O El-Ashy, I Maroni, H Mizyed, R Nammar & M Al-Maskati 'Big Brother in the Middle-East and North Africa: The expansion of imported surveillance technologies and their supportive legislation' (2019) 3 *Global Campus Human Rights Journal* 229-249 https://doi.org/20.500.11825/1577

Big Brother in the Middle-East and North Africa: The expansion of imported surveillance technologies and their supportive legislation

Ola El-Ashy, Ilaria Maroni,** Hazem Mizyed,*** Razan Nammar**** and Mohammed Al-Maskati******

Abstract: *The article analyses digital surveillance companies and the possibilities that technology makes available to oppressive regimes: from monitoring centres facilitating mass surveillance on all telecommunications, to firewalls that filter what users can access, and spyware that tap into the information stored in any personal device connected to the internet. This grim picture of new technologies becomes significantly darker when taking into account the volume of this 'international repression trade' and the market value of surveillance companies operating in states self-identified as democracies.*

Key words: *digital rights; surveillance; cyber-crime legislation; right to privacy; freedom of expression; national security; cyberwar; information technology; human rights defenders*

1 Introduction

Digital rights no longer are a simple extension of human rights. They have become central components of several rights: digital media for the right to information; social media for the right to free assembly; cybercommunication for the right to privacy; and so forth. Parallel to these developments, cyberspace has become a crucial arena for political action but also for repression. Activists use it to share information and to mobilise, while repressive governments have been resorting to surveillance technology in order to suppress social movements, and to identify and apprehend activists and dissidents.

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. MA holder (Arab Masters for Democracy and Human Rights), Human Rights and Legal Researcher; olaelashi93@gmail.com

** MA (Democracy and Human Rights in the MENA Region), MA (International and Diplomatic Affairs); Reporter, freelancer; ilaria.maroni@hotmail.it

*** MA (Human Rights and Democratisation); social entrepreneur interested in new technologies; Hazem.mizyed@gmail.com

**** MA (Democracy and Human Rights), MA (Democratic Governance – Rule of Law in the MENA Region); International Law Consultant, freelancer; r.namari@live.com

***** MA (international studies), Digital security expert, MENA Digital protection Coordinator for Front Line Defenders; mohdmaskati@protonmail.com

Authoritarian governments depend on cyber-surveillance companies based in democratic countries, which are developing and exporting sophisticated software needed to monitor electronic device activities and data stored on hard drives, or intercept data transmitted over wireless or cable networks. Surveillance technologies can map relationships, recognise patterns, and analyse discourse. They can target different types of data: Audio and video surveillance tap into household and corporation surveillance camera systems. Phone monitoring gathers data communicated across mobile, fixed or next generation networks. Location monitoring intercepts the location of a target using phone identifiers or tracking devices. Internet monitoring technologies gather information communicated across the internet, often on a mass scale. This can be done through monitoring centres that hack into internet communications, telephones, computer networks and databases using several tools. Intrusion is a tool that works though the installation of spyware on communication devices that can extract data and control functions. Biometrics software allows individuals to be monitored through the identification and recognition of their physiological or behavioural characteristics. Bug detection tools allow counter-surveillance (Privacy International 2016).

Even though some parts of the Middle East and North Africa are lagging behind technologically, authoritarian regimes have generally upgraded their control and repression mechanisms through the use of sophisticated digital surveillance technologies. The restriction on digital rights, most notably freedom of expression, the right to privacy and the right to information, is further supported by new legislation that aims to silence human rights defenders and activists calling for democratisation. We will first look into the exportation and use of digital surveillance technology through the study of three companies originating and functioning in countries that are considered democratic: Amesys, Netsweeper and the NSO group, headquartered in France, Canada and Israel respectively. We next examine how some states in the Middle East and North Africa that are importing these technologies are enacting anti-cybercrime laws to reap the full benefits of these technologies, focusing on Palestine, Jordan, Egypt and Bahrain.

2 Exporting surveillance technologies

The first part of this article examines three companies based in self-identified democracies that export different types of surveillance technologies to authoritarian regimes: French Amesys produces mass surveillance technologies to monitor communications on specific networks; the Canadian Netsweeper provides technologies and services for internet content filtering and blocking; and the Israeli NSO Group infects targeted devices through spyware that extracts data.

3 Monitoring centres: The case of the French Amesys

'We are in a world now where not only is it theoretically possible to record nearly all telecommunications traffic out of a country, all telephone calls, but where there is an international industry selling the devices now to do it' (Wikileaks.org nd). This statement by Julian Assange was well

illustrated in an Amesys brochure that Wikileaks had found and published in 2011. One of its illustrations shows the difference between lawful interception that only tracks internet protocol addresses and the mass surveillance that the company proposes which allows the monitoring of the whole traffic on any given network, regardless of data format (audio, video or text). The services that this French company offers do not require the hacking of individual devices through the use of malicious software but monitors the national network, or any specific network, through the use of keywords (Wikileaks.org 2011).

Following the fall of Muammar Gaddafi's regime in Libya, an abandoned monitoring centre in Tripoli was discovered containing Amesys training manuals and posters. One of the posters about the Eagle system read: 'Whereas many internet interception systems carry out basic filtering on IP address and extract only those communications from the global flow [legal interception], Eagle Interception system analyses and stores all the communications from the monitored link [massive surveillance]' (Garcia et al 2015). The Libyan authorities had been using a Deep Packet Inspection technology and analysis software developed by Amesys. In an interview published by the French newspaper *Figaro* in September 2011 a former official of the Libyan External Security Organisation explained that the system was able to find 'targets within the country's massive flow' and to identify 'individual suspects using keywords'. This witness summed it up as follows: 'We listened in on the entire country.' The system was subsequently used to create data analysis methods that were applied to the collected data to hone keywords used for queries and to monitor the findings obtained collaboratively with Libyan authorities, in particular the Libyan military high command' (FIDH 2014).

Amesys had sold to the Libyan government the telecommunication surveillance system called Eagle, as a 'favour' on behalf of the French President (Tesquet 2017). This technology was allegedly used in the tracking and torturing of dissidents and activists. It allowed the Libyan authorities to confront dissidents and activists with private social media texts and emails (FIDH 2014). This sale took place following Libyan leader Muammar Gaddafi's visit to France in 2007. At that time, the International Federation for Human Rights and the Libyan League for Human Rights were pressuring the government not to support a regime responsible for 'serious human rights violations' by either 'tolerating' or directly committing such violations. This action did not prevent the sale or discourage the two civil society organisations from pursuing their pressure. In 2011 they filed a complaint which sparked an investigation into the sale of this technology (FIDH.org 2015). Shortly thereafter the company rearranged its operations. Stephan Salies, owner of Amesys, created two new companies with different names: Advanced Middle East Systems based in the United Arab Emirates (UAE), and Nexa Technologies in France. They improved the Eagle system and called it Cerebro with reference to a tracking device used in the X-Men science fiction series (Tesquet 2017). Their technical documentation 'promises "real-time surveillance of suspects", thanks to particularly intrusive sensors capable of tracking emails, text messages and accessing chat rooms and social media sites'. It adds that 'investigators can follow their target's activities by entering advanced criteria (email address, telephone numbers, keywords)' (Tesquet 2017). In 2017 Nexa Technologies made headlines by selling surveillance technology to Egypt. Cerebro had been gifted to Egypt by the

Emirati government. According to the French daily *Le Monde*, the UAE purchased for €10 million a monitoring system which was to be directed against the Muslim Brotherhood. 'In a nod to the pyramids, the operation was code-named Toblerone' (Tesquet 2017).

4 Canadian firewall and filters: The case of Netsweeper

Netsweeper provides internet filtering services to individuals, corporations and governments. On the website of this Canadian company, their products are associated with the rise in 'cyber-threats, cyber-crime, hacktivism, the proliferation of illicit content and attacks on critical infrastructure and intellectual property' (Netsweeper.com nd). The application of online filtering technologies determines the landscape of the internet with which the user can interact. Artificial intelligence (AI) offers 'dynamic classification and categorisation, which optimises network usage while providing a positive, productive, and safe internet experience' (Netsweeper.com nd). Indeed, the use of filtering technologies is varied. They are used by schools and universities to create a 'safe environment' for students. Internet service providers can filter websites harbouring criminal content linked to terrorist groups or child pornography. However, in all cases filtering technologies offers control over the content that is accessible on the network. This raises concerns related to freedom of thought, speech and action, with an intensity commensurate to the level to which this control is exerted.

The use of pre-set filters becomes particularly problematic when states use them to block a certain type of online content from their country. Netweeper offers multiple filtering categories from which the customer can choose. The categorisation occurs in more than 30 languages, and they are driven by AI and human review. As the Citizen Lab explained: 'A network administrator need only select a given content category – such as 'gambling' or 'hate speech' – and all content categorised as such will be blocked. Creating this database of websites and the ongoing process of categorisation is a substantial undertaking (The Citizen Lab 2018). The company claims that it has categorised over 10 billion uniform resource locators (URLs) and that it categorises 22 million new URLs each day (Netsweeper.com nd). By 2022 it is estimated that the value of the web content filtering market will be US $3,8 billion (The Citizen Lab 2018).

Netsweeper claims centralised control over its products. However, it has multiple distributing partners around the world and has branches in the Middle East, South America and the United States. Its software is installed on public networks in Bahrain, Pakistan, Qatar, Somalia, United Arab Emirates and Yemen (The Citizen Lab 2018). In the UAE, Netsweeper's filters categorise the entire World Health Organisation website as pornographic; and so are the websites of the Christian Science Monitor, the World Union for Progress Judaism, the Centre for Health and Gender Equity, and Change Illinois (Pangburn 2018). After criticisms relevant to the technologies enabling the blocking of lesbian, gay, bisexual, transgender and questioning (LGBTQ) and HIV-related content or pages categorising them as pornographic, Lou Erdelyi, Netsweeper's chief technology officer, explained that '[a]s of December 25th, 2018, Netsweeper no longer has a category titled LGBTQ+ nor does it block such content' (Pearson 2019). The company also claims less categorisation

relevant to the category of 'alternative lifestyles'. Nevertheless, there are concerns about the use of these technologies in countries considered authoritarian. While Netsweeper's technologies are often used for purposes of safe internet browsing, such as blocking child pornography websites or websites considered inappropriate for school internet, they also often are used by authoritarian regimes to block websites of opposing political views, and human rights-related content.

5 Intrusion technologies from Israel: The case of the NSO Group

In December 2018 an Israeli cyber-security company, NSO Group, gained media attention when Omar Abdulaziz, a Saudi dissident, accused it of infiltrating his smartphone. Abdulaziz pressed charges, claiming that the firm had sold its signature spyware to the Saudi government and given access to his conversations with Jamal Khashoggi. According to the lawsuit, this played a major role in 'the decision to murder' the *Washington Post* columnist and political opponent who was lured into the Saudi consulate in Istanbul and dismembered (Kirkpatrick 2018).

It was not the first time that the NSO Group came under the spotlight. In fact, after operating in the shadows for years, Citizen Lab brought it to light. Citizen Lab is an interdisciplinary laboratory at the Munk School of Global Affairs and Public Policy at the University of Toronto. It is tasked with producing 'evidence-based research on cyber-security issues that are associated with human rights concerns', using a 'mixed methods approach to research combining practices from political science, law, computer science, and area studies' (The Citizen Lab 2018). Academics at the Citizen Lab receive financial support from a vast range of donors, including the Canada Centre for Global Security Studies and Open Society Foundation. This internet 'watchdog' reported in 2016 that Ahmed Mansoor, a human rights activist living in the UAE, had received a text message with a suspicious link. Mansoor forwarded it to the task force and they were able to uncover what a cyber-security firm described as 'the most sophisticated, targeted, and persistent mobile attack ever found on iOS', and traced it back to the NSO Group (Lookout.com 2016). We will look into how a small Israeli start-up turned into one of the most controversial partners of Arab authoritarian governments in less than a decade.

The NSO Group is high-ranking among so-called 'internet mercenaries' (Mazzetti et al 2019). It was established by two high school and army friends, Shalev Hulio and Omri Lavie, who sought to break into encrypted communications by developing software that could hack smartphones. The company came into existence only two years later with the expertise of the Israel Defence Force's Unit 8200, of whom Hulio and Lavie are believed to be veterans (Brewster 2016). Unit 8200 is the equivalent of the US National Security Agency (NSA). It is an intelligence unit in the front lines of Israel's cyber-wars. According to Israeli investigative journalist Yossi Melman, one can find Unit 8200 'whenever there is a very significant or risky operation … Even days or weeks before the actual operation taking place. There is not a single major Israeli intelligence operation in which Unit 8200 is not involved' (Behar 2016). Allegedly, this unit was responsible for infecting computers at Iran's Natanz uranium enrichment

facility with Stuxnet, a worm created in cooperation with the NSA and the Central Intelligence Agency (CIA) (Behar 2016).

This unit of the Israeli army is not only involved in international warfare but also in the daily occupation of Palestinian territories. As such, it is also engaged in managing the daily lives of Palestinians living in the West Bank and under blockade in the Gaza Strip. In 2014, 43 former soldiers and active reservists spoke out, revealing how they were responsible for collecting an extensive range of electronic communications from Palestinians, such as 'email, phone calls and social media in addition to targeting military and diplomatic traffic' (Beaumont 2014). Long before experts raised doubts about the potential risks of technology use for human rights, Unit 8200 started enacting massive surveillance and espionage at the expense of 'innocent people unconnected to any military activity'. Other testimonies published stated: 'On a personal level, there is no respect for Palestinian privacy'; 'if anyone interests us, we'd collect information on his or her economic situation and mental state … in order to turn them into a collaborator or something of the sort'; and 'whether said individual is of a certain sexual orientation, cheating on his wife, or in need of treatment in Israel or the West Bank – he is a target for blackmail' (*The Guardian* 2014). The 43 *refuseniks* were quickly expelled from the Unit for crossing 'a red line' and acting 'inappropriately' (*The Guardian* 2015).

In early 2011 the company tested the first version of *Pegasus*, its signature spyware software. Its website claims that its technology 'helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe' against 'terrorists, drug traffickers, paedophiles, and other criminals' and 'the world's most dangerous offenders'. Pegasus is spyware that acts in the background to extract private information. It usually installs itself through malicious texts and emails, or public wi-fi networks (Perlroth 2016). In late 2016 the *New York Times* received internal NSO Group correspondence and contracts from two sources close to the company. The article lists the price of surveillance: starting from a $500 000 installation fee, an extra $650 000 for access to ten iPhone users; $650 000 for ten Android; $500 000 for five BlackBerry; and $300 000 for five Symbian (Perlroth 2016). Six months later the Israeli newspaper *Haaretz* wrote that the Saudis agreed to pay 55 million for the Pegasus 3 (Harel et al 2018). For this price, Pegasus can extract text messages, contacts, e-mails, GPS locations and passwords; it can record and listen to phone calls, and even turn on the microphone and the camera on a smartphone. What is distinctive about this product is the complete absence of footprint: It is almost impossible to discover, and it has a 'self-destructive' feature that destroys all traces if detected (Franceschi-Bicchierai et al 2018).

In order to prevent the technology from 'falling into the wrong hands', NSO Group co-president Tami Shachar explained in an interview that the company has three levels of vetting (Stahl 2019). As cyber-surveillance technology sales are equivalent to arms exports, the Israeli Defence Ministry needs to approve every potential customer. However, so far there is no evidence of any rejection. The company has also created a business ethics committee, which had denied sales to Turkey but not to Mexico and Saudi Arabia (Mazzetti et al 2019). Lastly, every client must sign a

'contractual agreement' in which they declare that 'the only intended use of the system will be against terror and crime' (Stahl 2019).

Under this legal vacuum and lack of accountability, Pegasus has infected devices in possibly as many as 45 countries (Marczak et al 2018). Between August 2016 and August 2018, researchers found more than a thousand IP addresses and domain names related to the Israeli firm's 'dirty work' (Marczak et al 2018). Two important cases have revealed its *modus operandi*: one in the UAE and one in Mexico. The first case is that of Ahmed Mansoor, a world-renowned activist who is currently serving a 10-year prison sentence for expressing his criticism of the Emirati government's human rights abuses. After more than a year in prison without trial, he was condemned on charges of disseminating fake news online and jeopardising the country's reputation (Front Line Defenders 2019). His health is deteriorating and appeals from Human Rights Watch, Amnesty International, Frontline Defenders and others have so far remained unheard. In the summer of 2016, while on a *de facto* travel ban with his passport having been confiscated by the authorities (Human Rights Watch 2019), Mansoor received a suspicious text containing a link that promised 'new secrets' about detainee conditions in UAE. Mansoor did not fall for the bait. Instead, he sent the message content to the Citizen Lab that was able to trace it back to the NSO Group and their attempt to install Pegasus on the activist's iPhone.

In June 2017 the *New York Times* broke the news on how the Mexican government was using NSO Group's technology against citizens who were neither terrorists nor criminals. The media outlet revealed that Pegasus had infiltrated the devices of lawyers, anti-corruption activists, journalists and civil society representatives (Ahmed et al 2017). In the same hours, the Citizen Lab posted its comprehensive findings: Victims, including media and television personalities, non-governmental organisation (NGO) members, and even the under-age son of a reporter, received fake messages containing the spyware (Scott-Railton et al 2017). Following the public outcry, then President Enrique Peña Nieto responded with a letter to the *New York Times*, denying all accusations and stating that there was no evidence that the Mexican government was behind the surveillance (Beauregard 2017).

Throughout 2018 Pegasus's attacks increased, and so did attention from public opinion and media, which started questioning cyber-security companies and governments buying their technology. The NSO Group's products were used to infiltrate devices of Amnesty International staff (Ingleton 2018), which quickly prompted the Israeli Ministry of Defence to withdraw licences for the firm (Amnesty International 2018). Saudi Arabia was the most prolific customer, with many attempts on dissidents living abroad, such as Ghanem Almasarir, a comic in London (Stahl 2019), and Omar Abdulaziz.

Since Jamal Khashoggi's murder in the Saudi consulate in Istanbul, the NSO Group has focused all its efforts on rebranding (Franceschi-Bicchierai 2019). Under a new marketing strategy to make the company appear more appealing and transparent, co-founder and CEO Hulio declared on television that Pegasus prevents 'crime and terror' saving 'tens of thousands of people' and helping 'create a safer world' (Stahl 2019). When asked about the role of his company in the killing of the Saudi dissident, he evaded the question, saying that he was not willing to 'talk about

specific customers'. Other public relation moves consist of allowing cameras inside their once-secretive headquarters in Herzliya, creating a brand-new website, and releasing public statements after any allegation made by the media. Current estimates value the NSO Group around $1 billion (Haaretz 2018). Not all the rebranding efforts are succeeding. At the beginning of 2019, AP News broke the story of individuals using fake names and affiliations who contacted two Citizen Lab researchers investigating the NSO Group. The academics were filmed while they were being questioned about Israel, anti-Semitism and religion. Although no connection with the NSO Group was proven, these tactics recall the assignments of the Black Cube, a private Israeli intelligence agency, tasked with harassing Harvey Weinstein's accusers (Satter 2019).

Although producing different surveillance technologies, the NSO Group, Amesys and Netsweeper operate with a similar pattern. The three companies are all based in democratic countries, but that does not prevent them from selling their products to authoritarian governments with little control or accountability. In fact, most of their activity is kept hidden from public scrutiny. Nevertheless, the multiple scandals surrounding the sale of surveillance technology to authoritarian governments, especially the judicial case that was opened against Amesys, drew more attention aimed at better regulating the export of surveillance and dual-use technologies. The Wassenaar Arrangement is the main regulatory regime for such technologies. '[It] has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies' (Garcia el al 2015). It stipulates which military and dual-use goods (that have both military and civilian use) should be subject to licensing and has 41 participating states, including Russia, Japan, the US and the member states of the European Union. However, the list of items is also used by a large number of non-signatory states as part of their own licensing regulations, including Israel and China (Privacy International 2016).

As technology progresses, the regulation of exports of digital surveillance needs to be continuously updated. The EU Dual-Use Regulation 429/2008 restricts the export of specialised large-scale IP monitoring systems. The French government specifically pushed for export control mechanisms within the European Union that would regulate Amesys's technology and it implemented these regulations immediately after their adoption by Wassenaar in 2013 (FIDH.org 2015). Nevertheless, Amesys was granted nine other licences since the beginning of 2016: three in West Africa, two in the Middle East, one in sub-Saharan Africa, one in Europe, one in Asia and one in South America. The surveillance technologies arms race goes on. As a person in the business confided (Tesquet 2017):

> Of course the French services subcontract technical intelligence. It's either that or handing control to the Chinese or the Israelis. We aren't Care Bears. We tell ourselves we are doing it in the interests of our country. In any case, all the countries are equipping themselves, whether it's through us or elsewhere.

The exportation of digital surveillance tools sometimes is referred to as the international repression trade (Privacy International 2016). Born over four decades ago, it has expanded exponentially in the last decade, yet reliable

data remains scant. Nevertheless, the trade volume of surveillance technologies is estimated (CAUSE, 2015) between US $5 and $12 billion (Kirkpatrick 2019). This probably explains the failings of international regulations and the national legislation of countries that export surveillance technologies. However, they are also supported by the political needs of the importing governments that have been developing and upgrading their legislation in an effort to regulate the internet and cyber-space usage, but also to fully benefit from the features and results that those powerful weapons provide.

6 Domestic legal support systems for surveillance: Middle Eastern cyber-crime legislation

Governments in the Middle East and North Africa have been updating their legislation relevant to cyber-crimes following a similar repressive pattern meant to support the use of surveillance technologies. This has led to a trending practice of persecuting journalists and activists for views and posts shared on social media platforms. With the widespread use of social media in recent years, some states have dealt suspiciously with journalists, bloggers, human rights defenders and activists, and started to censor criticism towards public figures. Some authorities have detained, interrogated, prosecuted and, in some cases, physically harmed internet users due to their posts. Imported surveillance technologies play a central role in this repression as they allow the identification of critics and political opponents, and the gathering of data that can be used against them. However, in order to prosecute them a new legislation needs to be drafted, allowing the state to qualify their actions as offences. We will look into how this legislative process is unfolding in Bahrain, Egypt, Jordan and Palestine, and the specific tools used to support repression, namely, vague terminology, numerous regulatory bodies and the possibility of shutdowns.

7 Vague cyber-offences and creeping cyber-crime laws

There is a striking similarity between two cyber-crime laws enacted recently in the Middle East; those of Jordan and Palestine. The similarities go beyond their content and into the way in which they were actually adopted. Both states passed them without a public consultation or debate. However, this approach meant to bypass civil society and stifle any opposition to them. Both legislation was met with opposition from civil society organisations (CSOs) that considered them a breach to the right of freedom of expression and opinion.

In 2015, the Jordanian government introduced draft cyber-crime legislation, intended to update the Information Systems Crime Law of 2010 (House 2016). It was met with immediate condemnation from CSOs. Protests flared for two years when this legislation was used to sentence six journalists to six months imprisonment and a fine of $80 000 (Ersan 2018). The journalists had been arrested due to a complaint by Secretary-General Youssef Issawi to the Anti-Cyber Crime Unit at the Public Security Directorate for a video shared on Facebook accusing him of 'appropriating government funds and state lands to build a road to his palace'. Protestors argued that the law infringed on the right to privacy, freedom of

expression and digital rights. In December 2018 these protests resulted in the government withdrawing the 2015 law for further amendments (Now 2019). Two days later, the Jordanian government presented to the Parliament an amended law, once again without engaging with CSOs. The amendments expanded the scope of cyber-crime to encompass hate speech. It also increased the penalty from one week to three months' and up to one year's imprisonment and raised the fines for perpetrators from $140-$280 to $700-$1 400. The amendments raised concerns among human rights activists and advocates who feared that the Bill would restrict freedom of speech online. In November 2018, Jordanian activists launched a social media campaign, calling on the government to withdraw the cyber-crime law.

In February 2019, the Jordanian Parliament voted in favour of amending certain clauses of the law, in particular the clauses on hate speech and fake news. The definition of hate speech that it introduced was vague, stating that 'every writing and every speech or action intended to provoke sectarian or racial sedition, advocate violence or foster conflict between followers between different religions'.

Activists, journalists and human rights defenders perceived this vagueness of terms as an increased threat and feared that the government would use this law to prosecute its critics. It blurred the lines between hate speech, criticism of public figures and freedom of opinion and expression (Times 2019).

In Palestine the cyber-crime legislation was enacted in June 2017 through a Presidential Decree. In several of its 61 clauses, Cyber-Crime Law 16 allows disproportionate and indiscriminate infringements on several rights, including freedom of expression and opinion, the right to privacy and access to information. The Law uses vague terms to describe several offences, such as 'threat to national security', which can lead to harsh imprisonment sentences and excessive fines for online criticism. Some clauses of the Law, particularly articles 32, 33 and 34, authorise surveillance of social media users and blocking websites and pages without a court warrant. Security services can easily force internet providers to disclose their customers' data, even if this breaches the company's code of conduct and violates the customer's privacy (Advancement 2018). It has also become common practice for Palestinian security services to force civilians to disclose their passwords to access their personal pages and deliberately interfere with what they post (Watch 2018).

The enactment of the Law came about without previous consultation with CSOs or a public debate. Based on this Law, especially its article 20, journalists, activists and human rights defenders were arrested for propagating news that allegedly threatened national security (Ayad 2018). The adoption of the cyber-crime law increased the scope of repression allowing security forces to prosecute and silence voices due to loose clauses and vague terminology (Watch 2017). Immediately upon the enactment of the Law, a large-scale surveillance campaign was carried out against independent and opposition news websites in the West Bank. In one month alone, internet providers blocked 29 websites following an official order issued by the Attorney-General of Palestine, Ahmad Barrak (Odeh 2018). On 4 June 2017 Palestinian security forces detained a Palestinian journalist, Thaher Al-Shamali, for publishing an article that criticised the Palestinian President. He was charged with 'insulting higher

authorities and causing strife'. Nasser Jaradat, a media student, was also arrested for sharing Al-Shamali's article on his Facebook page. Both were detained for 15 days under the same charges (AbuShanab 2017; Abdelbaqi 2016).

Human rights organisations campaigned against the cyber-crime law and demanded its immediate suspension. This demand was raised in a session at the office of the Palestinian Liberation Organisation (PLO) in Ramallah, where a coalition of 11 organisations submitted their comments and objections to Hanan Ashrawi, the head of the PLO Department of Culture and Information (Musawa 2017). This action led to the Ministry of Justice organising governmental consultations with CSOs to discuss possible amendments to the Law. Some amendments were adopted, but these were minimal, and the Law remained vague and prone to infringe on freedom of expression and opinion and digital rights, under the pretext of combating cybercrimes (Ayad 2018).

The Palestinian anti-cybercrime legislation is not the only framework through which the freedom of expression and opinion in cyber-space is breached in Palestine. The country is not a sovereign state and is divided into two entities governed by rival Palestinian factions. The Gaza Strip is governed by Hamas and is under Israeli blockade, while the West Bank is governed by Fatah and is under Israeli occupation. This means that the Palestinian authority's legal instruments and practices are not the only ones to directly impact Palestinian lives, their digital rights, freedom of expression and access to information. In recent years, Israel has been manipulating and pressuring social media giants such as Facebook and YouTube, to remove posts and block personal and official Palestinian pages under the guise that they 'incite' against Israel (Odeh 2016). This goes contrary to the International Covenant on Civil and Political Rights (ICCPR), particularly article 19 (UN General Assembly 1966) in its General Comment 34 which states that offences 'such as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying" or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression'. The compliance of Facebook and YouTube with the Israeli government's requests undoubtedly restricts freedom of expression, reducing the role and the capacity of social media and internet platforms, and preventing journalists from accomplishing their work on informing the general public (Odeh 2016).

At the same time, criticism on social media of Fatah and Hamas among media activists, human rights defenders and the public in general is met with firm actions by Palestinian security forces (Watch 2018). These actions sometimes lead to the detention and torture of journalists and activists giving rise to self-censorship on social media and internet platforms (Odeh 2016). The Palestinian government had targeted journalists and activists who opposed or criticised the government prior to the enactment of the cyber-crime law, prosecuting them under the Penal Code. Similarly, in Gaza freedom of expression has declined sharply since the internal political divide, in 2007. Hamas uses different forms of restrictions against journalists and activists, including detention, threats and torture, to stifle any element that criticises or threatens its rule.

8 The multiplication of regulatory bodies and the instrumentalisation of internet technology companies

Some anti-cybercrime legislation in the region have relied on legal techniques other than 'vague terminology' to ensure stronger control over cyber-communication and social media. Bahrain, for example, set up several regulatory bodies to monitor and prosecute dissenters. Egypt has transformed internet service providers into control agents executing the government's policies. The establishment of regulatory bodies and the transformation of information technology (IT) companies into regulatory agents are not the only tools governments use to 'regulate' internet use. They sometimes resort to non-regulated shutdowns of local or national communication systems in an effort to silence the opposition.

In Bahrain the government has over the years gradually introduced several restrictive instruments varying from laws and regulations, governmental bodies, and surveillance software to monitor citizen activities online. These instruments are allegedly meant to safeguard national security and order. However, they resulted in a massive crackdown on internet users that reveal their intention to silence political dissidents (Bahrain Centre for Human Rights 2018).

Bahraini authorities practise surveillance and censorship through several laws and regulations. The government passed the Press Law 47/2002, which regulates both online and print media. This law allows strict control on the circulation of sensitive topics. Article 19 prohibits the publication of any content 'instigating hatred of the political regime, encroaching on the state's official religion, breaching ethics, encroaching on religions and jeopardising public peace' (Bahraini Journalists Association 2019). The Minister of Information issued Decree 68/2016, which further restricts the distribution of electronic media and empowers the state to target and prosecute content publishers (Bahraini Journalist Association 2019). In 2014 Bahrain passed its national cyber-crime legislation under Law 60/2014 on Information Technology Crimes. The Law is complementary to the Media Regulation Law of 2002, as it provides in article 23 penalties for infringing the complementary regulations (Bahraini Journalists Association 2019).

The government did not limit itself to drafting new laws and regulations. It also created governmental bodies to monitor cyber-activities: the Information Affairs Authority, established in 2010; the General Directorate of Anti-Corruption and Economic and Electronic Security, established in January 2011; and the Cyber Safety Directorate, established in November 2013. The Information Affairs Authority (IAA) is responsible for monitoring all media outlets in Bahrain, whether printed or online media, to ensure their compatibility with media regulations. It has the authority to block any website or content for allegedly 'instigating hatred of the political regime, encroaching on the state's official religion, breaching ethics, encroaching on religions and jeopardising public peace or raising issues whose publication is prohibited by the provisions of this law' (Bahraini Journalist Association 2019). The Ministry of Interior set up another monitoring authority, namely, the General Directorate of Anti-Corruption and Economic and Electronic Security. This authority tracks internet users who violate the media regulation laws, and opens an investigation of those who offend, defame and insult others online. The

Directorate has summoned and interrogated human rights defenders, political activists and social media activists over charges of insulting or offending a governmental body, the King, or a neighbouring country (General Directorate of Anti-Corruption and Economic and Electronic Security 2019). The third governmental body was set up by the Ministry of Telecommunications Affairs. The mandate of the Cyber Safety Directorate is to 'assume its role in monitoring websites and social media networks to ensure they are not used to instigate violence or terrorism and disseminate lies and fallacies that pose a threat to the kingdom's security and stability' (Bahrain Centre for Human Rights 2013). In addition, a hotline and an email address were published for the general population to report any infringement of the 'right cyber-agenda' as regulated by the laws (Bahraini Ministry of Interior 2013).

The legislation and governmental bodies that were set up to 'regulate' cyber activity actually curb freedom of expression and the right to information. Criticism of the royal family and sometimes of the political and economic situation is not tolerated. Activists were arrested for sharing satirical content opposing the regime. For example, a women's rights activist, Ghada Jamsheer, was arrested in 2014, her blog and Twitter account were blocked, and she was sentenced to a year in prison for defamation and insulting the royal family through a tweet she posted about corruption in a hospital managed by a royal family member (Bahrain Centre for Human Rights 2015). Similarly, the president of Bahrain's Centre for Human Rights (BCHR), Nabeel Rajab, was arrested in 2016, allegedly for disseminating false news on his Twitter account when he published a report on torture incidents in Bahrain's prison and violations committed by the Saudi Coalition forces in Yemen (Bahrain Centre for Human Rights 2016). This type of censorship is supplemented by another one that targets websites: Over 1 000 websites were blocked 'for sharing illegal content', and so was an encrypted messaging and Voice over IP service such as Telegram in 2011 (The Verge 2019) and prominent live streaming services broadcasting Shiite religious ceremonies such as PalTalk and Matam.tv in 2013 (Reporter-ohne-grenzen.de 2019). Not surprisingly, a United Nations (UN) spokesperson at the Human Rights Council in Geneva noted that Bahrain had failed to obey 176 of the Council's recommendations (Civicus.org 2017).

In Egypt the government not only blocked websites, but shut down all communication systems in an effort to curb the mobilisation efforts of the opposition forces and isolate the protests from the world's attention at the wake of the Arab Spring. Indeed, the government obliged telecommunication companies in January 2011 to shut down the internet, and voice and texting services. In 2014 the Egyptian government used a surveillance system called 'See Egypt' to monitor the internet activity of activists, tapping into their email accounts and Skype calls (Buzzfeed News 2018). This surveillance system penetrates laptops remotely and access personal data, such as pictures, passwords and files. It can also operate cameras and microphones to record conversations. It was used against Esraa Abd El- Fatah, a prominent human rights activist, who had her personal photos, email and phone calls leaked on Facebook. This was used to 'expose her indecency' and undermined her credibility (Freedom House 2018).

In 2018 the President of the republic ratified Law 180, an anti-cyber-crime law directed towards users and internet service providers, further restricting digital rights. Article 7, for instance, allows the blocking of websites accused of publishing content constituting a threat or a crime against national security and the economy. Also, it obliges internet service providers to block access to the website within 48 hours whenever notified. This allowed the blocking of 500 websites in March 2018 under the claim of disseminating fake news (Access Now 2018). This anti-cyber-crime legislation also focuses on regulating social media discussions. It provides that any user with 5 000 followers can be considered as operating a media platform and could be held accountable for sharing 'fake news'. Consequently, it led to the imprisonment of Facebook users for the dissemination of unfavourable opinion (BBC News 2018). Such was the case of Masoum Marzouk, a former diplomat, who had called for early presidential elections on his Facebook page (BBC News 2018). Article 9 of the Law authorises internet service providers to store their customers' information and data, such as messages, website visits and telephone calls, up to 180 days and to hand it to the authorities when requested (IFEX 2018). This provision was translated into reality when the government requested Uber and Careem car services to hand over their customers' data (Mada Masr 2018). Allegedly, the purpose of this legislation and policy is to counter terrorism. Nevertheless, they contradict article 57 of the Egyptian Constitution which states:

> The right to privacy may not be violated, shall be protected and may not be infringed upon. The state shall protect citizens' right to use all forms of public means of communications. Interrupting or disconnecting them, or depriving the citizens from using them, arbitrarily, is impermissible. This shall be regulated by law.

Internet shutdowns not only affect the social interaction and communication between individuals, but also have major negative implications on the economy. Internet disruptions caused great losses to the global economy estimated at US $2,4 billion between July 2015 and July 2016 (Brookings Institution 2016). In Egypt the five-day internet shutdown meant to disperse protesters generated a loss estimated at $90 million. In Bahrain the government shut down mobile internet services in the Duraz area following protests against the government's decision to revoke a Shiite religious leader's citizenship. This decision cost an estimated US $1,2 million to the Bahraini economy (Brookings Institution 2016).

The shutdown decision not only affects political and civil rights, but also strongly impacts social and economic rights, affecting manufacturers and service providers that rely on e-commerce, cutting them off from domestic customers and global trade (Seib 2007). Even the health sector was affected by the shutdown as it disrupted communications with its suppliers (OECD 2011).

9 Conclusion

In 2011 new technologies undoubtedly supported the wave of contestation that swept over North Africa and the Middle East. When this wave toppled three regimes and shook the foundations of many others, what was then referred to as the Arab Spring was also dubbed the 'Twitter revolutions',

highlighting the important role digital social media and, more broadly, information and communication technologies played in political mobilisation and the contestation of authoritarian rule. This reflected a certain transformation of cyber-space into a public sphere, close to Jurgen Habermas's definition of a space (albeit virtual) in which citizens gather to articulate the needs of their society. Such analysis and interpretations today are much debated, but at the time they reflected a general optimistic narrative surrounding the use of information and communication technologies and the possibilities they offered.

In this article we looked into the promises of digital surveillance companies and the possibilities that technology makes available to oppressive regimes, from monitoring centres facilitating mass surveillance on all telecommunications, to firewalls that filter what users can access, and spyware that taps into the information stored in any personal device connected to the internet. This paints a grimmer picture of new technologies, one which becomes significantly darker when one takes into account the volume of this 'international repression trade' and the market value of those surveillance companies operating in states that are self-identified as democracies.

Even when there is general agreement that these surveillance technologies are powerful weapons that can be used in both civil and military terrains, their economic value for the nations that produce them, and their political importance to the nations that import them, have deeply affected the way in which governments regulate their sale and use.

On an international level, the sale of these technologies is not regulated by a treaty, but through a voluntary agreement that does not contain provisions for enforcement and compliance. Each member state to the Wassenaar Agreement develops and enforces its own control policies and only consults with other member states. The core objectives of the Agreement, namely, the promotion of transparency and greater responsibility in transfers of dual-use goods and technologies, seem to be contradicted by the sales of surveillance systems to several countries in the Middle East and North Africa. Not only are these sales not transparent, with the public never hearing about them unless information is leaked or some evidence of their criminal use is found many years after their sale; but the governments of exporting countries seem to regularly turn a blind eye to their sale to repressive governments because of the economic importance of these transactions and the wealth generated by these companies.

At the national level the use of these technologies in the Middle East and North Africa is not directly regulated by any particular law. This means that there is no particular legislation that bans or authorises the use of mass surveillance, interception technologies or filters. However, anti-cybercrime laws indirectly authorise the use of some of these technologies (that is, monitoring, filtering and banning), and inform on the repressive intentions of the legislator and the controlling character of the regulations. We have seen four indicators that can be used to determine the repressive nature of an anti-cybercrime legislation: the use of vague terminology in the definition of cyber-offences; the absence of discussions with CSOs when passing the legislation; the multiplication of regulatory bodies; and the transformation of internet service providers into control agents. These

indicators may be used as red flags when it comes to the sale of surveillance technologies.

We have also seen that public opinion and CSO mobilisation against repressive anti-cybercrime legislation or the sale of surveillance technology to repressive regimes has not been very effective. In the case of mobilisation against legislation, they can delay the enactment of anti-cybercrime laws, but have sometimes resulted in the passing of even more problematic legislation. As far as the mobilisation against the sale of repressive technologies is concerned, the media and CSOs have played a vital role in informing the public about these sales and the use of these technologies that massively violate human rights. In this regard, there are several success stories that show the importance but also the limits of such actions. The French courts put Amesys under judicial investigation in 2012 on account of the sale of surveillance technology used against political opponents to apprehend them. In 2017 the Italian Ministry of Economic Development revoked the authorisation given to several companies to sell internet network surveillance systems to Egypt following media attention and pressure from CSOs. However, these actions have not prevented authoritarian regimes from upgrading their repressive techniques through other surveillance products proposed by other companies, most of which are equally based in self-identified democratic countries. This reveals the fragility of digital rights that remain largely unprotected in both international and domestic laws, but also how this fragility directly impacts broader human rights.

References

7amleh (2018) *Has the Palestinian Cybercrime Law really been amended?* available at https://www.apc.org/en/news/has-palestinian-cybercrime-law-really-been-amended (last visited 22 April 2019)

Abdelbaqi M 'Enacting cybercrime legislation in an endeavour to counter cybercrime in Palestine' (2016) 5 *Global Journal of Comparative Law* 226

Access Now 'Access now' (2019), available at https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/ (last visited 15 April 2019)

Ahmed A 'A journalist was killed in Mexico. Then his colleagues were hacked' (2018) Nytimes.com, available at https://www.nytimes.com/2018/11/27/world/americas/mexico-spyware-journalist.html?login=email&auth=login-email (last visited 15 April 2019)

Amnesty 'Rogue NSO Group must have licence revoked' (2018), available at https://www.amnesty.org/en/latest/news/2018/11/israelroguenso-group-must-have-licence-revoked-over-controversial-surveillance-software/ (last visited 15 April 2019)

Ayad C 'Policing the digital sphere: The impact of Palestine's cybercrime legislation', available at https://archives.arab-reform.net/en/node/1384 (last visited 15 April 2019)

BBC (nd) 'Egypt to regulate popular social media users', available at https://www.bbc.com/news/world-middle-east-44858547 (last visited 17 July 2017)

Bahraini Journalists 'Bahraini Journalists Association – Press law' (2019), available at http://www.bahrainijournalists.org/References_and_documents/Law (last visited 15 April 2019)

Bahrain Rights 'Bahrain: The "cyber safety directorate" monitors internet activity in style similar to Big Brother' | Bahrain Centre for Human Rights (2013), available at http://www.bahrainrights.org/en/node/6624 (last visited 23 June 2019)

Bahrain Rights 'Women human rights activists Zainab Al-Khawaja and Ghada Jamsheer sentenced to prison again' | Bahrain Centre for Human Rights (2015), available at http://www.bahrainrights.org/en/node/7540 (last visited 22 June 2019)

Bahrain Rights 'Updates: Arrest and detention of BCHR's President Nabeel Rajab' | Bahrain Centre for Human Rights (2016), available at http://bahrainrights.org/en/updates-arrest-and-detention-bchrs-president-nabeel-rajab?_ga=2.268717169.104442301.1555430839-556041828.1554588691 (last visited 22 June 2019)

Bahrain Rights 'Bahrain: The "cyber safety directorate" monitors internet activity in style similar to Big Brother' | Bahrain Centre for Human Rights (2019), available at http://www.bahrainrights.org/en/node/6624 (last visited 22 June 2019)

Beaumont P 'Israeli intelligence veterans refuse to serve in Palestinian territories' *The Guardian* (2014), available at https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories (last visited 22 June 2019)

Beauregard L '*El Gobierno mexicano declaró secretos los contratos sobre el "software" del espionaje a periodistas*' *El País* (2017), available at https://elpais.com/internacional/2017/06/20/mexico/1497984473_017962.html (last visited 22 June 2019)

Behar R 'Shadow wars: In missions stretching from Iran to Syria, Israel's Unit 8200 can be (not) seen' (2016), Forbes.com, available at https://www.forbes.com/sites/richardbehar/2016/05/11/shadow-wars-in-missions-stretching-from-iran-to-syria-israels-unit-8200-can-be-not-seen/#2b01c2c759ae (last visited 22 June 2019)

Ben-Hassine W 'Egyptian Parliament approves cybercrime law legalizing blocking of websites and full surveillance of Egyptians' Access Now (2018), available at https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/ (last visited 22 June 2019)

Bing C & Schectman J 'Special report: Inside the UAE's secret hacking team of US mercenaries' reuters.com (2019), available at https://www.reuters.com/article/us-usa-spying-raven-specialreport/special-report-inside-the-uaes-secret-hacking-team-of-u-s-mercenaries-idUSKCN1PO19O (last visited 22 June 2019)

Brewster R 'Everything we know about NSO group: The professional spies who hacked iPhones with a single text' Forbes.com (2016), available at https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#262c2f213997 (last visited 22 June 2019)

Brookings Institution 'Global economy loses billions from internet shutdowns' 6 October 2016, available at https://www.brookings.edu/blog/techtank/2016/10/06/global-economy-loses-billions-from-internet-shutdowns (last visited 22 June 2019)

Buzzfeed New 'Egypt begins surveillance of Facebook, Twitter, and Skype on unprecedented scale' (2019), available at https://www.buzzfeednews.com/

article/sheerafrenkel/egypt-begins-surveillance-of-facebook-twitter-and-skype-on-u (last visited 22 June 2019)

European Parliamentary Research Service 'STOA – Science and Technology Options Assessment', available at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf (last visited 22 June 2019)

FIDH (The International Federation for Human Rights) 'A critical opportunity: Bringing surveillance technologies within the EU Dual-Use Regulation' (2015), available at https://www.fidh.org/IMG/pdf/cause_report_final.pdf (last visited 23 June 2019)

Franceschi-Bicchierai L & Cox J 'Inside a demo of NSO group's powerful iPhone malware' Vice (2018), available at https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo (last visited 22 June 2019)

Franceschi-Bicchierai L 'Israeli hacking company NSO group is trying to clean up its image' Vice (2019), available at https://www.vice.com/en_us/article/qvy97x/israeli-nso-group-marketing-pr-push (last visited 22 June 2019)

Freedom House 'Freedom of the net' (2016), available at https://freedomhouse.org/report/freedom-net/2016/jordan (last visited 16 May 2019)

Freedom House 'Freedom on the net 2018 – Egypt' 1 November 2018, available at https://www.refworld.org/docid/5be16b1c4.html (last visited 22 June 2019)

Front Line Defenders 'UAE – Human rights defender Ahmed Mansoor detained' (2019), available at https://www.frontlinedefenders.org/en/case/ahmed-mansoor-detained. (last visited 22 June 2019)

Gallagher R 'French company that sold spy tech to Libya faces judicial inquiry amid new allegations' (2012), available at https://slate.com/technology/2012/06/amesys-facing-inquiry-in-france-over-selling-eagle-surveillance-technology-to-qaddafi.html (last visited 25 June 2019)

General Directorate of Anti-Corruption & Economic & Electronic Security .acees.gov.bh. (2019), available at http://www.acees.gov.bh/about-acees/ (last visited 22 June 2019)

Harel A, Levinson C & Kubovich Y 'Israeli NSO negotiated with Saudis advanced cyberattack capabilities sale, Haaretz reveals' haaretz.com (2018), available at https://www.haaretz.com/israel-news/.premium-israeli-company-negotiated-to-sell-advanced-cybertech-to-the-saudis-1.6680618 (last visited 22 June 2019)

Human Rights Watch 'Palestine: Reform restrictive cybercrime law (2017), available at https://www.hrw.org/news/2017/12/20/palestine-reform-restrictive-cybercrime-law (last visited 15 April 2019)

Human Rights Watch 'Two authorities, one way, zero dissent: Arbitrary arrest and torture under the Palestinian authority and Hamas' (2018), available at https://www.hrw.org/report/2018/10/23/two-authorities-one-way-zero-dissent/arbitrary-arrest-and-torture-under (last visited 18 April 2019)

Human Rights Watch 'UAE: Free rights defender Ahmed Mansoor' (2019), available at https://www.hrw.org/news/2019/04/12/uae-free-rights-defender-ahmed-mansoor (last visited 22 June 2019)

IFEX 'Egypt's cybercrime law and Media Regulation Bill violate right to freedom of expression' – IFEX (2018), available at https://www.ifex.org/egypt/2018/09/06/egypt-cybercrime-media-regulation (last visited 22 June 2019)

Ingleton D 'Meet NSO Group: A go-to company for human rights abusers' Amnesty.org (2018), available at https://www.amnesty.org/en/latest/news/2018/08/is-nso-group-a-goto-company-for-human-rights-abusers/ (last visited 22 June 2019)

Jordanian Times 'MPs reject new amendments to cybercrime law' (2019), available at http://www.jordantimes.com/news/local/mps-reject-new-amendments-cybercrime-law (last visited 25 April 2019)

Julliard J 'Enemies of the internet countries under surveillance' Reporter-ohne-grenzen.de. (2019), available at https://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/2010/Feinde_des_Internets.pdf (last visited 22 June 2019)

Kirkpatrick D 'Israeli software helped Saudis spy on Khashoggi, lawsuit says' Nytimes.com. (2018), available at https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html (last visited 22 June 2019)

Lookout 'Trident zero-day iOS vulnerabilities lead to real-world espionage' (2016), available at https://www.lookout.com/trident-pegasus-enterprise-discovery (last visited 22 June 2019)

Mada Masr 'Interference with uber app tied to company's refusal to share user data with security bodies' Mada Masr (blog) (2019), available at https://madamasr.com/en/2019/01/30/feature/politics/sources-say-uber-blocked-in-egypt-for-refusing-to-share-customer-data-with-government/ (last visited 22 June 2019)

Marczak B & Scott-Railton J 'The million dollar dissident: NSO Group's iPhone zero-days used against a UAE human rights defender' The Citizen Lab (2016), available at https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (last visited 22 June 2019)

Marczak B et al 'Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries The Citizen Lab (2018), available at https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ (last visited 22 June 2019)

Mazzetti M et al 'A new age of warfare: How internet mercenaries do battle for authoritarian governments' Nytimes.com. (2019), available at https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html (last visited 22 June 2019)

Musawa 'A legal memo to Dr Hanan Ashrawi regarding Decree-Law No (16) for 2017 on Cybercrimes' (2017), available at http://www.musawa.ps/post/a-legal-memo-to-dr.-hanan-ashrawi-regarding-decree-law-no.-16-for-2017-on-cybercrimes.html (last visited 15 April 2019)

Netsweeper (nd) 'Web Content Filtering • Netsweeper', available at https://www.netsweeper.com (last visited 23 June 2019)

NSO Group 'NSO Group – Cyber intelligence for global security', available at https://www.nsogroup.com (last visited 23 June 2019)

Odeh GB MADA (2016), available at http://www.madacenter.org/images/text_editor/FBviolationsE.pdf (last visited 16 April 2019)

Odeh GB 'Media freedom violations in Palestine 2017' (2018), available at http://www.madacenter.org/images/text_editor/annualrepE2017(1).pdf (last visited 19 April 2019)

OECD 'The economic impact of shutting down internet and mobile phone services in Egypt – OECD' (2019), available at https://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm (last visited 19 April 2019)

Pangbur D 'An app for protecting kids online is growing popular with autocrats' Fast Company (2018), available at https://www.fastcompany.com/40585513/an-app-for-protecting-kids-online-is-growing-popular-with-autocrats (last visited 23 June 2019)

Pearson J 'Canadian internet filtering company says it's stopped "alternative lifestyles" censorship' Vice (2019), available at https://www.vice.com/en_us/

article/3kgznn/netsweeper-says-its-stopped-alternative-lifestyles-censorship (last visited 23 June 2019)

Perlroth N 'How spy tech firms let governments see everything on a smartphone' Nytimes.com. (2016), available at https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html (last visited 23 June 2019)

Police Media Centre Archives (2019), available at https://www.policemc.gov.bh/en-archives/?cat=important-telephone-number&type=month&year=2016&month=8&start=01/08/2016&end=31/08/2016 (last visited 23 June 2019)

Privacy International 'The global surveillance industry' (2016), available at https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf (last visited 23 June 2019)

Privacy International. 'Italy cancels surveillance export to Egypt but new undercover documentary shows surveillance industry brazenly continues to export to repressive regimes' (2017), available at https://privacyinternational.org/advocacy-briefing/759/italy-cancels-surveillance-export-egypt-new-undercover-documentary-shows (last visited 25 June 2019)

Satter R 'AP NewsBreak: Undercover agents target cybersecurity watchdog' AP NEWS (2019), available at https://www.apnews.com/9f31fa2aa72946c694555a5074fc9f42 (last visited 25 June 2019)

Scott-Railton J et al 'Reckless VII: Wife of journalist slain in cartel-linked killing targeted with NSO group's spyware' - *The Citizen Lab* (2019), available at https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/ (last visited 25 June 2019)

Scott-Railton J et al 'Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware' - *The Citizen Lab* (2017), available at https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (last visited 25 June 2019)

Seib P (2007) *New media and the new Middle East* Palgrave Macmillan

Sonne P & Coker M 'Firms aided Libyan spies first look inside security unit shows how citizens were tracked' Nytimes.com. (2011), available at https://www.wsj.com/articles/SB10001424053111904199404576538721260166388 (last visited 25 June 2019)

Stahl L 'CEO of Israeli spyware-maker NSO on fighting terror, Khashoggi murder, and Saudi Arabia' Cbsnews.com. (2019), available at https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/ (last visited 25 June 2019)

Tesquet O 'Amesys: Egyptian trials and tribulations of a French digital arms dealer' Telerama (2017), available at https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php (last visited 25 June 2019)

The Citizen Lab 'Planet Netsweeper executive summary' (2018), available at https://citizenlab.ca/2018/04/planet-netsweeper/ (last visited 25 June 2019)

The Citizen Lab 'The Citizen Lab: Research and development at the intersection of digital media, global security, and human rights' Citizenlab.ca. (2018), available at https://citizenlab.ca/wp-content/uploads/2018/05/18033-Citizen-Lab-booklet-p-E.pdf (last visited 25 June 2019)

The Citizen Lab 'About the Citizen Lab - The Citizen Lab' (2019), available at https://citizenlab.ca/about/ (last visited 25 June 2019)

The Guardian 'Any Palestinian is exposed to monitoring by the Israeli Big Brother' (2014), available at https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-unit-testimonies (last visited 25 June 2019)

The Guardian 'Israel expels 43 intelligence veterans who refused to spy in Palestinian territories' (2015), https://www.theguardian.com/world/2015/jan/27/israel-expels-intelligence-veterans-who-refused-spy-occupied-palestinians (last visited 25 June 2019)

The International Federation for Human Rights 'The Amesys case' (2014), available at https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf (last visited 25 June 2019)

Toor A 'Bahrain's internet shutdown marks a "new form of information control"' The Verge (2019) available at https://www.theverge.com/2016/8/4/12373676/bahrain-internet-shutdown-duraz-protests (last visited 18 April 2019)

West DM 'Internet shutdowns cost countries $2.4 billion last year' Brookings.edu (2016), available at https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf (last visited 18 April 2019)

Wikileaks *WikiLeaks - The spy files* (2011), available at https://wikileaks.org/spyfiles/docs/amesys/99_eagle-glint-operator-manual-version-1-0.html (last visited 23 June 2019)