases such as Ahmed Mansour's, it led to prolonged imprisonment in deplorable conditions.

These findings are corroborated by Freedom of the Net and Digital Repression Index scores. Digital repression, which correlates to human rights abuses and violations, has increased in four of the five countries assessed. It is important to note that the Digital Repression Index measures all forms of digital repression except for targeted surveillance, while Freedom on the Net scoring measures similar digital repression tools including targeted surveillance. Only Lebanon has lessened its use of digital repression since the start of the Arab uprisings.

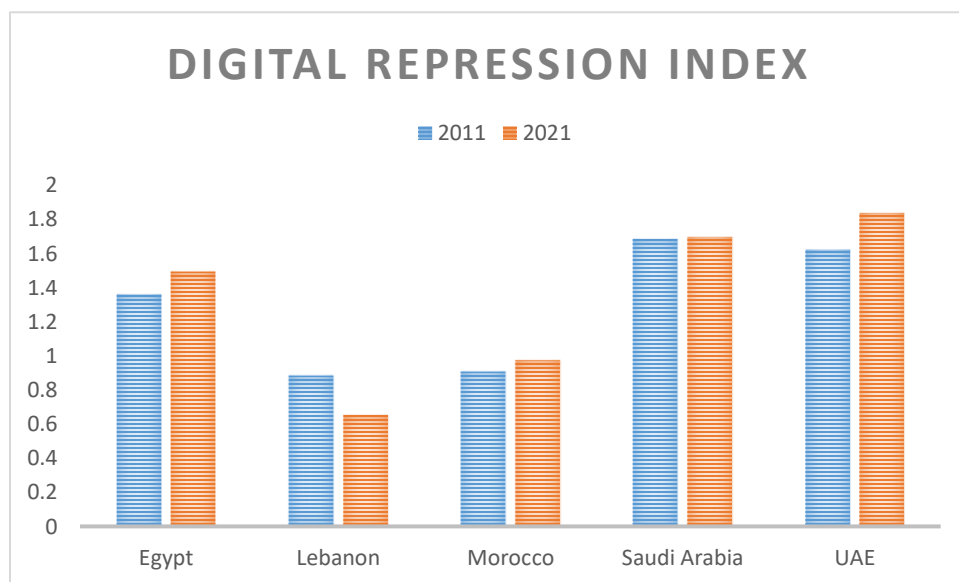


Figure 4. Digital Repression Index Comparison of 2011 and 2021 levels

*Digital repression has grown in four of the five case study countries*

Freedom on the Net stats for the five case study countries show a similar trend of increasing restrictions on the internet except for Lebanon.

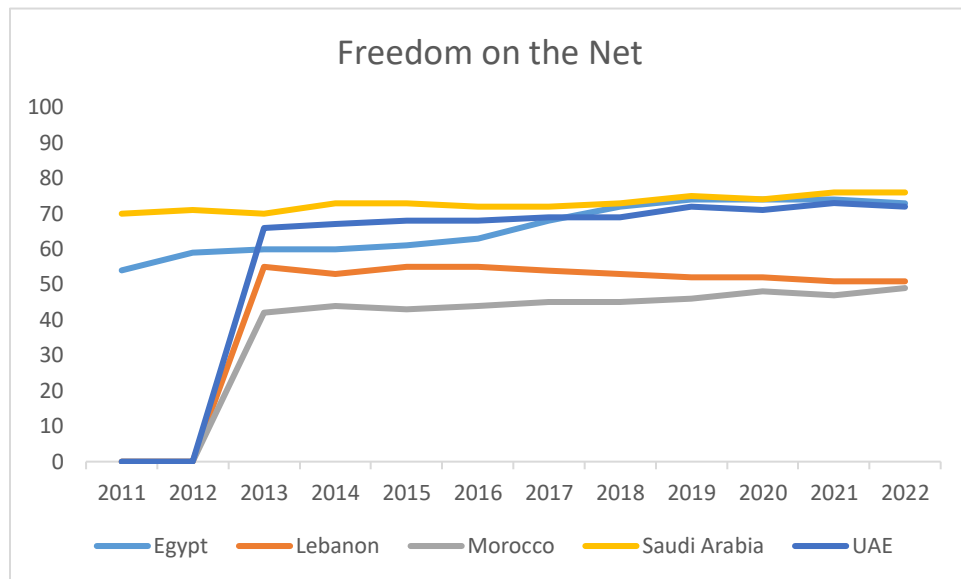


Figure 5. Freedom on the Net for Select MENA Countries

*In this chart, least free=100. Egypt, Morocco, Saudi Arabia, and the UAE all saw increasing restrictions on the internet over the past decade, except for Lebanon, where the internet became freer.*

Individuals profiled in the case studies described their experiences with spyware and digital repression, and their responses suggest that they were deprived of rights that are delineated in the International Bill of Human Rights.<sup>380</sup> This list is non-exhaustive:

- Freedom of association
- Freedom of expression

<sup>380</sup> “OHCHR | International Bill of Human Rights.”

- Freedom of religion and belief
- Freedom from torture
- Right to fair trial
- Right to freedom of movement
- Right to liberty and security of person
- Right to life
- Right to privacy

### Spyware poses a unique risk

Many of the experts I interviewed argued that spyware by governments poses a greater risk than other forms of digital repression and traditional surveillance. First, spyware is not location bound like data-extraction technology.<sup>381</sup> It is seemingly easy to use and does not require high technical capacity, compared to some forms of passive or mass surveillance, such as Russia's use of the System for Operative Investigative Activities (SORM) to intercept and monitor communications at the network level.<sup>382</sup> Spyware replaces the need for law enforcement to dedicate dozens of staff for round-the-clock physical surveillance.<sup>383</sup> Similarly, it obviates the need to surreptitiously break into someone's home to install malware on a computer device, as was done before spyware became available.<sup>384</sup> There are usually few if any fingerprints pointing to state operators

---

<sup>381</sup> Allie Funk, Interview by author, January 26, 2023.

<sup>382</sup> Allie Funk.

<sup>383</sup> Brian Dooley, Interview by author.

<sup>384</sup> "How Western Spyware Helps Dictators with Phillip Adams."

of spyware, making it difficult to seek justice for transnational repression conducted by foreign spyware operators.<sup>385</sup>

Spyware's reach is unprecedented. It allows operators to see over your shoulder, or to be the spy in your pocket, with a greater invasion of privacy than any other tool.<sup>386</sup> It is not restricted to metadata like other forms of surveillance, as it captures and monitors content and everything else on a device. It also provides real-time tracking of the targeted individual's network. An example of this is the likely use of Hanan Elatr's phone to track Jamal Khashoggi's whereabouts.<sup>387</sup>

For the person targeted, spyware is more difficult to remove compared to options to remove problematic content on social media.<sup>388</sup> There are also some preventative steps that individuals can take to protect themselves from other forms of digital repression, but these are less effective with spyware, especially the zero-click variety.<sup>389</sup>

One expert argued that spyware is dangerous but should not be viewed as net new. "When asking whether digital repression is worse now than it was a decade ago, I'd say that the only part of the sentence that is new is the word 'digital'," offered Brian Dooley, Senior Advisor to the Special Rapporteur on Human Rights Defenders. As someone who has worked with human rights defenders for four decades, Dooley said that he sees no difference between targeting now and in the 1980s. He witnessed the pre-internet surveillance of anti-apartheid activists in London in the 1980s, which included mail opening, phone tapping, identifying intimate details for blackmail, and collecting

---

<sup>385</sup> U.S. government official, Interview by author, January 17, 2023.

<sup>386</sup> Manal al-Sharif, Interview by author.

<sup>387</sup> Allie Funk, Interview by author.

<sup>388</sup> U.S. government official, Interview by author, January 17, 2023.

<sup>389</sup> U.S. government official, Interview by author, September 23, 2022.

information from relatives and friends to get at their target. These efforts had the same chilling effect on activists, journalists, and human rights defenders. He also pointed to the assassination attempt on Albie Sachs in Mozambique and Russia's use of poison to silence critics and supposed enemies of the state as examples of physical repression that predated digital surveillance and continues today.<sup>390</sup> "I don't want to underplay the role of digital surveillance, but much of the harm and threat [pre-internet] is similar if not identical to what there is now," he said.<sup>391</sup>

#### Governance systems and use of spyware

In the five countries profiled, each country used spyware in concert with different forms of physical and digital repression, regardless of system of governance.

Furthermore, two of the case study countries demonstrated that any suggested correlation between governance systems and overall level of digital repression is imperfect. Egypt's Freedom on the Net and Digital Repression Index scores are worse than Morocco's, though Egypt is an electoral autocracy and Morocco is a closed autocracy, as shown in Figures 4 and 5.

The case studies illustrated several micro-trends in how spyware is complimented by other forms of repression. In Egypt, Mozn Hassan and other NGO representatives were subjected to travel bans and asset freezes in addition to spyware. Targeted regime critics such as Khaled Dawoud and Shady al-Ghazaly Harb were accused of sponsoring terrorist groups, which allowed officials to keep them in pre-trial detention for up to two

---

<sup>390</sup> Brian Dooley, Interview by author.

<sup>391</sup> Brian Dooley.

years. State defense was unable to tell Dawoud and al-Ghazaly Harb with which terrorist groups they were supposedly aligned.

In Morocco, two of the cases involved sex: Fouad Abdelmoumni was secretly filmed having sex with his partner and the videos were distributed in an attempt to shame him into silence, while Omar Radi was sentenced for sexual assault and espionage. Human Rights Watch said that these charges are part of Morocco's playbook to crush dissent, a practice that authorities have used since the mid-2010s to accuse and prosecute high-profile journalists and activists of non-speech crimes, including crimes involving consensual sex. Political activist and university professor Maati Monjib, who was imprisoned for three months on money-laundering charges, explained why it is so effective:

The political trials of the past gave prestige to [Moroccan] dissidents, made them heroes, mobilized public opinion around them. Designating them as traitors, thieves, and rapists – that's a better way to silence them.<sup>392</sup>

Abdessadek el Bouchattaoui also noted that Moroccan surveillance is carried out in an open, brazen way, so that the person targeted feels pressure. This is the author's experience as well having been blatantly tailed when she visited Western Sahara, a territory administered by Morocco.

The Saudi government used Pegasus for the surveillance of all of the citizens and foreigners profiled in this research. Three of those targeted, Saad al-Jabri, Omar Abdulaziz, and Ghanem al-Masarir all live in exile and were informed by local law enforcement that there were credible threats against their lives; al-Masarir was also physically attacked on the streets of London. Both al-Jabri and Abdulaziz have had

---

<sup>392</sup> Human Rights Watch, “‘They’ll Get You No Matter What’: Morocco’s Playbook to Crush Dissent.”

friends and family members arbitrarily detained to compel their return to the kingdom, though they have resisted. They also have stories that sound eerily similar to Jamal Khashoggi's in approach and timing, though with different outcomes: a Saudi hit squad was sent to Canada for al-Jabri (it was stopped at the border), and Abdulaziz was invited to the Saudi Embassy to renew his passport (he declined), both within the period immediately before and after Khashoggi's murder. A U.S. government official speaking on background said that Khashoggi's killing was a "rookie mistake" by Crown Prince Mohamed bin Salman; they doubt the crown prince would repeat it now given the international blowback from revelations about the journalist's murder.<sup>393</sup>

Keeping targeted Emiratis in the UAE was a common theme for several of the individuals profiled. Princess Latifa was forcibly returned to the UAE twice, including once with the likely aid of Pegasus; Ahmed Mansour had his passport cancelled so that he was prevented from leaving; and Emirati officials lobbied Qatari leaders at least twice to hand Alaa al-Siddiq over to them. Mansour, al-Siddiq, Princess Latifa, and Ghada Oueiss (who was either targeted by Saudi Arabia or the UAE), were all also the subject of public smear campaigns intended to discredit them.

---

<sup>393</sup> U.S. government official, Interview by author, September 23, 2022.

## Chapter XIII.

### Conclusion

Spyware has contributed to the worsening of human rights in the MENA region since the Arab uprisings. In most cases, it was used concurrently with other forms of digital and physical repression to silence dissent and suppress civic movements online, making it difficult to isolate the precise impact of the technology. Experts spoke to the unique threat that spyware poses given the ease of use, depth of information it provides, lack of attribution, inability to stop it, and chilling effect on targeted individuals, though the use of repression to silence voices is not new. Each profiled government in the region uses spyware differently, and the overall level of digital repression varies regardless of whether the country using it has a more liberal system of governance or not.

The effects of spyware are not limited to the region, as some governments surveil targets living abroad. Profiled victims that fled their countries of origin to live in exile discovered that they could not escape their governments' grip, as transnational repression—both physical and digital—is hard to stop. This is evident with the targeting of Jamal Khashoggi, Ayman Nour, Saad al-Jabri, Omar Abdulaziz, and Alaa al-Siddiq. “They were burgled in their home country and find that the same actors still have the keys to their home when they move abroad. There is nowhere they can feel safe,” said Sarah Yager, the Washington, DC Director of Human Rights Watch.<sup>394</sup>

### Mitigating the risks of spyware

---

<sup>394</sup> Sarah Yager, Interview by author, January 11, 2021.

This research has mainly focused on governments' use of spyware on civilians. Governments also use spyware to spy on each other, with significant implications for national security. In addition, there is growing evidence that non-state actors may be using this technology.<sup>395</sup> With this information in mind, there are specific steps that governments, groups of like-minded countries, and individuals should take to mitigate the risks of spyware.

## Governments

As a first step, the U.S. and like-minded governments should deepen their understanding of the commercial surveillance industry. They should develop lists of companies engaging in problematic practices, such as those selling spyware and other surveillance products to countries with poor human rights records or with inadequate legal frameworks to protect human rights; companies selling to non-state actors; and companies selling products without auditing ability or a remote "kill switch" when potential product misuse is suspected. Similarly, like-minded governments should create lists of countries engaging in the abuse of spyware and other surveillance technology including by targeting political activists, human rights defenders, journalists, and other members of civil society.

Armed with these lists, governments should reduce incentives for countries and companies selling spyware and other surveillance products to countries with records of

---

<sup>395</sup> John Scott-Railton, "Written Testimony of John Scott-Railton, Senior Researcher, the Citizen Lab House Permanent Select Committee on Intelligence Hearing on "Combating the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware"" (Washington, D.C.: House Permanent Select Committee on Intelligence, July 27, 2022), <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-Scott-RailtonJ-20220727.pdf>.

human rights abuses and inadequate legal protections. This would have the effect of slowing the proliferation of spyware to buy more time to improve regulatory frameworks guiding their sale and use. Reducing incentives could be achieved by signaling to investors and other surveillance sector stakeholders that there will be repercussions such as financial loss for selling spyware to countries without adequate human rights protections. The United States took such a step when it added NSO Group and Candiru to the U.S. Department of Commerce's Entity List, though more work is needed on the U.S. side to get its house in order. Placing these companies on the entity list was a welcome step, but reports of the FBI's purchase of Pegasus and the CIA's purchase of the spyware for Djibouti undermine U.S. credibility when delivering foreign demarches to demand better practices by other governments.

Like-minded governments should carefully weigh human rights and national security implications when considering spyware as a diplomatic sweetener, as it should any foreign military sale. In gaining support for the Abraham Accords, the Trump administration supported the Netanyahu government's use of Pegasus as a bargaining chip to normalize relations between several MENA states and Israel. These are the same MENA states that are using the spyware in abusive ways. Where possible, governments should disincentivize countries with abusive records from purchasing spyware instead of incentivizing them.

Governments should mandate a cooling off period for former intelligence community members, as the U.S. Congress did when it passed legislation in 2022 in response to the Project Raven revelations. Section 308 of Division X of the 2022 Consolidated Appropriations Act prohibits former U.S. intelligence community members

from working for a foreign government or a private entity under the influence of a foreign government for a period of five years.<sup>396</sup> GAO, Congress’s intelligence committees, or another independent body should review whether the legislation has achieved the intended outcome of curbing the misuse of past intelligence experience in several years’ time.

Countries should develop comprehensive export controls and greater transparency for their own domestically developed spyware and surveillance assistance. In 2021, the Commerce Department tightened export controls on items used for cyber surveillance, noting that “these new rules will help ensure that U.S. companies are not fueling authoritarian practices.”<sup>397</sup> These new controls should assist the U.S. Department of State’s Directorate of Defense Trade Controls (DDTC) work to curb the proliferation of spyware tools globally. The DDTC was the entity that approved Maryland-based CyberPoint’s export license to assist the UAE with intelligence support over a decade earlier. Relevant oversight bodies should actively monitor this space to understand whether export controls are adequate and update them as technologies and external demands evolve.

Governments should also ensure that domestic legal protections are modernized to hold companies and countries to account for using spyware to transnationally repress citizens and residents in their territory. Some companies prohibit the use of their spyware to target certain country codes – notably NSO Group’s Pegasus spyware cannot target

---

<sup>396</sup> “Section 308’s Overbroad Restrictions on Post-Intelligence Community Jobs,” Lawfare, December 12, 2022, <https://www.lawfareblog.com/section-308s-overbroad-restrictions-post-intelligence-community-jobs>.

<sup>397</sup> “Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and Other Malicious Cyber Activities,” U.S. Department of Commerce, October 20, 2021, <https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private>.

U.S. numbers – but this offers insufficient protection by itself given that there are many companies operating in this space, victims are spread out globally, and there are enterprising actors working to circumvent such prohibitions.

#### Multilateral efforts

Like-minded countries should work together to establish a multilateral regulatory framework for the sale and use of commercial spyware and other surveillance products to mitigate their abuse. Should powerful countries align on such a framework, it would send a strong signal to sellers and buyers. At a minimum, this framework should require that spyware only be sold to governments that meet the obligations of international human rights law and that have democratic institutions that consult the public to correct mistakes. It should prevent the third-party sale of spyware to mitigate circumvention of the framework. The framework should also clearly articulate consequences for stakeholders that violate the agreement. Potential groupings of like-minded countries could include the Five Eyes intelligence alliance (Australia, Canada, New Zealand, the United Kingdom, and the United States) or the G-7 (Canada, France, Germany, Italy, Japan, the United Kingdom, the United States, and the European Union).

#### Individual risk mitigation

Spyware is insidious and hard if not impossible to prevent. However, there are some steps that individuals can take to lessen their risk, including basic smartphone hygiene, testing tools, and behavior changes. Individuals should:

- Avoid clicking on links unless completely certain that the sender and link is known. Some spyware uses malicious links and can only be downloaded if the link is clicked. This mitigation measure will not work for zero-click spyware.
- Keep the smartphone's operating system up to date by installing security patches as soon as they are available. These patches close vulnerabilities that spyware exploits.
- Not use free Wi-Fi or connect to unknown networks. More recent versions of Pegasus have used network injections to download the spyware onto smartphones. Although injection infections can be forced upon a person, avoiding networks that may be hacked reduces the overall risk.
- Avoid communicating sensitive topics over the phone, opting instead to convey these messages in person.
- Check Amnesty International's Mobile Verification Toolkit (<https://mvt.re>) if a spyware infection is suspected on an iOS and Android smartphone.

### Outstanding questions

This thesis examined the role that spyware played in worsening human rights for people in the MENA region and those targeted beyond its borders. It identified unique ways that MENA governments use spyware. Some authorities use the extracted information to arrest, detain, and prosecute individuals; others use it to facilitate a physical attack; and a third group uses it to harass and defame a target. Digital surveillance via spyware was often combined with traditional repression and coercion tactics. The limited literature on governments' use of digital and traditional repression

has focused on the impact to protest mobilization. Deeper analysis of how autocratic governments in the region use the various digital and traditional methods of repression would enable a more nuanced understanding of how rulers maintain power. A related topic could be how governments use the chilling effects of spyware and other digital repression tools to influence behavior toward more socially accepted norms; this could be coupled with China's social credit model to punish and reward individuals with the overall goal of shaping public behavior.

In focusing on spyware in my study, I excluded data-extraction technology and drew a line between targeted surveillance and mass surveillance; the former targets an individual at the personal device level while the latter targets a broader group at the network level. This distinction is likely arbitrary given that some of the emerging technologies exhibit some of the capabilities of spyware. NSO Group's former CEO made a similar observation when he stated that the Chinese government—which excels in producing passive surveillance, big data, and AI technologies—is giving capabilities similar to Pegasus in Africa.<sup>398</sup> Future studies may wish to compare all digital technologies that provide real-time data and content on a targeted individual to expand our understanding of the technology space.

In a similar vein, this body of research demonstrated that the current focus on the dangers of Pegasus has the potential to limit the public's understanding of the threat that digital surveillance poses to human rights. In many ways, the academic and journalistic reporting on Pegasus have facilitated beneficial government and civic discourse but have caused us to overlook similar products and technologies that pose risks as significant as

---

<sup>398</sup> Farrow, "How Democracies Spy on Their Citizens."

Pegasus. Future analyses should also help answer what more governments can do to protect their citizens and residents from the dangers these technologies pose when used in illegitimate ways.

## References

- Abir Ghattas. "For Arab Human Rights Defenders, Hacking Team Files Confirm Suspicions of State Surveillance." *Global Voices Advox* (blog), July 8, 2015. <https://advox.globalvoices.org/2015/07/08/for-arab-human-rights-defenders-hacking-team-files-confirm-suspicions-of-state-surveillance/>.
- "About the Citizen Lab." Citizen Lab, University of Toronto. Accessed January 21, 2023. <https://citizenlab.ca/about/>.
- "About The Pegasus Project | Forbidden Stories." Accessed January 21, 2023. <https://forbiddenstories.org/about-the-pegasus-project/>.
- "About Us | Nazra for Feminist Studies." Accessed December 27, 2022. <https://nazra.org/en/about-us>.
- Abouzzohour, Yasmina. "Heavy Lies the Crown: The Survival of Arab Monarchies, 10 Years after the Arab Spring." *Brookings* (blog), March 8, 2021. <https://www.brookings.edu/blog/order-from-chaos/2021/03/08/heavy-lies-the-crown-the-survival-of-arab-monarchies-10-years-after-the-arab-spring/>.
- Adams, Tim. "Khashoggi Confidant Omar Abdulaziz: 'I'm Worried about the Safety of the People of Saudi Arabia.'" *The Guardian*, February 20, 2021, sec. Film. <https://www.theguardian.com/film/2021/feb/20/me-jamal-khashoggi-mohammed-bin-salman-omar-abdulaziz-the-dissident-netflix>.
- "Administrative Judiciary Obliges Cairo University to Return Dr. Shadi Al-Ghazali Harb to His Work as an Assistant Professor of Medicine in Al-Qasr Al-Ainy." Egyptian Center for Economic & Social Rights, July 20, 2022. <https://ecesr.org/en/2022/07/20/administrative-judiciary-obliges-cairo-university-to-return-dr-shadi-al-ghazali-harb-to-his-work-as-an-assistant-professor-of-medicine-in-al-qasr-al-ainy/>.
- Adrian Shahbaz. "Freedom on the Net 2018, The Rise of Digital Authoritarianism." Freedom House, November 2018.
- Adrian Shahbaz and Allie Funk. "Freedom on the Net 2020, The Pandemic's Digital Shadow." Freedom House, November 2020. [https://freedomhouse.org/sites/default/files/2020-10/10122020\\_FOTN2020\\_Complete\\_Report\\_FINAL.pdf](https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf).
- . "Freedom on the Net 2021: The Global Drive to Control Big Tech." Freedom House, November 2021. <https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech>.
- Amnesty International. "Ahmed Mansoor Selected as the 2015 Laureate Martin Ennals Award for Human Rights Defenders," October 6, 2015. <https://www.amnesty.org/en/latest/press-release/2015/10/ahmed-mansoor-selected-as-the-2015-laureate-martin-ennals-award-for-human-rights-defenders/>.
- Al Jazeera. "Timeline: Egypt's Revolution." Al Jazeera, February 14, 2011. <https://www.aljazeera.com/news/2011/2/14/timeline-egypts-revolution>.
- Allie Funk. Interview by author, January 26, 2023.

- ROBERT F. KENNEDY HUMAN RIGHTS. "Aminatou Haidar | RFK Human Rights." Accessed January 12, 2023. <https://rfkhumanrights.org/aminatou-haidar>.
- Amitai Ziv. "Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed." *Haaretz*, September 7, 2020. <https://www.haaretz.com/israel-news/tech-news/2020-09-07/ty-article/.premium/mobile-spytech-millions-in-gulf-deals-top-secret-israeli-cyberattack-firm-reve/0000017f-e1eb-d568-ad7f-f3eb36390000>.
- Amnesty International. "Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools." Amnesty International, June 22, 2020. <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/>.
- . "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware." Amnesty International, October 10, 2019. <https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/>.
- . "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware." Amnesty International, October 10, 2019. <https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/>.
- Amnesty International. "Amnesty Tech." Accessed January 21, 2023. <https://www.amnesty.org/en/tech/>.
- Amos, Deborah. "In Morocco, The Arab Spring's Mixed Bounty." *NPR*, February 7, 2012, sec. Africa. <https://www.npr.org/2012/02/07/146526685/in-morocco-the-arab-springs-mixed-bounty>.
- Amr Magdi. "Al-Sisi Is Leaving the Sick to Suffer in Egypt's Prisons." *Human Rights Watch*, September 1, 2021. <https://www.hrw.org/news/2021/09/01/al-sisi-leaving-sick-suffer-egypts-prisons>.
- An Exclusive Interview with His Excellency the Deputy Prime Minister and Minister of Foreign Affairs - #Al-Haqiqa # 10/1/2018*. Al Haqiqa. Qatar Television, 2018. <https://www.youtube.com/watch?v=IP908poMGIE>.
- Washington Post. "Analysis | The Cybersecurity 202: Trump's ZTE Reversal Flouts Warnings from Top National Security Officials." Accessed October 29, 2022. <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/14/the-cybersecurity-202-trump-s-zte-reversal-flouts-warnings-from-top-national-security-officials/5af87ab030fb0425887994ca/>.
- Apple Newsroom. "Apple Sues NSO Group to Curb the Abuse of State-Sponsored Spyware." Accessed October 13, 2022. <https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/>.
- "As It Happens." *As It Happens*. CBC Radio, January 25, 2021. <https://www.cbc.ca/radio/asithappens/as-it-happens-monday-edition-1.5886768/january-25-2021-episode-transcript-1.5888366>.
- "Background on Case No. 173 - the 'Foreign Funding Case' | Egyptian Initiative for Personal Rights." Accessed December 27, 2022. <https://eipr.org/en/press/2016/03/background-case-no-173-%E2%80%9Cforeign-funding-case%E2%80%9D>.

- Amnesty International. "Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy," June 16, 2020.  
<https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/>.
- Benjamin Barthe. "Au Liban, les monarchies du Golfe surveillent autant leurs amis que leurs ennemis." *Le Monde.fr*, July 19, 2021. [https://www.lemonde.fr/projet-pegasus/article/2021/07/19/au-liban-les-monarchies-du-golfe-surveillent-autant-leurs-amis-que-leurs-ennemis\\_6088812\\_6088648.html](https://www.lemonde.fr/projet-pegasus/article/2021/07/19/au-liban-les-monarchies-du-golfe-surveillent-autant-leurs-amis-que-leurs-ennemis_6088812_6088648.html).
- Bergman, Ronen, and Mark Mazzetti. "Israeli Companies Aided Saudi Spying Despite Khashoggi Killing." *The New York Times*, July 17, 2021, sec. World.  
<https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html>.
- . "The Battle for the World's Most Powerful Cyberweapon." *The New York Times*, January 28, 2022, sec. Magazine.  
<https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>.
- Bergman, Ronen, and Declan Walsh. "Egypt Is Using Apps to Track and Target Its Citizens, Report Says." *The New York Times*, October 3, 2019, sec. World.  
<https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html>.
- Brewster, Thomas. "Meet Candiru — The Mysterious Mercenaries Hacking Apple And Microsoft PCs For Profit." *Forbes*, October 3, 2019.  
<https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/>.
- . "Two Spyware, One iPhone: A Khashoggi Murder Trial Witness Fears He Was Hacked By Rival Surveillance Tools." *Forbes*. Accessed December 23, 2022.  
<https://www.forbes.com/sites/thomasbrewster/2021/12/16/nso-and-cytrox-spyware-allegedly-hacks-iphone-of-egypt-opposition-politician-in-exile/>.
- Brian Dooley. Interview by author, January 16, 2023.
- Bruce Schneier. "The Quick vs the Strong: Commentary on Cory Doctorow's Walkaway." *Crooked Timber* (blog), April 26, 2017.  
<https://crookedtimber.org/2017/04/26/the-quick-vs-the-strong-commentary-on-cory-doctorows-walkaway/>.
- Bryant, Elizabeth. "The Iron Fist vs. the Microchip." *Journal of Strategic Security* 5, no. 2 (2012): 1–26. <https://doi.org/10.5038/1944-0472.5.2.1>.
- Bureau of Democracy, Human Rights, and Labor. "2021 Country Reports on Human Rights Practices: Egypt." U.S. Department of State, 2021.  
<https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/egypt/>.
- Çali, Başak, Nazila Ghanea, and Benjamin Jones. "Big Promises, Small Gains: Domestic Effects of Human Rights Treaty Ratification in the Member States of the Gulf Cooperation Council." *Human Rights Quarterly* 38, no. 1 (2016): 21–57.  
<https://doi.org/10.1353/hrq.2016.0017>.
- Cellebrite. "Cellebrite Provides Facts About Its Business and Solutions." Accessed January 28, 2023. <https://cellebrite.com/en/cellebrite-facts/>.

- Front Line Defenders. "Charges against Mozn Hassan Dropped and Case Closed," October 28, 2021. <https://www.frontlinedefenders.org/en/case/charges-against-mozn-hassan-dropped-and-case-closed>.
- Chin, Joe Parkinson, Nicholas Bariyo and Josh. "Huawei Technicians Helped African Governments Spy on Political Opponents." *Wall Street Journal*, August 15, 2019, sec. Tech. <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>.
- Christopher Bing and Joel Schectman. "Special Report: Inside the UAE's Secret Hacking Team of U.S. Mercenaries." *Reuters*, January 30, 2019, sec. Special Reports. <https://www.reuters.com/article/us-usa-spying-raven-specialreport-idUSKCN1PO19O>.
- Citizen Lab. "Communities @ Risk: Targeted Digital Threats Against Civil Society." University of Toronto, November 11, 2014. <https://targetedthreats.net/media/1-ExecutiveSummary.pdf>.
- Coker, Paul Sonne And Margaret. "Foreign Firms Helped Gadhafi Spy on Libyans." *The Wall Street Journal*, August 30, 2011, sec. World News. <http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html>.
- U.S. Department of Commerce. "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities." Accessed November 6, 2022. <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>.
- U.S. Department of Commerce. "Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and Other Malicious Cyber Activities," October 20, 2021. <https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private>.
- Cox, Joseph. "U.S. Company Sold Zero-Click Hacking Tool to UAE Spy Operation." *Vice* (blog), September 14, 2021. <https://www.vice.com/en/article/3aq9a5/us-company-sold-zero-click-exploit-project-raven-uae>.
- Craig Timberg, Michael Birnbaum, Drew Harwell, and Dan Sabbagh. "Heads of State Found on List of Numbers Examined by Pegasus Project - The Washington Post." *Washington Post*, July 20, 2021. <https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/>.
- NSO Group. "CYBER INTELLIGENCE SECTOR LEADER NSO GROUP UNVEILS THE INDUSTRY'S FIRST 'TRANSPARENCY AND RESPONSIBILITY REPORT.'" Accessed October 17, 2021. <https://www.nsogroup.com/News/cyber-intelligence-sector-leader-nso-group-unveils-the-industrys-first-transparency-and-responsibility-report/>.
- Dana Priest. "UAE Agency Put Pegasus Spyware on the Phone of Hanan Elatr, Jamal Khashoggi's Wife." *Washington Post*, December 21, 2021. <https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/>.
- Dannia Akkad and Umar Farooq. "US Judge Throws out Former Saudi Spy Chief's Case against Crown Prince." *Middle East Eye*, October 3, 2022.

- <http://www.middleeasteye.net/news/us-saudi-arabia-former-spy-chief-crown-prince-case-thrown>.
- “Dark Caracal: Cyber-Espionage at a Global Scale.” Lookout, Electronic Frontier Foundation, January 18, 2018. [https://info.lookout.com/rs/051-ESQ-475/images/Lookout\\_Dark-Caracal\\_srr\\_20180118\\_us\\_v.1.0.pdf](https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf).
- Deborah Brown. “NSO Fails to Explain Targeting of Human Rights Watch Employee.” *Human Rights Watch* (blog), July 15, 2022. <https://www.hrw.org/news/2022/07/15/nso-fails-explain-targeting-human-rights-watch-employee>.
- “Definition of SPYWARE.” Accessed January 22, 2023. <https://www.merriam-webster.com/dictionary/spyware>.
- Deibert, Ron. “UK Government Officials Infected with Pegasus.” Citizen Lab, University of Toronto, April 18, 2022. <https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/>.
- Deji Olukotun and Peter Micek. “Five Years Later: The Internet Shutdown That Rocked Egypt.” *Access Now* (blog), January 22, 2016. <https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/>.
- deMeritt, Jacqueline H. R. “The Strategic Use of State Repression and Political Violence.” *Oxford Research Encyclopedia of Politics*, October 26, 2016. <https://doi.org/10.1093/acrefore/9780190228637.013.32>.
- Diana Hodali. “Omar Abdulaziz: A Critic of Saudi Arabia Becomes a Target – DW – 06/24/2020.” *Dw.Com*, June 24, 2020. <https://www.dw.com/en/omar-abdulaziz-a-critic-of-saudi-arabia-becomes-a-target/a-53924977>.
- Middle East Eye. “Digital Nightmare: The Arab Dissidents Ruined by Phone Hacking.” Accessed September 26, 2022. <http://www.middleeasteye.net/big-story/digital-nightmare-arab-dissidents-lives-torn-apart-hacking>.
- Doherty, David, and Peter J. Schraeder. “Social Signals and Participation in the Tunisian Revolution.” *The Journal of Politics* 80, no. 2 (2018): 675–91. <https://doi.org/10.1086/696620>.
- Dr. Saad Al-Jabri v. Mohammed bin Salman bin Abdulaziz al Saud, No. Civil Action 20-2146 (TJK) (U.S. District Court for the District of Columbia September 30, 2022).
- Earp, Madeline. “Al-Jazeera’s Ghada Oueiss on Hacking, Harassment, and Jamal Khashoggi.” *Committee to Protect Journalists* (blog), February 11, 2021. <https://cpj.org/2021/02/ghada-oueiss-hacking-harassment-jamal-khashoggi/>.
- “EP Inquiry Committee for Pegasus and Other Spyware Launched | News | European Parliament,” April 19, 2022. <https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched>.
- Evans, Rob. “BAE ‘Secretly Sold Mass Surveillance Technology to Repressive Regimes.’” *The Guardian*, June 14, 2017, sec. Business. <https://www.theguardian.com/business/2017/jun/15/bae-mass-surveillance-technology-repressive-regimes>.
- Eytan Avriel. “Two UAE Princes Each Got Their Own Personal NSO Spyware.” *Haaretz*, November 17, 2021. <https://www.haaretz.com/israel-news/tech->

- news/2021-11-17/ty-article/.premium/two-uae-princes-each-got-their-own-personal-nso-spyware/0000017f-e395-d9aa-afff-fbdd23c30000.
- Fahad Desmukh. "Bahrain Government Hacked Lawyers and Activists with UK Spyware." *Bahrain Watch* (blog). Accessed August 15, 2014. <https://web.archive.org/web/20140815233325/https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/>.
- Farrow, Ronan. "How Democracies Spy on Their Citizens." *The New Yorker*, April 18, 2022. <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.
- Feldstein, Steven. *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. New York, NY: Oxford University Press, 2021.
- BBC News. "Five Jailed UAE Activists 'Receive Presidential Pardon,'" November 28, 2011, sec. Middle East. <https://www.bbc.com/news/world-middle-east-15922492>.
- Ford, Liz. "Egyptian Feminist Leader Mozn Hassan Resolute in Face of Official Investigation." *The Guardian*, March 31, 2016, sec. Global development. <https://www.theguardian.com/global-development/2016/mar/31/egyptian-feminist-leader-mozn-hassan-resolute-investigation>.
- "Former Saudi Official Calls Mohammed Bin Salman a 'Psychopath,' Says Saudi Crown Prince Fears What He Knows." News. CBS, July 10, 2022. <https://www.cbsnews.com/news/mohammed-bin-salman-alleged-plot-saad-aljabri-60-minutes-2021-10-24/>.
- Franceschi-Bicchierai, Lorenzo. "The Vigilante Who Hacked Hacking Team Explains How He Did It." *Vice* (blog), April 15, 2016. <https://www.vice.com/en/article/3dad3n/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it>.
- Freedom House. *Freedom in the World 2013: The Annual Survey of Political Rights and Civil Liberties*. Freedom in the World. Lanham, MD: Rowman & Littlefield Publishers, 2013.
- . "Freedom on the Net 2019: The Crisis of Social Media." Freedom House, 2019. <https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>.
- . "Freedom on the Net, A Global Assessment of Internet and Digital Media." Freedom House, April 1, 2009. [https://freedomhouse.org/sites/default/files/2020-02/FOTN\\_Freedom\\_OnThe%20Net\\_Full%20Report\\_2009.pdf](https://freedomhouse.org/sites/default/files/2020-02/FOTN_Freedom_OnThe%20Net_Full%20Report_2009.pdf).
- . "Morocco: Freedom in the World 2021 Country Report." Freedom House. Accessed August 7, 2021. <https://freedomhouse.org/country/morocco/freedom-world/2021>.
- . "Morocco: Freedom on the Net 2018 Country Report." Freedom on the Net. Freedom House, 2018. <https://freedomhouse.org/country/morocco/freedom-net/2018>.
- . "Saudi Arabia: Freedom on the Net 2016 Country Report." Freedom House, 2016. <https://freedomhouse.org/country/saudi-arabia/freedom-net/2016>.
- . "Saudi Arabia: Freedom on the Net 2018 Country Report." Freedom House, 2018. <https://freedomhouse.org/country/saudi-arabia/freedom-net/2018>.
- . "United Arab Emirates: Freedom on the Net 2016 Country Report." Freedom House, 2016. <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2016>.

- . “United Arab Emirates: Freedom on the Net 2017 Country Report.” Freedom House, 2017. <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2017>.
- . “United Arab Emirates: Freedom on the Net 2018 Country Report.” Freedom House, 2018. <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2018>.
- . “United Arab Emirates: Freedom on the Net 2022 Country Report.” Freedom House, 2022. <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2022>.
- “Freedom in the World 2010.” Freedom House, 2010. [https://freedomhouse.org/sites/default/files/2020-03/FIW\\_2010\\_Complete\\_Book\\_Scan.pdf](https://freedomhouse.org/sites/default/files/2020-03/FIW_2010_Complete_Book_Scan.pdf).
- Freedom House. “Freedom on the Net Research Methodology.” Accessed January 21, 2023. <https://freedomhouse.org/reports/freedom-net/freedom-net-research-methodology>.
- Gail Horak. Letter to Cole Stangler and Abdellatif El Hamamouchi. “Question about ‘Morocco’s Surveillance Machine,’” January 11, 2023.
- Gallagher, Ryan. “How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists.” *Slate*, August 20, 2012. <https://slate.com/technology/2012/08/moroccan-website-mamfakinch-targeted-by-government-grade-spyware-from-hacking-team.html>.
- George, Rachel A. “Dialogue as Progress?: Islam and UN Human Rights Treaty Ratification in the Gulf Cooperation Council States.” In *The Arab Gulf States and the West*, 1st ed., 289–307. Routledge, 2019. <https://doi.org/10.4324/9780429505300-15>.
- Amnesty International. “German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed,” September 25, 2020. <https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/>.
- Ghada Oueiss. “Opinion | I’m a Female Journalist in the Middle East. I Won’t Be Silenced by Online Attacks.” *Washington Post*, July 9, 2020. <https://www.washingtonpost.com/opinions/2020/07/08/im-female-journalist-middle-east-i-wont-be-silenced-by-online-attacks/>.
- “Ghada Oueiss: ‘Saudi Has Based Its Rule on the Suppression of Women’ – Middle East Monitor.” Accessed November 16, 2022. <https://www.middleeastmonitor.com/20210210-ghada-oueiss-saudi-has-based-its-rule-on-the-suppression-of-women/>.
- Ghanem al-Masarir. “Opinion | Saudi Arabia Has Had Complete Access to My Private Life. So Now I’m Suing.” *Washington Post*, January 26, 2020. [https://www.washingtonpost.com/opinions/saudi-arabia-has-been-spying-on-me-for-years-so-im-suing/2020/01/25/0fa55462-3f00-11ea-8872-5df698785a4e\\_story.html](https://www.washingtonpost.com/opinions/saudi-arabia-has-been-spying-on-me-for-years-so-im-suing/2020/01/25/0fa55462-3f00-11ea-8872-5df698785a4e_story.html).
- Ghanem Almasarir *Political Satirist Attacked in London for Mocking Saudi Royals*, 2018. <https://www.youtube.com/watch?v=vKyTBrvWdP4>.

- “Global Spyware Scandal: Exposing Pegasus.” *FRONTLINE*. PBS, January 3, 2023. <https://www.pbs.org/wgbh/frontline/documentary/global-spyware-scandal-exposing-pegasus/>.
- “Hacking Team Founder: ‘Hacking Team Is Dead.’” Accessed October 17, 2021. <https://www.vice.com/en/article/n7wbnd/hacking-team-is-dead>.
- Hamza Guessous. “Egyptian Authorities Arrest More than 1,000 Anti-Corruption Protesters.” *Morocco World News*. <https://www.moroccoworldnews.com/>, September 25, 2019. <https://www.moroccoworldnews.com/2019/09/283389/egyptian-authorities-anti-corruption-protesters>.
- Harwell, Drew. “Customs Officials Have Copied Americans’ Phone Data at Massive Scale.” *Washington Post*, September 19, 2022. <https://www.washingtonpost.com/technology/2022/09/15/government-surveillance-database-dhs/>.
- Herrera, Linda. “Citizenship under Surveillance: Dealing with the Digital Age.” *International Journal of Middle East Studies* 47, no. 2 (2015): 354–56. <https://doi.org/10.1017/S0020743815000100>.
- Hibrawi, Reema. “Egypt Leads the Pack in Internet Censorship across the Middle East.” *Atlantic Council* (blog), August 28, 2018. <https://www.atlanticcouncil.org/blogs/menasource/egypt-leads-the-pack-in-internet-censorship-across-the-middle-east/>.
- Hisham Almiraat. How a hacking campaign helped shut down an award-winning news site, December 9, 2016. <https://www.amnesty.org/en/latest/research/2016/12/how-a-hacking-campaign-helped-shut-down-an-award-winning-news-site/>.
- “How Dubai’s AI Cameras Helped Arrest 319 Suspects Last Year.” Accessed September 13, 2021. <https://gulfnews.com/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675>.
- “How Western Spyware Helps Dictators with Phillip Adams.” *ABC Radio National*. Australian Broadcasting Corporation, August 3, 2021. <https://www.abc.net.au/radionational/programs/latenightlive/pegasus-israeli-spyware-manal-alsharif/13482000>.
- Huang, Kalley, and Kate Conger. “Former Twitter Employee Convicted of Charges Related to Spying for Saudis.” *The New York Times*, August 9, 2022, sec. Technology. <https://www.nytimes.com/2022/08/09/technology/twitter-saudi-arabia-spying-ahmad-abouammo.html>.
- Hubbard, Ben. “I Was Hacked. The Spyware Used Against Me Makes Us All Vulnerable.” *The New York Times*, October 24, 2021, sec. Times Insider. <https://www.nytimes.com/2021/10/24/insider/hacking-nso-surveillance.html>.
- Human Rights Council Working Group on Arbitrary Detention. “Opinions Adopted by the Working Group on Arbitrary Detention at Its Ninety-Third Session, 30 March–8 April 2022.” United Nations Human Rights Council, May 12, 2022. <https://www.ohchr.org/sites/default/files/2022-06/A-HRC-WGAD-2022-29-ARE-SAU-AEV.pdf>.
- Human Rights Watch. “‘They’ll Get You No Matter What’: Morocco’s Playbook to Crush Dissent.” Human Rights Watch, July 28, 2022.

- <https://www.hrw.org/report/2022/07/28/theyll-get-you-no-matter-what/morocco-s-playbook-crush-dissent>.
- Right Livelihood. "In Welcome Development, Egypt Drops Charges against Mozn Hassan." Accessed December 26, 2022. <https://rightlivelihood.org/news/in-welcome-development-egypt-drops-charges-against-mozn-hassan/>.
- International Federation for Human Rights. Press release. "Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies Executives Indicted." Press release, June 22, 2021. <https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa>.
- International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database. "Mobile Cellular Subscriptions (per 100 People) - Middle East & North Africa | Data." Accessed March 19, 2022. <https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2020&locations=ZQ&start=1960&view=chart>.
- Interview by author with U.S. government official, December 1, 2022.
- Jamal Khashoggi. "Opinion | Read Jamal Khashoggi's Columns for The Washington Post." *Washington Post*. Accessed October 29, 2022. <https://www.washingtonpost.com/news/global-opinions/wp/2018/10/06/read-jamal-khashoggis-columns-for-the-washington-post/>.
- Jane McMullen. "Princess Latifa: The Dubai Ruler's Daughter Who Vanished." *BBC News*, February 16, 2021, sec. Middle East. <https://www.bbc.com/news/world-middle-east-56085369>.
- Jenna McLaughlin. "BAE Systems Sells Internet Surveillance Gear to United Arab Emirates." *The Intercept*, August 26, 2016. <https://theintercept.com/2016/08/26/bae-systems-sells-internet-surveillance-gear-to-united-arab-emirates/>.
- John Scott-Railton. "Written Testimony of John Scott-Railton, Senior Researcher, the Citizen Lab House Permanent Select Committee on Intelligence Hearing on "Combating the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware"." Washington, D.C.: House Permanent Select Committee on Intelligence, July 27, 2022. <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-Scott-RailtonJ-20220727.pdf>.
- Jones, Marc Owen. *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. New York, NY: Oxford University Press, 2022.
- Josh Wood. "Lebanon Cracks Down on Internet Freedom." *The New York Times*, November 3, 2010. <https://www.nytimes.com/2010/11/04/world/middleeast/04iht-m04m1leblog.html>.
- "Journalists under Surveillance | Forbidden Stories." Accessed January 21, 2023. <https://forbiddenstories.org/pegasus-journalists-under-surveillance/>.
- Khaled Dawoud. Journalism and Politics in Egypt. Interview by Jon Alterman, May 4, 2021. <https://www.csis.org/analysis/journalism-and-politics-egypt>.
- Kirchgaessner, Stephanie. "British Judge Rules Dissident Can Sue Saudi Arabia for Pegasus Hacking." *The Guardian*, August 19, 2022, sec. World news.

- <https://www.theguardian.com/world/2022/aug/19/british-judge-rules-dissident-ghanem-almasarir-can-sue-saudi-arabia-for-pegasus-hacking>.
- . “Jeff Bezos Hack: Amazon Boss’s Phone ‘Hacked by Saudi Crown Prince.’” *The Guardian*, January 22, 2020.  
<http://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince>.
- . “New Evidence Suggests Spyware Used to Surveil Emirati Activist Alaa Al-Siddiq.” *The Guardian*, September 24, 2021, sec. World news.  
<https://www.theguardian.com/world/2021/sep/24/new-evidence-suggests-spyware-used-to-surveil-emirati-activist-alaa-al-siddiq>.
- . “Saudis behind NSO Spyware Attack on Jamal Khashoggi’s Family, Leak Suggests.” *The Guardian*, July 18, 2021, sec. World news.  
<https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>.
- . “UN-Backed Investigator into Possible Yemen War Crimes Targeted by Spyware.” *The Guardian*, December 20, 2021, sec. World news.  
<https://www.theguardian.com/world/2021/dec/20/un-backed-investigator-into-possible-yemen-war-crimes-targeted-by-spyware>.
- Kirkpatrick, David D., and Azam Ahmed. “Hacking a Prince, an Emir and a Journalist to Impress a Client.” *The New York Times*, August 31, 2018, sec. World.  
<https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html>.
- Lama Fakih. Interview by author, January 18, 2023.
- . Interview: Phone of HRW Director Attacked Using Pegasus Spyware, January 26, 2022. <https://www.hrw.org/news/2022/01/26/interview-phone-hrw-director-attacked-using-pegasus-spyware>.
- Land, Molly K., and Jay D. Aronson. “Human Rights and Technology: New Challenges for Justice and Accountability.” *Annual Review of Law and Social Science* 16, no. 1 (2020): 223–40. <https://doi.org/10.1146/annurev-lawsocsci-060220-081955>.
- #FreeLatifa. “Learn More About Princess Latifa Of Dubai - Missing Since March 2018.” Accessed January 16, 2023. <https://freelatifa.com/about-latiifa/>.
- Freedom House. “Lebanon: Freedom on the Net 2019 Country Report.” Accessed January 11, 2023. <https://freedomhouse.org/country/lebanon/freedom-net/2019>.
- Freedom House. “Lebanon: Freedom on the Net 2021 Country Report.” Accessed January 10, 2023. <https://freedomhouse.org/country/lebanon/freedom-net/2021>.
- Freedom House. “Lebanon: Freedom on the Net 2022 Country Report.” Accessed January 10, 2023. <https://freedomhouse.org/country/lebanon/freedom-net/2022>.
- Lee Fang. “Why Did the Firm That Sold Spyware to the UAE Win a Special Export License From State Department?” *The Intercept*, July 7, 2015.  
<https://theintercept.com/2015/07/07/baltimore-firm-supplying-united-arab-emirates-surveillance-software-won-special-export-license-state-department/>.
- Levenson, Michael. “F.B.I. Secretly Bought Israeli Spyware and Explored Hacking U.S. Phones.” *The New York Times*, January 28, 2022, sec. World.  
<https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html>.

- Louis Charbonneau. "Morocco May Have Spied on Western Sahara Mission: UN." *Reuters*, April 12, 2012, sec. Emerging Markets. <https://www.reuters.com/article/us-sahara-un-idUSBRE83B0IL20120412>.
- Lynfield, Ben. "Israel's Rewarding Road to Normalization." *Foreign Policy*, January 31, 2021. <https://foreignpolicy.com/2022/01/31/israel-abraham-accords-normalization-middle-east/>.
- MacFarquhar, Neil. "In Saudi Arabia, Royal Funds Buy Peace for Now." *The New York Times*, June 9, 2011, sec. World. <https://www.nytimes.com/2011/06/09/world/middleeast/09saudi.html>.
- Magdi, Amr. "Sisi Is Leaving the Sick to Suffer in Egypt's Prisons." *Foreign Policy*, September 1, 2021. <https://foreignpolicy.com/2021/09/01/sisi-egypt-prisoners-health-human-rights-abu-al-fotouh/>.
- Malsin, Jared. "Throughout Middle East, the Web Is Being Walled Off." *WSJ*. Accessed January 8, 2023. <https://www.wsj.com/articles/throughout-middle-east-the-web-is-being-walled-off-1531915200>.
- Manal al-Sharif. Interview by author, January 19, 2023.
- Marc Owen Jones. "Israeli Spyware: What You Read Could Make You a Target." *Middle East Eye*, November 18, 2021. <http://www.middleeasteye.net/opinion/candiru-israel-spyware-surveillance-imperialism>.
- Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. "Mapping Hacking Team's 'Untraceable' Spyware." University of Toronto, February 17, 2014. <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>.
- Marczak, Bill, and John Scott-Railton. "Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents." University of Toronto, May 29, 2016. <https://citizenlab.ca/2016/05/stealth-falcon/>.
- . "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender." University of Toronto, August 24, 2016. <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>.
- Marczak, Bill, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert. "The Great IPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit." University of Toronto, December 20, 2020. <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/>.
- Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert. "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus." University of Toronto, July 15, 2021. <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>.
- Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." University of Toronto, September 18, 2018. <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
- Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert. "FORCEDENTRY: NSO Group iMessage

- Zero-Click Exploit Captured in the Wild.” University of Toronto, September 13, 2021. <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.
- . “Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytox Mercenary Spyware.” University of Toronto, December 16, 2021. <https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/>.
- Marczak, Bill, John Scott-Railton, Adam Senft, and Sarah McKune. “Pay No Attention to the Server Behind the Proxy.” Citizen Lab. University of Toronto, October 15, 2015. <https://tspace.library.utoronto.ca/bitstream/1807/97784/1/Report%2364--finfisher.pdf>.
- Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. “Mapping FinFisher’s Continuing Proliferation.” University of Toronto, October 15, 2015. <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/>.
- Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert. “The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil.” University of Toronto, October 1, 2018. <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>.
- Marquis-Boire, Morgan, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola. “Hacking Team’s Tradecraft and Android Implant.” University of Toronto, June 24, 2014. <https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/>.
- MEE staff. “Egypt Arrests Prominent Critics of Sisi with 1,400 Detained since Friday Protests.” Middle East Eye, September 25, 2019. <http://www.middleeasteye.net/news/egypt-arrests-prominent-political-scientists-critical-sisi>.
- Megiddo, Gur. “Secretive Israeli Cyber Firm Selling Spy-Tech to Saudi Arabia.” *Haaretz*. June 8, 2021. <https://www.proquest.com/docview/2538079950/citation/5128B78F82A54D99PQ/1>.
- Mike Dvilyanski, David Agranaovich, and Nathaniel Gleichder. “Threat Report on the Surveillance-for-Hire Industry.” Meta, December 16, 2021. <https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf>.
- Moeckli, Daniel, Helen Keller, and Corina Heri. *The Human Rights Covenants at 50: Their Past, Present, and Future*. First edition. Oxford: University Press, 2018.
- Human Rights Watch. “Morocco: Espionage Case Against Outspoken Journalist,” September 21, 2020. <https://www.hrw.org/news/2020/09/21/morocco-espionage-case-against-outspoken-journalist>.
- The Economist. “Morocco’s Regime Is Accused of Blackmailing Critics.” Accessed January 16, 2023. <https://www.economist.com/middle-east-and-africa/2021/01/28/moroccos-regime-is-accused-of-blackmailing-critics>.
- Mozn Hassan. Interview by author, December 8, 2022.

- “Mozn Hassan/ Nazra for Feminist Studies Biography.” The Right Livelihood Award. Accessed December 27, 2022.  
<https://rightlivelihood.org/app/uploads/2016/09/MoznHassanNazra.pdf>.
- Right Livelihood. “‘My Private Life Has Been Stolen’: Aminatou Haidar Reveals How Her Life Has Changed after Pegasus Hacking.” Accessed January 12, 2023.  
<https://rightlivelihood.org/advocacy-updates/my-private-life-has-been-stolen-aminatou-haidar/>.
- Nakashima, Ellen. “As Cyberwarfare Heats up, Allies Turn to U.S. Companies for Expertise.” *Washington Post*, November 22, 2012, sec. National Security.  
[https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c\\_story.html](https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c_story.html).
- NSO Group. “NSO Group Transparency and Responsibility Report.” Tel Aviv, Israel, June 30, 2021. <https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf>.
- NSO Group. “NSO GROUP - About Us.” Accessed April 18, 2022.  
<https://www.nsogroup.com/about-us/>.
- “NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware.” Accessed October 13, 2022. <https://news.bloomberglaw.com/privacy-and-data-security/nso-loses-latest-challenge-to-meta-lawsuit-over-whatsapp-spyware>.
- OHCHR. “OHCHR | A/HRC/51/47: Cooperation with the United Nations, Its Representatives and Mechanisms in the Field of Human Rights - Report of the Secretary-General.” Accessed October 13, 2022.  
<https://www.ohchr.org/en/documents/thematic-reports/ahrc5147-cooperation-united-nations-its-representatives-and-mechanisms>.
- OHCHR. “OHCHR | Inquiry into the Killing of Mr. Jamal Kashoggi.” Accessed January 21, 2023. <https://www.ohchr.org/en/special-procedures/sr-executions/inquiry-killing-mr-jamal-kashoggi>.
- OHCHR. “OHCHR | International Bill of Human Rights.” Accessed January 10, 2023.  
<https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights>.
- Olivier Tesquet. “Amesys: Egyptian trials and tribulations of a French digital arms dealer,” July 5, 2017. <https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php>.
- Omar Abdulaziz. “Opinion | Saudi Spies Hacked My Phone and Tried to Stop My Activism. I Won’t Stop Fighting.” *Washington Post*, November 15, 2019.  
<https://www.washingtonpost.com/opinions/2019/11/14/saudi-spies-hacked-my-phone-tried-stop-my-activism-i-wont-stop-fighting/>.
- Omer Benjakob. “The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware - Tech News - Haaretz.Com.” *Haaretz*, April 5, 2022.  
<https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000>.
- Middle East Eye. “Pegasus: Saudi Arabia ‘targeted Phone’ of UN Investigator into Yemen War Crimes,” December 20, 2021.  
<http://www.middleeasteye.net/news/pegasus-spyware-saudi-arabia-targeted-phone-un-investigator-yemen>.

- Pegg, David, Paul Lewis, Michael Safi, and Nina Lakhani. "FT Editor among 180 Journalists Identified by Clients of Spyware Firm." *The Guardian*, July 20, 2021, sec. World news. <https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware>.
- Penney, Jon. "Chilling Effects: Online Surveillance and Wikipedia Use." SSRN Scholarly Paper. Rochester, NY, 2016. <https://papers.ssrn.com/abstract=2769645>.
- Penney, Jonathon. "Understanding Chilling Effects." *SSRN Electronic Journal*, 2021. <https://doi.org/10.2139/ssrn.3855619>.
- Perlroth, Nicole. "Governments Turn to Commercial Spyware to Intimidate Dissidents." *The New York Times*, May 29, 2016, sec. Technology. <https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html>.
- . *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. New York: Bloomsbury Publishing, 2020.
- PRB. "In Arab Countries, Mobile Internet and Social Media Are Dominant, but Disparities in Access Remain." PRB. Accessed December 11, 2022. <https://www.prb.org/resources/in-arab-countries-mobile-internet-and-social-media-are-dominant-but-disparities-in-access-remain/>.
- Priest, Dana, Souad Mekhennet, and Arthur Bouvart. "Jamal Khashoggi's Wife Targeted with Spyware before His Death." *Washington Post*, July 18, 2021. <https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/>.
- BBC News. "Princess Haya: Dubai Ruler Had Ex-Wife's Phone Hacked - UK Court," October 6, 2021, sec. Middle East. <https://www.bbc.com/news/world-middle-east-58814978>.
- "Princess Latifa: 'Hostage' Ordeal of Dubai Ruler's Daughter Revealed." *Panorama*. BBC, February 16, 2021. <https://www.bbc.com/news/world-middle-east-56075528>.
- Privacy International. "State of Privacy Morocco." Privacy International, January 26, 2019. <http://privacyinternational.org/state-privacy/1007/state-privacy-morocco>.
- Aljazeera. "Prominent UAE Activist Alaa Al-Siddiq Dies in UK Car Crash," June 20, 2021. <https://www.aljazeera.com/news/2021/6/20/prominent-emirati-activist-dies-in-london-car-crash>.
- Ramy Raoof [@RamyRaoof]. "From the #HackingTeam Leaks: Invoice to #Egypt - 58,000 EURO - January 2012. Http://T.Co/PgSJOWUwQq." Tweet. *Twitter*, July 6, 2015. <https://twitter.com/RamyRaoof/status/618011320496050176>.
- The Guardian. "Response from NSO and Governments," July 20, 2021, sec. News. <https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments>.
- Reuters. "U.S. Court Tosses Saudi Suit against Former Top Saudi Intelligence Officer." *Reuters*, December 30, 2021, sec. United States. <https://www.reuters.com/world/us/us-court-tosses-saudi-suit-against-former-top-saudi-intelligence-officer-2021-12-30/>.
- Ronald Deibert. "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy." *Foreign Affairs*, December 12, 2022.

- <https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert>.
- Rori Donaghy. "Falcon Eye: The Israeli-Installed Mass Civil Surveillance System of Abu Dhabi." *Middle East Eye*, July 15, 2015.  
<http://www.middleeasteye.net/news/falcon-eye-israeli-installed-mass-civil-surveillance-system-abu-dhabi>.
- . "Post | Feed | LinkedIn." Social media. LinkedIn. Accessed January 16, 2023.  
<https://www.linkedin.com/feed/update/urn:li:activity:6843634248063164417/>.
- Sabbagh, Dan. "Data Leak Raises New Questions over Capture of Princess Latifa." *The Guardian*, July 21, 2021, sec. World news.  
<https://www.theguardian.com/world/2021/jul/21/data-leak-raises-new-questions-over-capture-of-princess-latifa>.
- Sabbagh, Dan, Dan Sabbagh Defence, and security editor. "'The Walls Are Closing in on Me': The Hacking of Princess Haya." *The Guardian*, October 6, 2021, sec. World news. <https://www.theguardian.com/world/2021/oct/06/walls-closing-in-story-behind-princess-haya-hacking-ordeal>.
- Samuel Osborne. "Princess Latifa: New Photo Emerges of Dubai Royal in Iceland as Campaign to Free Her Is Disbanded." *Sky News*, August 10, 2021.  
<https://news.sky.com/story/princess-latifa-new-photo-emerges-of-dubai-royal-in-iceland-as-campaign-to-free-her-is-disbanded-12377367>.
- Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong. "Freedom on the Net 2014, Tightening the Net: Governments Expand Online Controls." Freedom House, 2014.
- . "Freedom on the Net 2015, Privatizing Censorship, Eroding Privacy." Freedom House, October 2015.
- Sanja Kelly, Mai Truong, Adrian Shahbaz, and Madeline Earp. "Freedom on the Net 2016, Silencing the Messenger: Communication Apps under Pressure." Freedom House, November 2016.
- Sanja Kelly, Mai Truong, Adrian Shahbaz, Madeline Earp, and Jessica White. "Freedom on the Net 2017, Manipulating Social Media to Undermine Democracy." Freedom House, November 2017.
- Sanja Kelly, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, and Ashley Greco-Stoner. "Freedom on the Net 2013, A Global Assessment of Internet and Digital Media." Freedom House, October 3, 2013.
- Sanja Kelly and Sarah Cook. "Freedom on the Net 2011, A Global Assessment of Internet and Digital Media." Freedom House, April 18, 2011.  
[https://freedomhouse.org/sites/default/files/2020-02/FOTN\\_2011\\_Summary\\_Findings.pdf](https://freedomhouse.org/sites/default/files/2020-02/FOTN_2011_Summary_Findings.pdf).
- Sanja Kelly, Sarah Cook, and Mai Truong. "Freedom on the Net 2012, A Global Assessment of Internet and Digital Media." Freedom House, September 24, 2012.
- Santiago Gomez, Elvira, and Carmen Rodriguez Rodriguez. "Surveillance Technologies: A review of legitimate State violence in security and control contexts." *Encrucijadas (Salamanca, Spain)* 16 (2018).  
<http://gateway.webofknowledge.com/gateway/Gateway.cgi?GWVersion=2&SrcApp=Summon&SrcAuth=ProQuest&DestApp=WOS&DestLinkType=FullRecord&UT=000455807000011>.

- Sarah Yager. Interview by author, January 11, 2021.
- Freedom House. "Saudi Arabia Case Study | Understanding Transnational Repression." Accessed December 30, 2022. <https://freedomhouse.org/report/transnational-repression/saudi-arabia>.
- Deloitte Insights. "Saudi Arabia's Digital Government Stays Ahead of the Curve." Accessed January 24, 2023. <https://www2.deloitte.com/us/en/insights/focus/tech-trends/2023/saudi-arabia-government-digital-transformation-and-innovation.html>.
- Scott-Railton, John, Bill Marczak, Ramy Raoof, and Etienne Maynier. "Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society." University of Toronto, February 2, 2017. <https://citizenlab.ca/2017/02/nilephish-report/>.
- Lawfare. "Section 308's Overbroad Restrictions on Post-Intelligence Community Jobs," December 12, 2022. <https://www.lawfareblog.com/section-308s-overbroad-restrictions-post-intelligence-community-jobs>.
- Shah, Angela. "Why the Arab Spring Never Came to the UAE." *Time*, July 18, 2011. <https://content.time.com/time/world/article/0,8599,2083768,00.html>.
- Sharif, Manal. *Daring to Drive: A Saudi Woman's Awakening*. First Simon&Schuster hardcover edition. New York: Simon & Schuster, 2017.
- Stangler, Cole, and Abdellatif El Hamamouchi. "Morocco's Surveillance Machine: Morocco's Intelligence Apparatus Fuels a Crackdown on Dissent." *The Intercept* (blog), October 21, 2021. <https://theintercept.com/2021/10/21/morocco-pegasus-surveillance-journalists/>.
- Steven Feldstein. "The Global Expansion of AI Surveillance." *Carnegie Endowment for International Peace - Papers*. 2019. <https://search.proquest.com/docview/2299099093?pq-origsite=primo>.
- . "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, September 2019. [https://carnegieendowment.org/files/WP-Feldstein-AISurveillance\\_final1.pdf](https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf).
- Steven Feldstein and Brian Kot. "Democracy, Conflict, and Governance Program: Global Inventory of Commercial Spyware and Digital Forensics." Carnegie Endowment for International Peace. Accessed January 9, 2023. <https://carnegieendowment.org/programs/democracy/commercialspyware>.
- Suliman, Adela. "Dubai's Princess Latifa Tells U.N. She Is 'Well' during Meeting with Human Rights Chief in Europe." *Washington Post*, February 19, 2022. <https://www.washingtonpost.com/world/2022/02/19/princess-latifa-michelle-bachelet-human-rights-dubai/>.
- Szmolka, Inmaculada. *Political Change in the Middle East and North Africa: After the Arab Spring*. Edinburgh University Press, 2018.
- Taha Al-Esawi. "'Al-Sisi's Regime Is Weak and Will Not Stand up to the Accumulated Anger.'" *Middle East Monitor* (blog), July 12, 2018. <https://www.middleeastmonitor.com/20180712-al-sisis-regime-is-weak-and-will-not-stand-up-to-the-accumulated-anger/>.
- Tanis, Fatma. "Saudi Activist Who Led Campaign To Legalize Driving For Women Is Released From Jail." *NPR*, February 10, 2021, sec. Middle East. <https://www.npr.org/2021/02/10/966258281/loujain-al-hathloul-saudi-activist-jailed-for-driving-has-been-released>.

- The Citizen Lab. “BAD TRAFFIC: Sandvine’s PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?” The Citizen Lab, March 9, 2018. <https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/>.
- Engelsberg Ideas. “The Morality of Espionage,” February 9, 2021. <https://engelsbergideas.com/essays/the-morality-of-espionage/>.
- “Their Eyes on Me: Stories of Surveillance in Morocco.” Privacy International, 2014. [https://web.archive.org/web/20170417194607/https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English\\_0.pdf](https://web.archive.org/web/20170417194607/https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf).
- Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than \$1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government (U.S. Department of Justice September 14, 2021).
- Tim Adams. “Khashoggi Confidant Omar Abdulaziz: ‘I’m Worried about the Safety of the People of Saudi Arabia’ | Documentary Films | The Guardian.” *The Guardian*, February 20, 2021. <https://www.theguardian.com/film/2021/feb/20/me-jamal-khashoggi-mohammed-bin-salman-omar-abdulaziz-the-dissident-netflix>.
- Arabian Business. “UAE in Crackdown on Social Media Abuse - Arabian Business,” March 10, 2015. <https://www.arabianbusiness.com/industries/technology/uae-in-crackdown-on-social-media-abuse-585044>.
- United Nations Human Rights Treaty Bodies. “UN Treaty Body Database.” Accessed October 10, 2022. [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/treaty.aspx?treaty=cescr&lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/treaty.aspx?treaty=cescr&lang=en).
- Uniacke, Robert. “Authoritarianism in the Information Age: State Branding, Depoliticizing and ‘de-Civilizing’ of Online Civil Society in Saudi Arabia and the United Arab Emirates.” *British Journal of Middle Eastern Studies* ahead-of-print, no. ahead-of-print (n.d.): 1–21. <https://doi.org/10.1080/13530194.2020.1737916>.
- United Nations Human Rights Council. “Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi\*.” Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development, June 19, 2019. [https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session41/Documents/A\\_HRC\\_41\\_CRP.1.docx](https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_CRP.1.docx).
- United Nations Office of the High Commissioner for Human Rights. “OHCHR | A/HRC/51/47: Cooperation with the United Nations, Its Representatives and Mechanisms in the Field of Human Rights - Report of the Secretary-General.” OHCHR. Accessed December 23, 2022. <https://www.ohchr.org/en/documents/thematic-reports/ahrc5147-cooperation-united-nations-its-representatives-and-mechanisms>.
- Middle East Eye. “US Court Issues Summons for MBS and MBZ over Hacking of Al Jazeera Anchor.” Accessed November 16, 2022. <http://www.middleeasteye.net/news/us-court-issues-summons-mbs-and-mbz-over-hacking-al-jazeera-anchor>.

- U.S. Department of State. "Bureau of Near Eastern Affairs." United States Department of State. Accessed February 13, 2022. <https://www.state.gov/bureaus-offices/under-secretary-for-political-affairs/bureau-of-near-eastern-affairs/>.
- U.S. government official. Interview by author, September 23, 2022.
- . Interview by author, January 17, 2023.
- OHCHR. "Use of Spyware to Surveil Journalists and Human Rights Defenders, Statement by UN High Commissioner for Human Rights Michelle Bachelet," July 19, 2021. <https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner>.
- "Varieties of Autocratization – V-Dem." Accessed December 30, 2022. <https://v-dem.net/our-work/research-programs/varieties-of-autocratization/>.
- V-Dem Institute. "Autocratization Changing Nature?" Democracy Report 2022. V-Dem Institute, University of Gothenburg, March 2022. [https://v-dem.net/media/publications/dr\\_2022.pdf](https://v-dem.net/media/publications/dr_2022.pdf).
- Watch 60 Minutes: The Tool Meant to Hack Any Smartphone - Full Show on Paramount Plus*. Accessed October 17, 2021. [https://www.paramountplus.com/shows/60\\_minutes/video/PAw6rD\\_p57euS0hC9\\_6gtKM8AWYXMhCO/ceo-of-israeli-spyware-maker-nso-on-fighting-terror-khashoggi-murder-and-saudi-arabia/](https://www.paramountplus.com/shows/60_minutes/video/PAw6rD_p57euS0hC9_6gtKM8AWYXMhCO/ceo-of-israeli-spyware-maker-nso-on-fighting-terror-khashoggi-murder-and-saudi-arabia/).
- Weidmann. *The Internet and Political Protest in Autocracies*. Oxford University Press, 2019.
- Techopedia.com. "What Does Hack Mean in Security? - Definition from Techopedia." Accessed February 13, 2022. <http://www.techopedia.com/definition/3804/hack-security>.
- Techopedia.com. "What Is an Exploit in Computing? - Definition from Techopedia." Accessed February 13, 2022. <http://www.techopedia.com/definition/4275/exploit>.
- Cisco. "What Is Malware? - Definition and Examples." Accessed January 22, 2023. <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html>.
- "WikiLeaks - The Hackingteam Archives." Accessed October 21, 2022. <https://wikileaks.org/hackingteam/emails/emailid/5391>.
- Winnona Desombre, Lars Gjesvik, and Johann Ole Willers. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets." #ACCyber, November 2021. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/>.
- Zalfa Quino. "#HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices." *Global Voices Advox* (blog), July 28, 2015. <https://advox.globalvoices.org/2015/07/28/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/>.