AUSTRIA INSTITUT FÜR EUROPA- UND SICHERHEITSPOLITIK

AIES-STUDIES

Stefanie Felsberger

Colonial Cables – The Politics of Surveillance in the Middle East and North Africa

Nr. 10
February 2020
Vienna

Stefanie Felsberger is a PhD candidate at the Centre for Gender Studies at Cambridge University. Before she worked as Senior Researcher and Bartlett Fellow at the Access to Knowledge for Development Center (A2K4D) at the American University in Cairo. Her work focuses on questions of access and control of data, knowledge and technology, as well as the political economy of data, surveillance theory and the politics of gender; both globally and in the Middle East and North Africa. Felsberger previously worked as researcher at the AIES, where her research focused on the politics of democratization, EU policy in the Middle East, and discourses around political Islam. Felsberger studied Political Science and Arabic Studies at the University of Vienna.

AIES
Tivoligasse 73a
1120 Vienna
Austria
Tel: +43 1 3583080
office@aies.at
www.aies.at

Abbreviations

CIA	Central Intelligence Agency
EED	European Endowment for Democracy
ENP	European Neighbourhood Policy
EU	European Union
EUGS	European Global Strategy
GCC	Gulf Cooperation Council
ICT	Information, Communication, and Technology
IcSP	Instrument Contributing to Stability and Peace
ISP	Internet service provider
MENA	Middle East and North Africa
LRAD	Long Range Acoustic Device
NGO	Non-governmental organisation
PATN	Pegasus Anonymizing Transmission Network
PI	Privacy International
UAE	United Arab Emirates

Figures

Fig. 1 A Map of suspected *Pegasus* infections, ©Citizen Lab

Table of Contents

Abbreviations **1**

Figures **1**

Table of Contents **2**

1. Introduction ***3***

2. Colonial Cables: Tracing Technology and Surveillance in MENA ***4***

2.1.1. The Panopticon, a Colonial Invention 5

2.1.2. Colonial Legacies of Control 5

2.1.3. Surveillance Laboratories 6

3. The Sale of Surveillance Technology in MENA ***7***

3.1. European Companies: Hacking Team and Gamma Group **8**

3.1.1. Technological Capabilities: Products and Services 9

3.1.2. Use & Abuse 9

3.2. A Regional Company: the NSO Group **10**

3.2.1. Technological Capabilities: Products and Services 11

3.2.2. Use & Abuse 11

3.3. Insights **13**

4. Selling Surveillance: the EU's Principled Pragmatism ***15***

4.1. Principled Pragmatism vs. Democracy **15**

4.2. Spillover of Surveillance Technology **18**

5. Conclusions: Surveillance Spilling Over and Increased Authoritarianism ***19***

5.1. Recommendations **19**

6. Bibliography ***21***

1. Introduction

Neither security studies as a discipline, nor general analyses of geopolitics have placed great emphasis on questions of data, technology, or internet infrastructure. Focus has been put on studying arms development, energy dependency, access to natural resources or strategic geographic points, or infrastructure more broadly. The question of information, communication, and technology (ICT) has only recently come into clearer focus. Under the rubric cybersecurity, the question was debated how countries could protect their ICT infrastructure and other increasingly digitised infrastructure from malicious attacks by other states or non-state actors as war moved to the so-called 'cyberspace.' In line with a shift in critical security studies where the referent object of security studies are not states but individuals, the question of surveillance needs to be added to this agenda.

Surveillance as a threat for states but also people has been thrust on the public agenda by the whistle-blower Edward Snowden who worked as data analyst for a private company subcontracted by the United States Central Intelligence Agency (CIA). He revealed extensive, illegal mass surveillance programmes by the US government, and other states, to spy on people and state leaders all over the world.[1] The role of private companies was and is pivotal to his revelations: Snowden himself worked as data analyst for an external company and not within the CIA itself. Private companies also played a large role in the mass surveillance programmes he revealed.

Today, digital technologies play a role in almost every aspect of social, political, and economic life—albeit to different degrees in different places and income groups. Similar to private military contractors, core aspects of communications and intelligence infrastructure have been outsourced to or rely on technology companies. Thereby elements that used to be considered central to state sovereignty have become privatised. Just like the implementation of the Iraq War heavily relied on private military contractors, such as Blackwater, surveillance depends on private companies. This is true for mass as well as targeted surveillance. While we have some limited knowledge about mass surveillance, companies who sell surveillance technology operate in secrecy. We neither know much about their activities, nor how they tie in with geopolitical dynamics in the Middle East and North Africa (MENA). This is what I focus on in this study: the activities of the three best documented companies selling surveillance services in the context of the evolving geopolitics in the MENA region. What insights can be gained from studying the activities of companies that are crucial to surveillance operations in MENA? What do these companies mean for the different emancipatory uprisings in the region? What role does Europe play in this surveillance game? And what role does surveillance play in the

[1] Specifically, it was revealed that the NSA tracked the calls of 35 world leaders, including Germany (Ball 2013).

European Union's (EU) policies towards the MENA region? What lessons can the EU learn for their future policies towards surveillance technology?

In the first chapter, I present the framing of this study. I show that the existing colonial roots of global power imbalances have influenced current technology development, infrastructure, and surveillance practices. I argue that these colonial roots influence how technology and surveillance work, and how we think about both issues. This knowledge helps to better understand today's regional politics of surveillance (both in the MENA region but also in Europe). To trace these, the second chapter looks at the three big and well-known companies selling surveillance software to MENA countries: NSO, Gamma Group, and Hacking Team, two of which are European companies and one is Israeli. I illustrate what type of surveillance technology is sold, how it is used, and contextualise these insights. In the final chapter, I point to two consequences of the unbridled sale of surveillance software for the European Union and democracy at large. I address what this means for dealing with authoritarian governments in MENA and argue that the unchecked use of targeted surveillance software will eventually harm Europe. In my conclusion, I recommend steps for the future.

2. Colonial Cables: Tracing Technology and Surveillance in MENA

> The subsea cables girding South America are owned by corporations based in Madrid, even as countries there struggle to control their own oil profits. Fibre-optic connections funnel financial transactions by way of offshore territories quietly retained through periods of decolonisation. Empire has mostly rescinded territory, only to continue its operation at the level of infrastructure, maintaining its power in the form of the network. Data-driven regimes repeat the racist, sexist, and oppressive policies of their antecedents because these biases and attitudes have been encoded into them at the root.
> – James Bridle (2018)

In this section, I analyse the continued impact of coloniality in technology, tech infrastructure, and surveillance politics globally but specifically in the Middle East. Similar to how James Bridle demonstrates the continued influence of colonialism by tracing cables in the above quote, I trace the roots of colonialism in surveillance. Colonialism is not an event that ended with the so-called decolonisation process overseen by the United Nations, but is a 'structure' and process that is still ongoing (Kauanui 2016). In this section, I first demonstrate that the Panopticon, a concept which influenced the foundations of thinking about and the theory of surveillance, has roots in colonial practices of the 18th and 19th century and, in fact, needs to be considered in the context of continuing coloniality to understand surveillance as a practice. I, then, argue that surveillance as a practice in the Middle East and in Europe is connected to

its colonial history and post-colonial present. The erasure of these connections makes it more difficult to understand and to fight surveillance practices.

2.1.1. The Panopticon, a Colonial Invention

The Panopticon has been the most influential metaphor to theorize surveillance in surveillance studies. The Panopticon is a blueprint for a prison or school, asylum, hospital, or factory. The French theorist Michel Foucault utilised it in his book *Discipline and Punish* to develop his theory on power and control[2] and it, subsequently, became central for how power but also surveillance was theorised. The Panopticon was, how Timothy Mitchell calls it, "a colonial invention" (1988, 35). This crucial aspect is omitted in Foucault's theorisation of power and in many subsequent applications of the Panopticon in surveillance studies, but just like the actual blueprint of the Panopticon has a colonial context, so does surveillance as a practice.

The Panopticon's inventor, Jeremy Bentham, tested his panoptic ideas in factories run by his brother on former Ottoman land, colonized by Russia (see Mathew S. Anderson, 'Samuel Bentham in Russia', The American Slavic and East European Review 15 (1956): 157-72 cited in Mitchell 1988, 185). His ideas were more popular in colonial administrations than in Europe. Bentham even played a role as an advisor to the British government and their colonial policies in India (Zureik 2013). Bentham incidentally also served as advisor to Mohammad Ali, then ruler of Egypt (Mitchell 1988, 40). Many disciplinary institutions based on the idea of the Panopticon were established on colonial frontiers, such as in India, Russia, North and South America (Mitchell 1988; Kaplan 1995). The Panopticon, and the related imagined modes of power and surveillance can thus not fully be comprehended without also studying the colonial roots of the Panopticon.

2.1.2. Colonial Legacies of Control

Khalili and Schwedler (2010) demonstrate in their book *Policing and Prisons in the Middle East: Formations of Coercion* that colonial legacies were key in shaping current realities of policing, control, and surveillance in the Middle East. They demonstrate how the setup of the present Egyptian state's apparatus of policing, imprisonment, intelligence, and surveillance has been heavily influenced by the legacies of British occupation and the import of know-how from Europe (Khalili and Schwedler 2010). Both of those influences were detrimental to the collective and individual rights and freedoms of the Egyptian population. There is a long history

[2] The blueprint was developed by Jeremy Bentham who imagined the set-up of the architecture to inspire self-discipline and to induce self-monitored behaviour change in prison inmates through a feeling of constant surveillance from a central watchtower. For Foucault, this prison blueprint manifested a shift in how power in Europe moved from public punishments as dominant mode of exercising power to a more subtle and insidious exercise of power that influenced everyday acts and thereby sought to instil discipline and self-control at the individual level (Foucault 1977).

of European colonial influence on the policing methods and strategies in Egypt, but also, presently, many governments in the Middle East import policing know-how, techniques, equipment, and experts from Europe (or the United States). The same is true for surveillance technologies.

Khalili and Schwedler explain that centralized police forces did not exist in MENA. More commonly, these tasks were performed by the army, until the 19th century witnessed a transformation with the emergence of a modern police as a subsidiary to an interior ministry with both punitive and reformative functions and institutionally separate from the military (Khalili and Schwedler 2010, 6-7). In Egypt, for example, this process took a very different shape, because in the early 19th century, Muhammad Ali had already established a highly centralised and structured police force. Once the British took control of Egypt, they heavily shaped and influenced the character of the Egyptian police and security forces according to their own needs and interests. Similar to the rest of the British Empire, this model of colonial policing led to a more militarised police force—as opposed to locally controlled and civilianized—and primarily saw its function as an instrument of control of dissent than a tool to fight crime (Khalili and Schwedler 2010, 8-9). Thus, Khalili and Schwedler make clear that practices of control and surveillance in Europe and the Middle East influence each other.

2.1.3. Surveillance Laboratories

Paul Rabinow, Simone Browne, and Elia Zureik outline further connections between technologies of control and surveillance in the context of colonialism. Elia Zureik (2013) argues that colonialism and imperialism motivated the development of modern surveillance technologies, as it became a central tool to manage and control both territory and population. Surveillance, Zureik writes, was “a formal aspect of colonial policies whereby surveillance was embodied in bureaucratic, enumerative and legal measures that aimed to control the territory and classify the population” (2013). Surveillance was also an intrinsic part of the implementation of the slave trade and slavery in the United States. Simone Browne’s book *Dark Matter: On the Surveillance of Blackness* (2015) reads current surveillance theory against the archive of slavery to show how many existing theories around surveillance are blind to questions of race. To rectify this, her book demonstrates how today’s surveillance practices in the US can be traced back to strategies of controlling people of colour during slavery. A similar continuation was also described by Paul Rabinow (1989), who called the colonial world the “laboratory of modernity” to stress how many technologies and techniques of power and control were tested in the colonies only to be implemented in the home countries. This dynamic also becomes evident in Zureik’s work. He demonstrates an “eventual spillover” of surveillance practices to the home countries. Along with Rabinow, Zureik describes colonies

as “a laboratory for developing and testing surveillance technologies for home use and marketing purposes” (2013). Many fundamental tools for surveillance such as census taking, map-making, fingerprinting, and profiling were developed and refined during the 18th and 19th century in colonial settings by the French in Africa, the British in North Africa and India, as well as by the Dutch in Southeast Asia (Zureik 2013). Thus, colonialism as a structure and surveillance go hand in hand.

Therefore, it is crucial to consider the following factors: first, surveillance technologies cannot be fully understood without their origins as practices of control in colonial settings; and, second, these historic roots continue to shape today’s practices and spillovers of surveillance and practices of control.

3. The Sale of Surveillance Technology in MENA

Today, there are two modes of surveillance: mass and targeted surveillance. The so-called data revolution has changed the previous logic of surveillance and shifted it from targeted searching for information about something specific to gathering as much information and data as possible in order to gain unprecedented insights through computational methods (Andrejevic and Gates 2014). However, this does not mean that targeted surveillance has become a thing of the past. On the contrary, governments today employ both tactics with varying degree and sophistication.

In general, the role of private companies in preventing or aiding surveillance has increased in the digital age, since most communication today is mediated by at least one or two companies (for example, the Internet service provider (ISP) and the platform hosting the messaging service). This is true for targeted surveillance and mass surveillance. An example of mass surveillance is how the NSA gathered data stored by big tech companies by forcing the companies to provide them with access (Angwin et al. 2015). Private companies also develop very sophisticated tools for targeted surveillance and then sell them to governments. More often than not, governments who seek such surveillance tools do not follow the rule of law, are engaged in violent conflicts, or oppress citizens, members of civil society, academics, NGOs, social movements, journalists, and activists (McKune and Deibert 2017). Despite the fact that these companies claim that their technology is only used to target terrorists, paedophiles, and crime syndicates, it is used to bolster authoritarian regimes and undermine democracy, human rights, and social justice worldwide.[3]

[3] There are even cases of surveillance technology being used to intimidate and spy on health advocates in support of a soda tax in Mexico (McKune and Deibert 2017).

Yet, not much is known about the specifics of how these companies and governments interact and act. The information that is available is known because of research conducted by academics and different NGOs,[4] in cooperation with activists or journalists who were targeted through these tools. Ahmed Mansoor is one of the activists through whom much has been revealed about surveillance companies. The activist from the United Arab Emirates (UAE) was excessively targeted with different tools from the NSO Group, Gamma Group, and Hacking Team. He consulted with the *Citizen Lab*, a research centre in Canada with experts specialized in analysing targeted surveillance software. Mansoor was even the target of three separate zero-day exploits which reportedly sell for around one million dollars (McKune and Deibert 2017).

Zero-day exploits are gaps in the security of a software of which a company is unaware; this means the vulnerability can be used and exploited to whatever end until the company becomes aware of it. In the past, it was common for hackers to sell information about such loopholes to companies or governments to assist in tightening their security, but now they have become a valuable object traded between surveillance companies (Privacy International 2018a). Private surveillance companies purchase these exploits and sell them together with their own software to customers providing unparalleled access to the computer or phone of a target (Privacy International 2018a). This illustrates the urgent need to consider the activities of both governments and private companies in order to fully understand surveillance politics.

Therefore, this section highlights the activities of three different companies selling surveillance technologies to different governments in the Middle East and North Africa. Two of these companies—Gamma Group and Hacking Team—are European companies, while the third—NSO Group—is an Israeli company. In the following sections, I outline what information is known about these companies and what their activities reveal about different relationships in the MENA region.

3.1. European Companies: Hacking Team and Gamma Group

Gamma Group, a company based in the UK and Germany, sells its spyware *FinFisher* exclusively to governments 'for law enforcement and intelligence' (McKune and Deibert 2017). Their software has repeatedly been used by authoritarian governments to suppress civil society (Marczak et al. 2015). Hacking Team is an Italian company selling an intrusive spyware called *Remote Control System* (Marczak and Scott-Railton 2016). Their activities have also been linked to the suppression of civil society. Ironically, Hacking Team was hacked in 2015 and company emails, internal files and source code were shared on Twitter for anyone to

[4] For example, Amnesty International (2018), Access Now (2008), and Privacy International (2018a, b).

download (Franceschi-Bicchierai 2015). This put the company in serious financial trouble until investors from Saudi Arabia saved Hacking Team from financial ruin (Franceschi-Bicchierai 2018).

3.1.1. Technological Capabilities: Products and Services

FinFisher, a product by Gamma Group, is a combination of different spyware tools. Governments receive *FinSpy Master*, "a C&C server that is installed on the entity's premises" (Marczak et al. 2015). This tool is used to set up proxies (also called *FinSpy Relays*) which hide the location of the institution using the spyware. Infected targeted computers only communicate with the proxies, set up on a VPN (Virtual Private Server) in a third country. This way, governments using *FinFisher* usually can do so secretly. According to Privacy International (2018a), Gamma Group developed fake updates for widely used programmes to deliver *FinSpy* onto a target's computer. Recently, Gamma Group has also offered a so-called *FinFly Exploit Portal*, which provides access to zero-day and one-day[5] exploits for extremely widely used software, such as Adobe Acrobat Reader and Microsoft Office. By using the portal, governments can more easily target anyone with *FinSpy*. The software developed by Hacking Team, the so-called *Remote Control System*, is very similar to *FinFisher*. Both allow an entity to break into a device and harvest information available on the device. Hacking Team also offers a zero-day exploit library to customers, which helps them to deliver the software onto different devices (Privacy International 2018a).

3.1.2. Use & Abuse

Research conducted by Marczak et al. at Citizen Lab (2015) finds "32 countries where at least one government entity is likely using the spyware suite" by Gamma Group.[6] According to them, Ethiopian activists have been targeted with *FinFisher* by the Ethiopian government while in exile in the UK and the US. The Bahraini government used *FinFisher* technology to monitor lawyers, activists, leaders of the opposition, and journalists (Marczak et al. 2015). It was also used to attack a group of citizen journalists in Morocco. Research by Access Now (2018) revealed that *FinSpy* was also used to target civil society in Turkey, Indonesia, Ukraine, and Venezuela. Hacking Team's software has been used in Azerbaijan, Egypt, Ethiopia, Kazakhstan, Malaysia, Nigeria, Oman, Saudi Arabia, Sudan, Turkey and Uzbekistan. In

[5] A one-day exploit works like a zero-day exploit, meaning it refers to a loophole in software. While a zero-day exploit is a vulnerability the target is unaware of, a one-day exploit refers to a loophole the company has been made aware of but has not patched up yet.

[6] Angola, Bangladesh, Belgium, Bosnia and Herzegovina, Czech Republic, Egypt, Ethiopia, Gabon, Indonesia, Italy, Jordan, Kazakhstan, Kenya, Lebanon, Macedonia, Malaysia, Mexico, Mongolia, Morocco, Nigeria, Oman, Paraguay, Romania, Saudi Arabia, Serbia, Slovenia, South Africa, Spain, Taiwan, Turkey, Turkmenistan, and Venezuela (Marczak et al. 2015).

addition, it was used to target activists in Morocco and journalists in Ethiopia (Privacy International 2018a).

Products by both Hacking Team and Gamma Group were used to attack Ahmed Mansoor, an award-winning human rights activist from the UAE. What happened to Mansoor is a remarkable and terrifying case: he was targeted by tools from three separate companies and at least one million dollars were spent targeting him. In March 2011, *FinFisher* spyware was sent to Mansoor's phone disguised as a PDF file attached to an email. The PDF appeared to be a petition supporting democracy, which Mansoor had already signed. Noticing the file was an EXE file and not a PDF, he did not open it but instead sent it to Citizen Lab (Marczak and Scott-Railton 2016). In July 2012, he was targeted again, but this time with spyware by Hacking Team. Their spyware infected his laptop through a Microsoft Word document by exploiting an old vulnerability and information was sent to an intelligence agency based in the UAE (Marczak and Scott-Railton 2016).

3.2. A Regional Company: the NSO Group

The NSO Group is a company based in Herzelia, Israel, selling spyware for mobile phones to governments. It is majority-owned by Novalpina Capital, a private equity company based in Europe (Anstis 2018). According to Marczak and Scott-Railton (2016) from Citizen Lab, the company appeared to be owned by Francisco Partners Management LLC which had previously invested in Blue Coat. Blue Coat is a company specialised on network monitoring and filtering whose services have been used by authoritarian regimes, such as Egypt (Ahram Online 2014).

I chose to include it in my analysis because it has been used on targets in Europe and because it has been involved in many high-profile cases, such as the murder of the Saudi journalist Jamal Khashoggi in the Saudi Arabian embassy in Turkey (Kenyon 2019) and the attack on Amnesty International staff (Amnesty International 2018), as well as Facebook suing the company (Wolff 2019). Moreover, in January 2020, Jeff Bezos, the CEO of Amazon, made allegations that the Saudi government hacked his phone. The allegations were serious enough for Agnes Callamard, UN Special Rapporteur on extrajudicial, summary or arbitrary executions, to call for an investigation by law enforcement agencies. Callamard stated that both Hacking Team and the NSO Group were "potential sources" of the software used to hack Bezos (Hern 2020). The Israeli company counts Saudi Arabia and the UAE among its clients; a fact that indicates an ever-closer relationship between these Gulf countries and Israel.

3.2.1. Technological Capabilities: Products and Services

What is known about NSO's product *Pegasus* has been revealed by research from Citizen Lab, Amnesty International, and several journalists. When Ahmed Mansoor was targeted with NSO spyware in 2018, he received a suspicious text on his phone, which he forwarded to Bill Marczak at Citizen Lab (Marczak and Scott-Railton 2016). Researchers at Citizen Lab were then able to identify *Pegasus*, a remote monitoring tool developed by NSO Group. *Pegasus* allows the operator (the one using the spyware) to access a phone's camera, microphone, files, and messages from all messaging apps (Marczak and Scott-Railton 2016), as well as passwords, contacts, events in the calendar, and live voice calls (Marczak et al. 2018). This spyware turns the phone into an active and passive surveillance device. Similar to the products sold by Hacking Team and Gamma Group, the collected information is transmitted to a *Pegasus Data Server* via PATN (Pegasus Anonymizing Transmission Network). PATN is a system which serves to obscure the identity and location of the operator (Marczak and Scott-Railton 2016).

Pegasus is usually delivered onto a target's device by sending an exploit link which the target has to click on. After the click, *Pegasus* is then secretly installed on the target's phone (Marczak et al. 2018). Mansoor's iPhone was targeted with a zero-day exploit, but there are reports that NSO Group is able to hack into iPhones without any action required by the target. According to Lorenzo Franceschi-Bicchierai and Joseph Cox (2018), a source close to NSO Group witnessed the company accessing his iPhone with *Pegasus* after just seven minutes. Apple released a security update to the operating system of the iPhone which was supposed to patch up the loopholes being exploited by *Pegasus*, but "[w]ithin days […] NSO was already bragging that it had thwarted those defences too" (Wilson and Srivastava 2019).

3.2.2. Use & Abuse

Evidence brought to light by Citizen Lab shows that members of civil society from 45 countries have been targeted with *Pegasus* software from 36 different operators (Marczak et al. 2018).[7] Among these operators are countries with extremely worrying human rights records, such as Bahrain, the United Arab Emirates, and Saudi Arabia.

[7] The countries identified were "Algeria, Bahrain, Bangladesh, Brazil, Canada, Cote d'Ivoire, Egypt, France, Greece, India, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Mexico, Morocco, the Netherlands, Oman, Pakistan, Palestine, Poland, Qatar, Rwanda, Saudi Arabia, Singapore, South Africa, Switzerland, Tajikistan, Thailand, Togo, Tunisia, Turkey, the UAE, Uganda, the United Kingdom, the United States, Uzbekistan, Yemen, and Zambia." (Marczak et al. 2018).

Members of the Gulf Cooperation Council (GCC) use *Pegasus* software extremely frequently: Citizen Lab found operators focused on the UAE, Bahrain, and Saudi Arabia.[8] Two of the operators, they suggest, may also be involved in spying activities in Europe (France, Greece, and the United Kingdom) and North America (Marczak et al. 2018). Especially the UAE is an avid user of surveillance spyware. In the past, regional tension escalated surveillance attempts between the UAE and Qatar. In 2017, when the UAE and Saudi Arabia started a blockade of Qatar, officials from the Emirates targeted "159 members of the Qatari royal family, officials and others" with NSO software (Kirkpatrick and Ahmed 2018).[9] Interestingly, the UAE has also asked NSO to target the Saudi prince Mutaib bin Abdullah, who was then still a contender for the throne and a rival of the Emirati supported Crown Prince Mohammad bin Salman.

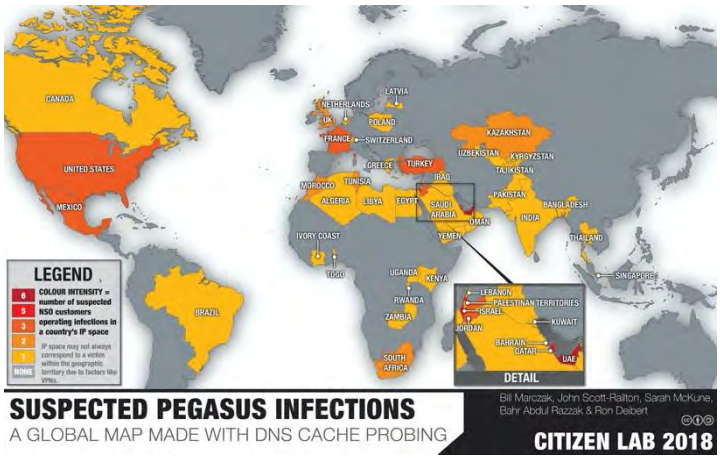

Fig.1: A Map of suspected Pegasus infections, © Citizen Lab

The Kingdom of Saudi Arabia is itself a prominent client of the NSO Group. Operators in Saudi Arabia targeted countries in the region and also individuals living in the United Kingdom, as well as a citizen from the US and Canada. Among these individuals are, first, the Saudi activist Yahya Assiri; second, an employee at Amnesty International working on matters related to Saudi Arabia; third, the Canadian activist Omar Abdulaziz; and, finally, Ghanem Almasarir, a Saudi activist (Brewster 2018). In January 2020, Citizen Lab stated that in June 2018, NSO software was used to target Ben Hubbard, who is a US citizen working for the New York Times as bureau chief in Lebanon. Hubbard was likely targeted for his reporting on Saudi Arabia (Marczak et al. 2020). Both Assiri and Abdulaziz were in close contact with Jamal Khashoggi, the Saudi journalist who was murdered in the Saudi embassy in Turkey by the Saudi state in October 2018. Omar Abdulaziz' phone was targeted with *Pegasus* and all his conversations with Jamal Khashoggi were recorded by operators based in Saudi Arabia (Liebermann 2019).

[8] I want to highlight that I intentionally refer to the GCC and not the Gulf region as a whole. There has been a split between mainly Qatar and the other GCC member states since 2013 when Saudi Arabia and the UAE (including the GGC) and Qatar were on opposing sides of the power struggle in Egypt. In 2013 the Egyptian military under now-President El-Sisi removed the elected President Morsi, a member of the Muslim Brotherhood, from power and then violently dispersed the sit-in of his supporters while killing more than 9000 civilians in a matter of days (HRW 2013). Qatar backed the Muslim Brotherhood, and the UAE as well as Saudi Arabia supported the new President El-Sisi.

[9] According to reporting by the New York Times, UAE officials requested NSO to demonstrate the effectiveness of their spyware and suggested NSO record the phone of the Qatari emir or the editor of an Arab newspaper based in London. NSO obliged and sent recordings four days later (Kirkpatrick and Ahmed 2018). These activities are now subject of a lawsuit filed against the NSO Group in Israel.

NSO Group does "not explicitly deny that Jamal Khashoggi's confidants were targeted with Pegasus" but continues to deny that its technology is used for anything other than to fight terrorism (Kenyon 2019). While NSO officially states that it applies ethical standards, the company "misdirect[s] questions about abuses, particularly concerning the critical issue of allowing clients to define what constitutes "terrorism" and "crime"" (Kenyon 2019). The widespread use of NSO's spyware to surveil members of civil society, journalists, activists, and human rights defenders, religious figures, lawyers, and officials shows the extent of the abuse of *Pegasus*. After being thrown into the spotlight by investigations by Citizen Lab, the NSO Group claims to have only found a 'handful' of cases of abuse (Wilson and Srivastava 2019).

3.3. Insights

In general, the use of spyware and surveillance technology are clearly more widespread in the region than ever. The Arab Uprisings, which started in 2010, seem to have stoked the fears of authoritarian governments in the region that they might be next. This idea was also voiced by Jerry Lucas, the President of *TeleStrategies*, the company which organises the world's biggest conferences where private surveillance companies and government officials meet (Arnold 2013). He confirmed that the surveillance business exploded after the uprisings, and that many vendors outside Europe started to emerge. The conferences Lucas organises are called ISS World and their growth is another indication of the increased business with surveillance. ISS World conferences take place annually in Dubai, the Czech Republic, the United States, Malaysia, and Panama. While ISS debuted in 2002 with only about 50 attendees, today, thousands of participants visit the conferences where millions of dollars change owners (Howell O'Neill 2017). Since 2009, the UAE has hosted the Middle East iteration of the conference, which is supposed to be the most "interesting," because "companies and governments are more aggressive in sales and purchases, the rule of law bends further than other areas of the world, and the potential for vast misuse of the products sold is closer to a guarantee than a hypothetical scenario" (Howell O'Neill 2017). Coincidentally, the European ISS has been sponsored by NSO Group in 2016 (Howell O'Neill 2017).

As Mansoor's case clearly highlights, even after years of cases revealing misuse of such intrusive software and increased public pressure, governments can and will use it to suppress civil society. While advertised as tools to combat terrorism, organized crime or other actors who are 'commonly accepted' as nefarious, these products are widely used against civil society: opposition politicians, journalists, lawyers, academics, researchers, and activists.

It is impossible for the companies selling this software to governments such as Bahrain, Ethiopia, Egypt, or Turkey to be unaware of the large potential for 'misuse' of their products. This point was stressed in a report by David Kaye, the *UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* to the United Nations Human Rights Council. Kaye stressed that "given the broad public knowledge of the repression practised by many of their clients, the companies cannot seriously claim to lack insight into the repressive uses of their tools."[10] The report went so far as to call for the immediate stop of sales of any dual-use surveillance technology.

The NSO Group's products continue to rise in popularity, which means that more governments will seek to become their clients. The list of NSO clients confirms interesting aspects of regional dynamics. This is because the NSO Group has to acquire an export license from the Israeli Ministry of Defense every time they want to sell their technology. An export license can be understood as permission slip by the Israeli government to sell surveillance technology to a foreign government (Franceschi-Bicchierai and Cox 2018). It is fair to assume that the Israeli government would not allow this technology in the hands of a country it understands to be an enemy. The fact that these GCC countries have been consistent customers of the Israeli company further confirms the close working relationship between the countries. Several Gulf countries have quietly improved relationships with Israel over the last years, in order to avoid public scrutiny. Israel is set to participate in Expo 2020, a present-day iteration of the 19th century world exhibitions taking place in the United Arab Emirates, despite the fact that the two countries have no formal relations (Nassar 2019). According to an Emirati official quoted in the *Times of Israel*, this does not signify "a change in relations between the UAE and Israel" (Times of Israel 2019). Bahrain is also reported to have welcomed a delegation of 30 people and Israel's economic minister for a business conference (TOI Staff 2019). The increased cooperation and relations between the GCC and Israel do not represent a new insight, but the fact that Israeli surveillance software is used by GCC countries with the explicit permission of the Israeli ministry of defence shows a surprising willingness of collaboration. Another interpretation might suggest that both Israel and the GCC countries prioritise containing Iran over each other. In the next section, I analzye the European policy towards the Mediterranean and situate the above described increased sale of surveillance technology in this context.

[10] UN General Assembly, Human Rights Council, Surveillance and Human Rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, ¶ 29 (May 28, 2019), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf.

4. Selling Surveillance: the EU's Principled Pragmatism

The policy of the European Union vis-à-vis the MENA region underwent many changes in the last decade; influencing factors were the Arab Uprisings, the increased numbers of refugees seeking asylum in European countries, and the changed US policies towards MENA after the election of Donald Trump (and proxy wars unfolding in Syria, Yemen, and Libya). Since 2014 the EU has engaged with the Mediterranean countries through the framework of the European Neighbourhood Policy (ENP). This policy is based on a series of contracts and aims to regulate and advance the EU's relations with its neighbours in the east and south.

In this final chapter, I situate the sale and use of surveillance technologies within the EU's policies towards the Med. I discuss the EU's favouring of stability over democracy and how this leads to increased authoritarianism**.** Finally, I pick up Zureik's (2013) argument on the spillover of surveillance technology in the context of colonialism and argue that the unchecked spread of such technology will eventually harm Europe.

4.1. Principled Pragmatism vs. Democracy

After the Arab Uprisings, the EU supported democratic developments in countries undergoing transitions by taking a *deep democracy* approach which meant that democratic reforms would lead to greater access to European markets and mobility for citizens; this conditionality was called 'more for more.' The European Parliament also supported a so-called 'less for less' approach where increased authoritarian policies would be met with punitive consequences in terms of access and mobility. The latter approach was never applied across the Med, not even in Egypt after its violent coup in 2013, argues Ruth Hanau Santini (2019). Regardless, most countries in the Med took paths towards stronger authoritarianism. When fears of asylum seekers and refugees began to take centre stage in European elections, even the former approach, which had been implemented "within a neoliberal procedural understanding of democracy," according to Hanau Santini (2019), was no longer applied. The EU needed countries in the Med to prevent asylum seekers from arriving on European shores and this goal trumped the aim to support democracy. Hanau Santini also argues that the EU's support for democracy was only ever "half-hearted" due to a procedural and depoliticised understanding of democracy, which influenced the EU's foreign policy approaches (2019).[11]

In 2015, the EU's policy with regards to the Med shifted to a focus on the following three areas: trade, security cooperation, and migration and mobility. Governance and democracy were still mentioned as aspects of the framework, but no actual plans or steps were mentioned. The

[11] Democracy and citizenship were regarded as consisting of mostly civil rights and less so political rights. The latter approach was only endorsed by the European Endowment for Democracy (EED) (Hanau Santini 2019).

Commission's new framework also included broad and unsubstantiated statements, such as "[a]n open and free internet should also be promoted" (European Commission 2015). This strongly influenced the EU's approach to Egypt where the military had regained absolute power after a coup in 2013 and after two years of increasingly oppressive policies against civil society, journalists, and the broader public. While the EU had supported the Egyptian steps towards democratic reforms before the coup, it neither halted economic cooperation after the coup, nor did it take any other significant steps to halt the authoritarian surge. As part of the policy shift in 2015 towards defence focus and mobility control, the EU instead focused on supporting the fight against cybercrime in the Med. Citing the *EU Cybersecurity Strategy* as framework, the Commission called on the EU to offer capacity building on cybersecurity to fight cybercrime and cyber terrorism, and on resilient information infrastructures (European Commission 2015).

In reaction to the so-called 'migrant-crisis' in 2015, the EU established the *Emergency Trust Fund for Africa* whose real aim was to curb irregular migration to Europe. The trust funded activities which provided capacity building and training for law enforcement in border management, migration management, and prevention of radicalisation (European Commission 2019).[12] The trust fund was part of investigations published in a report by Privacy International called *Teach 'em to Phish* (2018b). The report argued that a large section of the fund's money was actually spent on training and capacity building for law enforcement to better control and monitor borders. Thereby, PI argued, the EU and individual EU member states sponsored the spread of surveillance technologies globally in order to ensure that the majority of forcibly displaced people would be unable to cross the borders of countries in the Mediterranean. This has been immensely lucrative for the surveillance industries which are intricately involved in the sale and delivery of surveillance training programmes. As part of this goal to curb mobility, Frontex, the European borders agency, developed information sharing mechanisms with countries in North Africa (and elsewhere). The Libyan Coast Guard received limited access to Frontex and was trained in using a Geographic Information System platform which was specifically tailored to their needs to monitor the border (Frontex n.d., 1). Privacy International (2018b, 5) concludes that these policies facilitated "human rights abuses" and allowed "authoritarian […] leaders to use migration to gain political and economic support." This dynamic is not entirely new, albeit the focus on controlling the mobility of refugees and migrants is. In the wake of 9/11, authoritarian heads of states used their performances of counter-terrorist activities to avoid criticism of human rights abuses and presented their oppression of activists as counterterrorism.

[12] Seven percent of the fund's total budget are "used to fund security forces in third countries, which are implemented by private and public companies," says Privacy International (2018b, 26).

In June 2016, the EU adopted the European Global Strategy (EUGS) titled *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy* under the new overarching goal of 'principled pragmatism.' The strategy further strengthened the focus on security and defence, resilience of neighbouring states to respond to crises, and good governance (European Commission 2016). The guiding axiom of principled pragmatism indicated a neglect of democracy promotion, which was left to the EED, a much smaller policy instrument (Hanau Santini 2019). Instead focus was put on training or financing security agencies in third countries under the umbrella of the *Common Foreign and Security Policy* and the *Common Security and Defence Policy*.[13] In addition, individual EU member states heavily invest in training third countries in counterterrorism and intelligence gathering (Vallance 2016). The UK has had an established training partnership with the Saudi Ministry of the Interior since 2009, and planned to also train Saudi law enforcement in "High Tech Crime and IT Digital Forensics" and "I-Phone and GSM mobile telephone GSM examination and analysis."[14] Germany has been training Egyptian authorities on how to best investigate Internet users since 2011 (Privacy International 2018b). Faced with public pressure and investigations, the German government stated that until 2016, the Egyptian authorities had not misused the skills or the information shared with them as part of their training. The German government only cancelled a workshop to train authorities in Internet surveillance out of fear of misuse of this training in 2016 (Privacy International 2018b). Thus, the combination of a lack of genuine support for political, social and economic rights by the European Union with the training on surveillance and intelligence gathering for the authoritarian governments in the Med emboldened in their persecution of civil society and the opposition.

This was only worsened by the Trump administration's lacklustre support for democracy and human rights which has further contributed to the impunity of authoritarian leaders in MENA. Kristian Coates-Ulrichsen argues that this has become apparent in the dismissive reaction of Saudi Crown Prince Mohammed bin Salman to Sweden, Germany, and Canada criticising the kingdom's human rights practices (2019). Another example are the UAE informal business boycotts of European states after they suspended the sales of arms to the UAE out of fear they would be used in the Yemen War. As a consequence, the EU has struggled even more

[13] The Commission also financed many trainings in surveillance capabilities among EU members.

[14] See document at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/07_06_16_saudi_foi.pdf. The main mechanism for such external assistance is the *Instrument Contributing to Stability and Peace* (IcSP), which structures the delivery of trainings in conflict prevention, peace-building and short-term assistance in crises of the EU since 2014. One IcSP project trained Tunisian security forces "by developing "intelligence processing and analysis", "providing training in digital intelligence gathering including through social media and digital mapping", and "developing inter-service cooperation among Tunisian security agencies"" (Privacy International 2018b, 23). Another project focused on establishing a coordination centre in Iraq to ensure smooth collaboration between the different Iraqi intelligence services (Privacy International 2018b).

to balance support for democracy and the need for strategic economic and political alliances in the Middle East. In most cases, instead of stepping up support for democracy, the EU has opted for the support of stability.[15] Nevertheless, the belief that support of authoritarian regimes will increase longterm stability is a fallacy that has been proven wrong again and again; the large number of uprisings in the region are a clear indication. The EU's focus on stability is—in its own words—"built on democracy, human rights and the rule of law and economic openness" (European Commission 2015, 2). The stability of the Middle East should not be built on the opposite.

4.2. Spillover of Surveillance Technology

The widespread use of spyware leads to several potential harms for Europe. European countries have a history of selling weapons systems to third countries, but the crucial difference between conventional weapons and digital weapons is that the latter are geographically less limited. There is little difference between targeting a phone in the UK or within the Saudi borders. As a consequence, European states and their citizens or residents easily become targets of spyware. This has already become reality when Saudi Arabia spied on Amnesty International staff and other human rights activists residing in London.[16] It appears that Saudia Arabia can use this technology with impunity.

The sale of surveillance technology directly endangers the privacy and rights of European citizens and makes means of communication less safe for everyone. As mentioned in the first chapter, the application of surveillance technology does not take place in isolation. I cited Elia Zureik (2013) who argues that practices of surveillance and control would eventually spill over from colonized countries to what he refers to as home countries. Virginia Eubanks (2013) makes the similar argument that "most sweeping digital surveillance technologies are designed and tested in what could be called "low rights environments"—poor communities, repressive social programs, dictatorial regimes, and military and intelligence operations." One example she uses are Long Range Acoustic Devices (LRADs) which emit pain-inducing sounds over very long distances. Developed by the US military to be deployed in the Global South, they were used to disperse protestors at the G20 summit in Pittsburgh in 2009 (Eubanks 2013). Thus, the deployment and sale of surveillance technology for use in the Global South will lead (and has led) to a spillover of this technology into Europe.

[15] In other cases, the EU has taken a united, political stance against the US: for example, when the US retreated from the nuclear deal in 2018, the EU pushed forward which had a positive impact (Coates-Ulrichsen 2019).
[16] See section 3.2.2 on p 13 for details.

5. Conclusions: Surveillance Spilling Over and Increased Authoritarianism

In this study, I have argued that surveillance as an exercise of power needs to be understood in light of its origins in colonial settings. I showed how these roots influence surveillance practices today. I looked at three well-known companies selling surveillance technology in MENA: NSO, Gamma Group, and Hacking Team. I explained their capabilities and well documented cases where their software was used. I argued that, first, these companies operate under a veil of secrecy and should be aware of the potential abuse of their technology. Second, the activities of these companies have made it more apparent that some Gulf countries, prominently Saudi Arabia, Bahrain, and the UAE, are pursing closer relations with Israel. This shift in alliances has emerged in the past years but has taken clearer shape during the Trump administration. Finally I have argued that, in the last decade, the European Union's policy in the MENA region has shifted its emphasis from supporting social justice and democracy—albeit only a focus on formal aspects—to focusing on 'stability'—meaning, support for authoritarian governments. The latter have vastly expanded their use of surveillance technology and use it with increasing impunity. The sale of surveillance technologies in an environment where human rights infringements remain unchallenged by the EU and the US reduces the chances of the emancipatory movements active across the MENA region.[17] In this context, the extent of abuse of these technologies which I have demonstrated in this study makes a need for tighter regulations on their sale apparent.

5.1. Recommendations

Aside from emboldened authoritarian leaders through the sale of surveillance tools and a diminished support for democracy, the increased influence over policy by surveillance companies constitutes another potential global harm.[18] The *UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* warned that regulations around the sale of spyware were too loose and that companies have too much influence over the policies that should regulate their operations and business.[19] He argues in his 2019 report that industry interests were allegedly able to "significantly curtail the inclusion

[17] This does not mean that any support for emancipatory movements in the region is always helpful. It needs to be kept in mind that both the EU and the US pursue their own interests in the region which do not align with social justice or anti-neoliberal policies.
[18] A recent example is the case of the DigitalEurope association which represents among others the following companies: "Nokia, Siemens, AMETIC, IBM, ANITEC, Cisco and Microsoft" (RSF 2017). Together with representatives from Austria, Finland, France, Germany, Poland, Slovenia, Spain, Sweden and United Kingdom, they managed to significantly weaken regulation proposed by the European Council and Parliament that was intended to impede the sale technology that could also be used for surveillance (RSF 2017).
[19] A/HRC/41/35, ¶ 17.

of human rights safeguards in proposed regulatory changes, despite broad agreement on their adoption in the European Parliament."[20]

This dependency on private companies is reinforced by a revolving door phenomenon whereby many security officials often work in these companies and vice versa. In the end, these developments lead to the hollowing out of European sovereignty and democracy. Corporate social responsibility is not an option to curb the sale of invasive spyware to authoritarian regimes and more democratic governments worldwide, since the companies are already very aware to whom they sell their surveillance tools. In 2014, the EU has started to develop stricter guidelines for the sale of surveillance technology, but the efforts were thwarted by pressure from tech industry lobbyist (RSF 2017). In 2019, the European Parliament approved a proposed list of dual-use technology tech for sale, but again a group of seven countries blocked the suggestion from passing, arguing that it would portray Europe as "a technology-averse continent" (Stupp 2018). Nevertheless, more and stricter regulation is very necessary unless EU member states are willing to risk that their technology facilitates further crackdowns.

[20] A/HRC/41/35, ¶ 21.

6. Bibliography

Access Now. 2018. “EU: States Push to Relax Rules on Exporting Surveillance Technology to Human Rights Abusers.” *Access Now* (blog). June 11, 2018. https://www.accessnow.org/eu-states-push-to-relax-rules-on-exporting-surveillance-technology-to-human-rights-abusers/.

Ahram Online. 2014. "Egypt begins close monitoring of online communication with new technology." *Ahram Online*, September 17, 2014. english.ahram.org.eg/NewsContent/1/64/111038/Egypt/Politics-/Egypt-begins-close-monitoring-of-online-communicat.aspx.

Amnesty International. 2018. “Amnesty International Among Targets of NSO-Powered Campaign.” *Amnesty International*, August 1, 2018. https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

Angwin, Julia, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras and James Risen. 2015. “AT&T Helped U.S. Spy on Internet on a Vast Scale." *The New York Times*, August 15, 2015. https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0.

Anstis, Siena. 2018. “Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry.” *The Citizen Lab*, December 12, 2018. https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

Andrejevic, Mark and Kathy Gates. 2014. “Big Data Surveillance: Introduction.” *Surveillance and Society* 12: 185-196.

Arnold, Stephen E. 2013. Interview “Dr. Jerry Lucas of Telestrategies.” *ArnoldIT* (blog). January 15, 2013. http://arnoldit.com/search-wizards-speak/telestrategies-2.html.

Ball, James. 2013. "NSA monitored calls of 35 world leaders after US official handed over contacts." *The Guardian*, October 25, 2013. https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

Bridle, James. 2018. *New Dark Age: Technology and the End of the Future*. London and Brooklyn: Verso Books.

Brewster, Thomas. 2018. “Exclusive: Saudi Dissidents Hit With Stealth IPhone Spyware Before Khashoggi’s Murder.” *Forbes*, November 21, 2018. https://www.forbes.com/sites/thomasbrewster/2018/11/21/exclusive-saudi-dissidents-hit-with-stealth-iphone-spyware-before-khashoggis-murder/.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham and London: Duke University Press.

Coates-Ulrichsen, Kristian. 2019. “European ‘Middle Powers’ and the Middle East in the Age of Trump and Brexit.” *Project on Middle East Political Science* (blog). March 15, 2019. https://pomeps.org/european-middle-powers-and-the-middle-east-in-the-age-of-trump-and-brexit.

Eubanks, Virginia. 2014. "Want to Predict the Future of Surveillance? Ask Poor Communities." *The American Prospect*, January 15, 2014. https://prospect.org/power/want-predict-future-surveillance-ask-poor-communities./

European Commission. 2015. “Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.” *Review of the European Neighborhood Policy*, 18 November 2015.

European Commission. 2016. “Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union’s Foreign and Security Policy”. Accessed December 22, 2019. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

European Commission. 2019. “International Cooperation and Development: Regions: Africa: The EU Emergency Trust Fund for Africa.” Accessed December 14, 2019. https://ec.europa.eu/europeaid/regions/africa/eu-emergency-trust-fund-africa_en.

Foucault, Michel. 1979. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Franceschi-Bicchierai, Lorenzo. 2015. "Spy Tech Company 'Hacking Team' Gets Hacked." *Vice*, July 6, 2015. https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked.

———. 2018. "Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia." *Vice*, January 31, 2018. https://www.vice.com/en_us/article/8xvzyp/hacking-team-investor-saudi-arabia.

Franceschi-Bicchierai, Lorenzo, and Joseph Cox. 2018. “Inside a Demo of NSO Group’s Powerful IPhone Malware.” *Vice*, September 20, 2018. https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo.

Frontex. n.d. “Frontex cooperation with non-EU countries April 2015-April 2017.” Accessed December 22, 2019. https://www.asktheeu.org/en/request/4085/response/13249/attach/3/Frontex%20cooperation%20with%20non%20EU%20countries.pdf.

Hanau Santini, Ruth. 2019a. “EU Foreign Policy in MENA: The Pitfalls of Depoliticization.” *Project on Middle East Political Science* (blog). March 15, 2019. https://pomeps.org/eu-foreign-policy-in-mena-the-pitfalls-of-depoliticization.

Hern, Alex. "How the UN Unearthed a Possible Saudi Arabian Link to Jeff Bezos Hack." *The Guardian*, January 22, 2020. https://www.theguardian.com/technology/2020/jan/22/how-the-un-unearthed-a-possible-saudi-arabian-link-to-jeff-bezos-hack.

Howell O’Neill, Patrick. 2017. “ISS World: The Traveling Spyware Roadshow for Dictatorships and Democracies.” *CyberScoop,* June 20, 2017. https://www.cyberscoop.com/iss-world-wiretappers-ball-nso-group-ahmed-mansoor/.

HRW**.** 2013. "Egypt: No Acknowledgment or Justice for Mass Protester Killings." *Human Rights Watch*, December 10, 2013. https://www.hrw.org/news/2013/12/10/egypt-no-acknowledgment-or-justice-mass-protester-killings.

Kaplan, Martha. 1995. “Panopticon in Poona: An Essay on Foucault and Colonialism.” *Cultural Anthropology* 10: 85-98.

Kauanui, J. Kēhaulani. ""A structure, not an event": Settler Colonialism and Enduring Indigeneity," *Lateral* 5.1 (2016). https://doi.org/10.25158/L5.1.7.

Kenyon, Miles. 2019. “Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes.” *The Citizen Lab,* April 1, 2019. https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/.

Khalili, Laleh, and Jillian Schwedler. 2010. “Introduction.” In *Policing and Prisons in the Middle East: Formations of Coercion*, edited by Laleh Khalili and Jillian Schwedler, PP. London: C Hurst & Co Publishers Ltd.

Kirkpatrick, David D., and Azam Ahmed. 2018. “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.

Liebermann, Oren, and CNN. 2019. “How a Hacked Phone May Have Led Killers to Khashoggi.” *CNN*, January 20, 2019. https://www.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html.

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. 2015. “Mapping FinFisher’s Continuing Proliferation.” *The Citizen Lab*, October 15, 2015. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

Marczak, Bill, and John Scott-Railton. 2016. “The Million Dollar Dissident: NSO Group’s IPhone Zero-Days Used against a UAE Human Rights Defender.” *The Citizen Lab*, August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. 2018. “HIDE AND SEEK: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries.” *The Citizen Lab*, September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Marczak, Bill, Siena Anstis, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. 2020. "Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator." The Citizen Lab. January 28, 2020. https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/.

McKune, Sarah, and Ron Deibert. 2017. “Who’s Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking.” *The Citizen Lab*, March 2, 2017. https://citizenlab.ca/2017/03/whos-watching-little-brother-checklist-accountability-industry-behind-government-hacking/.

Mitchell, Timothy. 1988. *Colonizing Egypt*. Berkley, Los Angeles and London: University of California Press.

Nassar, Tamara. 2019. “Israel to Take Part in Dubai’s Expo 2020.” Text. *The Electronic Intifada,* May 2, 2019. https://electronicintifada.net/blogs/tamara-nassar/israel-take-part-dubais-expo-2020.

Privacy International. 2018a. “Exploiting Privacy: Surveillance Companies Pushing Zero-Day Exploits.” *Privacy International*, February 7, 2018. http://privacyinternational.org/blog/1245/exploiting-privacy-surveillance-companies-pushing-zero-day-exploits.

———. 2018b. “Teach ’em to Phish: State Sponsors of Surveillance.” London: Privacy International. https://privacyinternational.org/sites/default/files/2018-07/Teach-em-to-Phish-report.pdf.

Rabinow, Paul. 1989. *French Modern: Norms and Forms of the Social Environment*. Chicago and London: University of Chicago Press.

RSF. 2017. “International Regulations: Broken or Blocked by Lobbies | Reporters without Borders.” *RSF*, March 10, 2017. https://rsf.org/en/reports/international-regulations-broken-or-blocked-lobbies.

Stupp, Catherine. 2018. “Nine Countries Unite against EU Export Controls on Surveillance Software.” *Euractiv.Com* (blog). June 8, 2018. https://www.euractiv.com/section/cybersecurity/news/nine-countries-unite-against-eu-export-controls-on-surveillance-software/.

Times of Israel. 2019. “UAE officials: Relations with Israel won’t change despite invite to World Expo in Dubai.” *Times of Israel*, 2019. https://www.timesofisrael.com/liveblog_entry/uae-officials-relations-with-israel-wont-change-despite-invite-to-world-expo-in-duabi/.

TOI Staff. 2019. “Despite denials, official says Israeli delegation attended Bahrain conference.” *Times of Israel*, 18 April 2019. https://www.timesofisrael.com/despite-denials-official-says-israeli-delegation-attended-bahrain-conference/.

Vallance, Chris. 2016. "Torture Fears as UK Police Train Saudis." *BBC News*, June 7, 2016. https://www.bbc.com/news/uk-36468268.

Wilson, Tom, and Mehul Srivastava. 2019. “Inside the WhatsApp Hack: How an Israeli Technology Was Used to Spy.” *Financial Times*, October 30, 2019. https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229.

Wolff, Josephine. 2019. “Opinion | Whatever You Think of Facebook, the NSO Group Is Worse.” *The New York Times*, November 6, 2019, sec. Opinion. https://www.nytimes.com/2019/11/06/opinion/whatsapp-nso-group-spy.html.

Zureik, Elia. 2013. “Colonial Oversight.” *Red Pepper* (blog). November 16, 2013. http://www.redpepper.org.uk/colonial-oversight/.