APC ISSUE PAPERS

DIGITAL SAFETY IN CONTEXT: PERSPECTIVES ON DIGITAL SECURITY TRAINING AND HUMAN RIGHTS REALITIES IN THE ARAB WORLD

By Reem Almasri
7IBER

EXECUTIVE SUMMARY

During 2011, in the period dubbed the "Arab Spring", the internet was a space for mobilisation. Since then, it has also become a space for oppression of activism and dissent. In countries where demonstrations calling for democracy erupted, authoritarian regimes resurfaced in different forms and shapes with intensifying violations of the human rights of citizens. While one cannot ignore the spectrum of violations across this region, in the past five years Arab governments have been generally more active in cracking down on online speech, public gatherings and assemblies, and the privacy of citizens, especially activists and journalists.

After the Snowden revelations in 2013, the world was consumed by news of violations of the privacy of citizens led by different intelligence units of the National Security

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Agency (NSA) of the United States and its UK equivalent, the Government Communication Headquarters (GCHQ). Among these revelations were reports of collaboration between foreign and Arab intelligence entities in surveillance programmes.

The combination of intense human rights violations in the Arab region, and increasing world consciousness of the insecurity of communication, led many human rights organisations to refocus their efforts on the provision of digital security support. The last five years were also characterised by the wave of programmes aiming to provide digital security support for activists, journalists and citizens, whether as individuals or institutions. Digital security trainings, workshops and consultations were widely held across the Arab region, advising targeted groups on methods to protect themselves from digital threats posed by governments and other groups, which could undermine their activities.

This paper has been developed in collaboration with the Association for Progressive Communications (APC) for the project "Building a culture of online human rights and digital security in the Maghreb-Machrek region", funded by the European Instrument for Democracy and Human Rights (EIDHR). It aims to highlight the links between the efforts of digital security trainings in the region with the human rights realities, focusing on two case studies: Morocco and Palestine.

To describe the current state of human rights with its commonalities and differences, we identified three common, visible and consistently violated human rights across Arab countries: the right to privacy, the right to freedom of expression, and the right to freedom of assembly. To explore the extent to which digital security programmes respond to the human rights and infrastructural realities, the author of this paper met with four digital security trainers and advocates from Morocco, Palestine and Egypt. Their experience in participating in or leading digital security workshops led to the following recommendations for the planning of digital security programmes:

- To increase the effectiveness of digital security programmes, contextual research should address the diverse human rights realities, not only at the country level, but also at the level of the targeted group.
- It is important to factor in the layout of the internet infrastructure of the country when assessing risks to digital security and advising on tools or practices.
- Digital security trainings and manuals should be behaviours-focused more than tools-focused.
- It is necessary to subject digital security manuals to technical and security risk audits prior to publishing.

INTRODUCTION

The wide spread of the internet in the Arab world has shaken the status quo of state-produced and controlled information. The acceleration in penetration rates in the region has created alternative narratives through blogs, forums, websites and social media accounts, which challenge the "red lines" of officially permitted speech. For governments, it was hard to control the online narrative using the same tactics they used to control print media. At the beginning of the blogs outburst in 2006, governments in the Arab region lost control over mainstream messages and could not deal with the new realities of decentralised information production imposed by the nature of the internet. However, these governments later developed and adapted legislative systems and deployed censorship and surveillance tools in an attempt to reclaim some authority over knowledge production[1] and to curtail opposition.

As governments in the region began to understand the role of the internet in documentation and mobilisation during the 2011 uprisings, they became persistent in attempts to extend governmental authority over online speech and access to information. This was manifested through widespread official efforts at packaging legislation to regulate cyber crimes, online media and online speech. One of the most obvious examples is extending the same licensing requirements of print news to online news websites. These amendments were accepted in Jordan's Press and Publication Law in 2012, and drafted in the amendments of the Press Law in Egypt in 2015.[2] The swift passage of cyber crime laws and anti-terrorism laws across different countries – including Jordan, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates (UAE) – also extended to the criminalisation of speech that insulted religion or the authorities or that disrupted the loose definitions of "national security" or "friendly relationships with other countries".

Governments in the Arab region are not only building legislative frameworks to control the online environment, they are also utilising the internet's infrastructure to crack down on activists and opposition figures. The Snowden revelations, WikiLeaks and human rights reports from research groups such as the Citizen Lab and Privacy International reveal the deployment of mass surveillance equipment and hacking tools to monitor activists' and journalists' communications and private data. Reports from Tunisia, Syria, Morocco, Sudan and Bahrain have revealed tactics that official intelligence agencies used to target activists' laptops and mobile phones through malware.

The acceleration in the spread of privacy loopholes in communication tools has also intensified the programmes developed by international and regional human rights organisations with the aim of protecting the digital security of activists and journalists. Trainings, meetings, workshops and manuals on the protection of personal communications from surveillance and reclaiming digital security have been widely developed and spread in the past two years.

Democracy, internet freedoms and human rights in Maghreb-Machrek

This paper has been developed in collaboration with the Association for Progressive Communications (APC) for the project "Building a culture of online human rights and digital security in the Maghreb-Machrek region", funded by the European Instrument for Democracy and Human Rights (EIDHR). The primary objective of this policy paper is to look at how digital security training and support provide an opportunity to link local digital security concerns in the Maghreb-Machrek region with broader human rights issues.

Specifically, this paper aims to highlight the links between the efforts of digital security trainings in the region with the human rights realities, focusing on two case studies: Morocco and Palestine. We identified three common, visible and consistently violated human rights across Arab countries: the right to privacy, the right to freedom of expression, and the right to freedom of assembly. Through the perspective of digital security trainers and privacy advocates in the region, this paper aims to suggest different considerations that developers of digital security programmes should incorporate in their workshops or manuals based on the context of human rights violations.

1 Almasri, R. (2015, 1 July). How digital content is controlled in Jordan. *7iber*. 7iber.com/wireless_research/how-digital-content-is-controlled-in-jordan

2 Hamama, M. (2015, 4 November). New plans to regulate digital media. *Mada Masr*. www.madamasr.com/sections/politics/new-plans-regulate-digital-media

It is important to understand that the selection of these three rights does not prioritise them when it comes to the wider spectrum of government-violated rights in the region. The selection of these rights is based on the extent of the population affected by violations of these rights, and our belief that protection of these rights is fundamental, among other things, in ensuring the protection of other rights, such as the right to freedom of religion, the right to a fair trial, and protection from the practice of forced disappearances, which also take place in these countries.

This paper is intended as an overall guide to the human rights situations of countries in the Arab region, while acknowledging that there are big differences in the human rights situations across the region. Morocco and Occupied Palestine have been chosen as case studies for a deeper review of the digital security situation.

In these two countries, literature on state surveillance and its impact is the most available, thanks to revelations of state-sponsored hacking attempts and persecution of activists for their public and private communications.

Methodology

For the purpose of this paper, the author met with four digital security trainers from Morocco, Palestine and Egypt. The selection of the trainers was dependent on their expertise in digital security tools and the number of workshops that they had led in the region. The four trainers were asked the following main questions:

- How do you adapt the digital security programmes you provide to the political and infrastructural realities of the internet in the countries where you lead these workshops?
- What in your opinion is the role of the digital security manuals produced by international and regional organisations? What are their points of relevance to and departure from the digital security needs of the local context?

KEY HUMAN RIGHTS ISSUES

THE RIGHT TO PRIVACY

Most Arab constitutions cover the right to privacy, but vary in mentioning details of private spaces and mediums. The Tunisian and Sudanese constitutions, for example, have an overarching umbrella protection for the right to a private life, domiciles, and personal information. Other constitutions have a specific phrase that establishes the protection of communications, including postal, telephone, and "any other kinds of communication".[3]

Despite constitutional protection of the right to privacy and the right to private communications, loopholes in safeguarding this right begin with detailing the conditions under which it can be restricted or limited. Only eight constitutions in the Arab region require a "judicial order" or "court order" to allow interception of private life, spaces or communications. These are Jordan, Egypt, Morocco, Libya, Iraq, Algeria, Yemen and Palestine. Among these, only Egypt's constitution mentions a "definite period" as a condition for interception on top of a judicial order. Most constitutions, especially in the Gulf region, state "the provision of law" as the basis of exceptions for interception. In general, most Arab legislative frameworks do not comply with the internationally recognised International Principles on the Application of Human Rights to Communications Surveillance.[4]

In places where the lines between the executive and judicial branches are blurred, and where loopholes in legislative frameworks allow for violations of rights, these rights are never safeguarded. This is visible in the regularity of detentions of citizens and journalists across the region for what is deemed "illegal speech" in private communication. After 2011, most Arab governments passed laws that legitimised the interception of private communication under the excuse of national security. For example, the Jordanian Anti-Terrorism Law was amended in 2014 to state, among other things, that the public prosecutor can intercept communications if he has "received reliable information that a person is connected to a terrorist activity." The activities that the same law loosely defines as "terrorist" include "harming the environment, public and private properties, causing strife, or disturbing the public order."[5] Many of the citizens charged under this law were charged for sharing content produced by ISIS on their Facebook accounts or in WhatsApp groups, which are not public. In Egypt, the re-enacted Emergency Law in the Sinai region allowed the seizure, search and surveillance of any communication or private space without a warrant.[6]

In Tunisia, the notorious surveillance apparatus of the Tunisian Internet Agency, ATI, abolished after the fall of Ben Ali, resurfaced again in the shape of the Technical Telecommunication Agency (ATT). The primary functions of the agency are "to investigate and record ICT-related crimes, to coordinate with telecom operators and access networks, and to monitor national telecom traffic in accordance with international human rights treaties and personal data protection laws."[7] The same decree declares that the reporting of such activities will be secret and only available to the government, which negates recommendations on state transparency of surveillance practices made by the UN Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism.[8]

Some Arab governments prohibit the use of encryption in their laws. In Egypt, the Telecommunication Law prohibits the use of encryption devices without the written consent of the National Telecommunication Regulatory Authority (NTRA), the military, and national security authorities.[9] Bahrain, Tunisia, Morocco and Iraq also have legal restrictions on the use of encryption over communication networks.[10]

3 Such as Jordan, Egypt, Morocco, Libya, Iraq, Bahrain, Oman, Qatar, Kuwait and UAE.

4 https://en.necessaryandproportionate.org

5 Almasri, R. (2014, 30 April). Jordan's Anti-Terrorism Law: A Choice between Security or Speech. *7iber*. 7iber.com/2014/04/anti-terrorism-draft-law-a-choice-between-security-or-speech

6 Privacy International. State of Surveillance: Egypt. https://privacyinternational.org/node/739

7 Social Media Exhange. (2014, 17 October). SMEX Launches "Working Drafts" Series on the Emerging Legal Framework for Free Expression Online in the Arab World. www.smex.org/working-drafts-series-intro

8 United Nations General Assembly. (2014). Report of the UN Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism. www.un.org/ga/search/viewm_doc.asp?symbol=A/69/397

9 Freedom House. (2014). Freedom on the Net: Egypt. https://freedomhouse.org/report/freedom-net/2014/egypt

10 Koops, B. J. (2013). Crypto Law Survey: Overview per country. www.cryptolaw.org/cls2.htm

In the name of security, the laws described here are legitimising the official monitoring of telecommunications, photographing of private places, and monitoring of both electronic and written communication as well as social media. The growth of state surveillance is increasingly restricting the use of conventional spaces for mobilisation, whether offline or online.

Surveillance tools and leaks

Prior to the wide spread of the internet, phone and human surveillance were essential techniques for intelligence services to curtail activism and control media across Arab countries. As much as the spread of the internet is a threat to Arab governments' control over information, it is also a space to expand the state's surveillance apparatus.

For a region where access to public information remains under the grip of the state, international and local leaks revealing violations of privacy are integral entry points to assess and investigate mass surveillance techniques used by states against their citizens, as well as cross-intelligence cooperation.

In this section, we will review what these leaks tell us about the existence of surveillance equipment and activities in different Arab countries. It is important to note that while these international leaks reveal the existence of surveillance equipment or discussions about its import/export, the nature and scale of the usage of such software and the entities using it are still not fully known.

The Snowden files

The Snowden files revealed information about cooperation between the National Security Agency (NSA, United States), Government Communication Headquarters (GCHQ, United Kingdom) and Arab intelligence agencies, whether through the secret tapping of data centres or payments to Arab intelligence departments in return for intelligence information. It was revealed, for example, that Oman hosted three GCHQ undersea cable centres that tap into various undersea cables passing through the Strait of Hormuz into the Persian/Arabian Gulf. The tapping was coordinated with British Telecom and Vodafone, the companies that operated these long distance optical fibre cables. Codenamed TIMPANI, this base taps into the Iraqi communications located near the Strait of Hurmuz. CLARINET, the second base, is near Yemen.[11]

Saudi Arabia is another country where intelligence coordination was revealed. A 2013 top secret memo from the NSA outlined the provision of surveillance equipment from the NSA to the Ministry of Interior, and decryption capabilities to the Saudi Ministry of Defence as part of a programme called SIGINT.[12] Other leaked memos showed the NSA handing over bulk intercepted communication to the Israeli government, and cooperating with the Jordanian government and the Palestinian Authority to provide "vital spying service regarding Palestinian targets."[13] Jordan, Saudi Arabia, Tunisia and the UAE were all recipients of funds for their surveillance services according to the leaked "2013 Foreign Partner Review".[14]

Surveillance import/export

On the maps developed by the Citizen Lab of surveillance, filtering and censorship software, many Arab countries were highlighted. The research group produced maps depicting the proliferation of products from companies that pride themselves with producing tracking and blocking software such as Blue Coat, FinFisher and Hacking Team.

Blue Coat appliances were found on many Arab government networks in 2013. The filtering and SSL inspection appliance Blue Coat Proxy SG was found on the government networks of Egypt, Kuwait, Qatar, Saudi Arabia, Sudan and the UAE. PacketShaper, an appliance that controls traffic based on URL categories, was found on the networks of the governments of Bahrain, Iraq, Kenya, Kuwait, Lebanon, Qatar and Saudi Arabia.[15]

In another test by the Citizen Lab in 2013,[16] Qatar, Bahrain and the UAE were also detected to have the FinFisher remote intrusion and surveillance appliance known as FinSpy. Developed by Gamma International, the software was found on the servers operated by the government-owned Batelco ADSL service in Bahrain

11 Campbell, D. (2014, 2 June). Revealed: GCHQ's Beyond Top Secret Middle Eastern Internet Spy Base. *The Register*. www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base

12 Greenwald, G., & Hussain, M. (2014, 25 July). The NSA's New Partner in Spying: Saudi Arabia's Brutal State Police. *The Intercept*. https://firstlook.org/theintercept/2014/07/25/nsas-new-partner-spying-saudi-arabias-brutal-state-police/

13 Cameron, D. (2014, 4 August). Snowden leak reveals close relationship between NSA and Israel. *The Daily Dot*. www.dailydot.com/politics/nsa-us-israel-gaza

14 Greenwald, G.(2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*.

15 The Citizen Lab. (2013, 15 January). Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. *The Citizen Lab*. https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools

16 Marczak, B. et al. (2013, 13 March). You Only Click Twice: FinFisher's Global Proliferation. *The Citizen Lab* https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2

and the government-owned Qtel in Qatar. In their 2015 test[17] the Citizen Lab detected FinFisher equipment in Oman, Morocco, Saudi Arabia, Jordan and Egypt. However, they were only able to confirm its operation by the Technology Research Department in Egypt, the Conseil Superieur De La Defense Nationale in Morocco, and the General Directorate of General Security and Internal Security Forces (ISF) of Lebanon.

In July 2015 thousands of employee emails from the Italian surveillance company Hacking Team were leaked. Those emails reflected different levels of communications between the company and intelligence or government agencies in countries including Morocco, Lebanon, Bahrain, Oman, Saudi Arabia, the UAE, Sudan and Jordan. An investigation by Privacy International published in March 2016 revealed that in addition to the Hacking Team software, the Egyptian Technology Research Department had acquired programmes from Nokia Siemens Networks to spy on Egyptian dissidents.[18]

THE RIGHT TO FREEDOM OF EXPRESSION

Speech "red lines" exist in most Arab countries. In general, citizens and media professionals face the threat of persecution if they speak against ruling regimes, the military, religions protected in the constitution, and, in some countries like Jordan, the rulers in neighbouring Gulf nations. The limitations of speech are loosely codified in the legislative framework of the country and selectively stretched and tightened by the authorities.[19] Journalists, bloggers and citizens are held in prison for crossing what is deemed a "red line".

In April 2015 in Jordan, journalist Jamal Ayoub was charged with "disrupting relations with a foreign country" after writing an article criticising the Saudi-led war in Yemen. In Egypt, journalists of Al Jazeera were charged with "aiding a terrorist organisation" for covering Rabaa's crackdown in 2013.[20] In November 2015 in Saudi Arabia, poet Ashraf Fayyad was given a death sentence for "questioning the Divine itself" in his 2013 poetry collection *Instructions Within.*[21] In the UAE, blogger Osama Al Najar was sentenced to three years in prison in 2014 for "instigating hatred against the state" after opposing, on Twitter, the "UAE 94", through which 94 people were given life sentences for allegedly overthrowing the UAE regime. Amongst them was Osama's father, who is serving 11 years in prison.[22] Even speaking against the outcomes of elections can be a crime. In April 2015 in Sudan, 20 students were arrested for speaking against the presidential elections that eventually reinstalled the previous regime of Omar al Bashir.[23]

Participation in the US-led coalition against ISIS and the Saudi-led coalition against Yemen, and the rise of terrorist acts in Egypt, Tunis and Libya, were opportunities for regimes to spread nationalistic sentiments that promise security in exchange for freedoms. These sentiments strengthened the state's authority to impose a ban on publishing certain kinds of news unless a permit was granted by the state. Two websites were blocked instantly in Jordan after publishing news broadcast by ISIS on the abducted Jordanian pilot in early 2015.[24] Directly following this incident, a series of publishing bans were announced with regard to news involving ISIS, the military and public security. In Morocco, journalist Ali Anouzla was jailed for "glorifying terrorism" in 2013 after posting an article that contained a video from Al Qaeda that was published first by the Spanish daily *El Pais*.[25]

These cases are only a sample of the continuous arrests and detentions of citizens for speech that has always existed but intensified with the spread of the internet. However, for states to control a decentralised publishing environment, these detentions, intimidation techniques and "friendly threats" from the intelligence depart-

17 Marczak, B. et al. (2015, 15 October). Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. *The Citizen Lab*. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

18 Privacy International. (2016). *The President's Men? Inside the Technical Research Department*. https://t.co/UmUsUskQfQ

19 Social Media Exhange. (2014, 17 October). Op. cit.

20 BBC. (2015, 13 February). Who are the al-Jazeera journalists tried in Egypt? *BBC*. www.bbc.com/news/world-middle-east-27943387

21 Whitaker, B. (2015, 20 November). Poet 'sentenced to death' in Saudi Arabia. *Al-Bab.com*. www.al-bab.com/blog/2015/november/poet-death-sentence.htm

22 Reporters Without Borders. (2014, 24 March). Netizen arrested. *Reporters Without Borders*. en.rsf.org/united-arab-emirates-netizen-arrested-after-tweeting-24-03-2014,46036.html

23 African Centre for Justice and Peace Studies. (2015, 17 April). Sudan's Electoral Period Marred by Arrests and Incommunicado Detention; Insecurity in Darfur. www.acjps.org/sudans-electoral-period-marred-by-arrests-and-incommunicado-detention-insecurity-in-darfur

24 www.7iber.com/politics-economics/media-coverage-of-war-isis-and-yemen

25 Reporters Without Borders. (2016, 21 January). Drop All Charges Against Moroccan Journalist Ali Anouzla – Let Him Go Free, Once and For All. en.rsf.org/morocco-drop-all-charges-against-moroccan-21-01-2016,48755.html

ments are no longer affordable or effective, and require a pre-publishing filter. Arab states are starting to place structural restrictions on digital publishing platforms by proposing laws that extend their existing grip on print to online publications. In Jordan, the Press and Publication Law was amended in 2012 to state that news websites shall be blocked unless they obtain a licence to publish from the Media Commission. The law loosely defines an "online publication" that requires licensing as any website with a fixed URL that engages in publishing news, investigations, articles or comments related to Jordan's internal or external affairs.[26] As a result, 300 websites were blocked in 2013. Egypt is following suit by not only proposing a licence to publish, but also requiring the website to be registered as a shareholder company with capital of no less than half a million Egyptian pounds.[27] These actions allow states to filter content by restricting the pool of citizens who can legally start a publishing platform.

The number of arrested journalists or citizens is not a solid indicator of the extent to which censorship exists. Self-censorship is common, and in many countries journalists are known to be taking a risk when discussing certain topics. The concentration of state-owned or state-aligned online media by default also censors the non-mainstream.

THE RIGHT TO FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

The year 2011 was the year when thousands took to the streets to protest dictatorial regimes in the Arab region. Series of protests were contagious, demanding the fall of these regimes, and calling for economic, political and social reforms. Authoritarian regimes that reappeared in different shapes and forms after the Arab Spring used the chaos and instability following these demonstrations to clamp down on the right to freedom of peaceful assembly in the name of security.

Violating the right to freedom of assembly is common across many Arab regimes. In Saudi Arabia many activists were imprisoned for demonstrating, including Abdul Karim Al-Khodr, who in October 2015 was sentenced to 10 years in prison for "instigating chaos through the organisation of protest and demonstration."[28] In Bahrain, Abdulhadi al-Khawaja, who is among 13 high-profile leaders of peaceful protests, is serving a life sentence for participating in the 2011 demonstrations.[29] In Sudan, in addition to detention and brutal response to protests, the authorities closed down offices of civil society organisations like that of Salmmah Women's Resource Centre in June 2014.[30] In Oman, following the 2011 protests, authorities arrested a total of 216 people "on charges of assembly, assaulting public and private facilities," which were later pardoned in 2013.[31]

In some countries, violation of the right to assembly is not as brutal and consistent as opening fire on protesters or their mass detention. In Lebanon, while the right of assembly is generally unrestricted, dozens of activists were arrested while protesting in the 2015 #YouStink campaign, including its key organisers.[32]

The internet has served as an essential tool to facilitate the mobilisation of the masses and organisation of demonstrations. Therefore, internet disconnections and blocking of websites are also used to restrict the right to peaceful assembly. During protests, many governments in the region, including those of Egypt,[33] Libya[34] and Sudan,[35] have blocked or slowed down access to the internet, mobile networks and particular social networking sites. Governments have also starting targeting administrators of Facebook pages that call for action

26 7iber. (2013, 16 October). Blog Action Day 2013: How Jordan's Press Law Violates Human Rights. 7iber.com/2013/10/blog-action-day-2013-how-jordans-press-law-violates-human-rights

27 Hamama, M. (2015, 4 November). Op. cit.

28 Gulf Centre for Human Rights. (2015, 22 October). Saudi human rights advocate Abdulkarim Al-Khodr sentenced to 10 years in prison. *IFEX*. https://www.ifex.org/saudi_arabia/2015/10/22/sentenced_to_10_years/

29 Human Rights Watch. (2014, 21 January). Bahrain: Prospects of Reform Remain Dim. https://www.hrw.org/news/2014/01/21/bahrain-prospects-reform-remain-dim

30 Human Rights Watch. (2015). *World Report 2015: Sudan*. https://www.hrw.org/world-report/2015/country-chapters/sudan

31 Human Rights Watch. (2015, 23 March). Oman: UPR Submission March 2015. https://www.hrw.org/news/2015/03/23/oman-upr-submission-march-2015

32 Daily Star. (2015, 17 September). At least 20 injured, 38 detained during anti-government rallies in Beirut. *AlBawaba*. www.albawaba.com/news/least-20-injured-38-detained-during-anti-government-rallies-beirut-744956

33 Hassanin, L. (2011). Egypt's 25 January Revolution: The role of the internet and mobile technology in social resistance and public demonstrations. In Finlay, A. (Ed.), *Global Information Society Watch 2011: Internet rights and democratisation*. https://www.giswatch.org/en/country-report/civil-society-participation/egypt-0

34 Dyn Research. (2011, 18 February). Libyan Disconnect. research.dyn.com/2011/02/libyan-disconnect-1/#latest

35 Dyn Research. (2013, 25 September). Internet Blackout in Sudan. research.dyn.com/2013/09/internet-blackout-sudan

or highlight human rights abuses. For example, in December 2015, the administrator of the Facebook page "The Revolution of the Poor" was arrested in Egypt and charged with "instigating violence against national institutions like state institutions and police, promotion of the Muslim Brotherhood organisation's ideas, calling for demonstrations and bringing chaos."[36]

After the 2011 revolutions, governments found golden opportunities to inject legal restrictions on freedoms in the name of security amidst the rise of sentiments fearing terrorism. Anti-terrorism laws regulating the state's responses to acts of terrorism loosely expanded the definition of "terror acts" to causing disorder, disrupting public life, causing harm to the environment, facilities, public and private property, or disabling the application of the constitution, laws or regulations. In the past three years, many anti-terror laws passed across Arab countries have not only led to the detention of protesters for "disrupting the public order", but also of those who visit or share online content deemed "terrorist", as in Saudi Arabia,[37] Egypt,[38] Jordan[39] and Tunisia.[40] In Egypt and Jordan, anti-terror laws have given the public prosecutor the right to surveil suspected "terrorists". Most amended anti-terror laws are not in compliance with the recommendations of the UN Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism.[41] None of these laws provide safeguards of "independent prior authorization and subsequent independent review" (article 45). Following the passing of the amendment of the assembly law, many activists and citizens in Egypt were sentenced to five years in prison under the charge of "illegal assemblies"; among these were nine women detained in June 2014 for protesting the assembly law itself.[42]

36 www.almasryalyoum.com/news/details/852484

37 Human Rights Watch. (2014, 20 March). Saudi Arabia: New Terrorism Regulations Assault Rights. https://www.hrw.org/news/2014/03/20/saudi-arabia-new-terrorism-regulations-assault-rights

38 Mada Masr. (2015, 20 August). In first application of terrorism law, alleged terror cell members arrested. *Mada Masr*. www.madamasr.com/news/first-application-terrorism-law-alleged-terror-cell-members-arrested

39 www.7iber.com/2015/07/charges-under-anti-terrorism-law-jordan/

40 Samti, F. (2015, 18 August). Tunisia's New Anti-Terrorism Law Worries Activists. *Foreign Policy*. foreignpolicy.com/2015/08/18/tunisias-new-anti-terrorism-law-worries-activists-tunisia

41 United Nations General Assembly. (2014, 23 September). Op. cit.

42 Human Rights Watch. (2013, 26 November). Egypt: Deeply Restrictive New Assembly Law. https://www.hrw.org/news/2013/11/26/egypt-deeply-restrictive-new-assembly-law

CASE STUDY I: MOROCCO

The Moroccan constitution covers the right to privacy. Article 24 states: "Everyone has the right to privacy. The home shall be inviolable. Searches can be carried out only in such conditions and forms as provided by the law. Private communications, in whatever form, shall remain secret. It is prohibited to request permission to view or publish [private] content, whether in part or as a whole, or use it against anyone, except through a court order and in accordance with the conditions and processes of the law."[43] The Anti-Terrorism Law (amended in 2014) requires the Public Prosecutor to request the permission of the head of the Court of Cassation[44] to issue an order to record, copy and confiscate any communications if the alleged crime "threatens national security, or is connected to terrorism crimes, or criminal gangs, or death or poisoning, kidnapping and hostage-taking, or counterfeiting or forgery of public money or loan bonds, or drugs or psychotropic substances, or weapons, ammunition and explosives" (Article 102).[45]

The same law allows the government to filter and delete content that is deemed to "disrupt public order by intimidation, force, violence, fear or terror." Intermediaries must block or delete infringing content when made aware of it or upon receipt of a court order. This grants internet service providers (ISPs) an executive authority to determine what constitutes violence, fear and terror, and restricts the citizen's right to appeal.

It is important here to understand the ownership of the internet infrastructure in Morocco when estimating the centrality of surveillance systems and the role of ISPs. The previously state-owned Maroc Telecom owns and controls a fibre optic backbone of more than 10,000 kilometres covering the whole country. Even after its privatisation, the Moroccan government still owns 30% of the company. The national railway company, Office Nationale des Chemins de Fer (ONCF), and the national electricity and water utility, Office National de l'Electricité et de l'Eau Potable (ONEE), have also built 2,000 kilometres and 4,000 kilometres of fibre optic infrastructures, respectively.[46]

Reality of digital security

In global debates on the import/export movement of surveillance tools, many fingers were pointing at Morocco as a destination. Tests led by the interdisciplinary technical group the Citizen Lab revealed that the country has been hosting servers using the appliances of Hacking Team and FinFisher. The Moroccan government activated these tools after the threat of the so-called "February 20 movement", which aimed to hold protests in Morocco in 2012, a year after the regimes of Tunisia and Egypt stepped down responding to mass protests. The Citizen Lab tests revealed that Hacking Team appliances were first used in May 2012 and were still active at the time of the test in 2014. The results confirmed a story verified by Citizen Lab earlier in the same year of a government-sponsored malware targeting the editors of Mamfakinsh, an independent citizen media platform covering the protests at that time.

According to the Privacy International report *Their Eyes on Us*, the citizen media platform Mamfakinsh was launched to provide a different narrative of the February 20 activists' movement from that propagated by state-controlled media outlets. As activists took to the streets every weekend following February 20, Mamfakinsh was continuously capturing videos and photos documenting the protests and finding ways to narrate a different story from that in the mainstream media.[47]

When they were heavily covering the protests, the Mamfakinsh website was getting distributed denial of service (DDoS) attacks as the website's unique visitors got up to one million, according to the co-founder, Hisham Almiraat. These attacks became occasional throughout the year. When the protest movement began to decline after a few months, so did the coverage. However, the editors of Mamfakinsh were still a threat to someone.

43 www.ism.ma/basic/web/ARABE/Textesdeloiarabe/DocConst.pdf

44 The Court of Cassation replaced the Supreme Council. It was established by Act No. 58/11, promulgated under Royal Decree 1.11.170 of 25 October 2011, amending Royal Decree No. 1.57.223 of 27 September 1967 on the Supreme Council. It is composed of a first president, chambers, the prosecutor-general, assistant prosecutors and the clerk of the court. For more information: www.nyulawglobal.org/globalex/Morocco1.html

45 www.assabah.press.ma/index.php?option=com_content&view=article&id=4671:2011-01-26-16-15-20&catid=115:2010-11-19-14-26-07&Itemid=800

46 Freedom House. (2015). Freedom on the Net: Morocco. https://freedomhouse.org/report/freedom-net/2015/morocco

47 Blum-Dumontet, E. (2015, 10 July). Facing the Truth: Hacking Team leak confirms Moroccan government use of spyware. *Privacy International*. https://www.privacyinternational.org/node/622

In July 2012, the email account dedicated to receiving contributions on Mamfakinsh received an email message with the subject "Dénonciation" (denunciation), with an attachment titled "scandale.doc", and a message asking the recipients to maintain the secrecy of the sender's identity. Seven of the 15 editors who received the email opened it and downloaded the attachment. After soon realising that the email was a malware, they forwarded it for forensic testing by the Citizen Lab, which traced the origin of the spyware to the Remote Control System (RCS) software produced by the Italian company Hacking Team. RCS malware allows open access to someone's computer, making it possible to steal files, read emails, take photos, trace internet navigation activities, record passwords and remotely turn on the device's camera and microphone.

According to the Citizen Lab, the exploit was packaged by Hacking Team based on the requirements of the attacker. This exploit document "downloads a second stage containing shellcode that then downloads and installs a third stage implant."[48]

While the origin of the attackers was not identified by the Citizen Lab at first, the later scan testing of RCS servers conducted by the same group revealed that Morocco's Maroc Telecom, in which the government owns 30% of shares, was an end point server to three other RCS proxy servers in Kiev and Tampa at the time of the testing in 2014.

While the Mamfakinsh exploit in 2012 was the only publicly reported evidence of the use of the Hacking Team RCS, first-person accounts of surveillance shared by other Moroccan journalists were documented in the Privacy International report *Their Eyes on Us*, published in April 2015.[49] Journalist Ali Anouzla, for instance, reported incidents where he believed that phone tapping was the only way information about his private life, meetings and conferences could have been leaked to the press.

Morocco in maps and leaks

The Moroccan intelligence agencies spent around three million pounds on acquiring and maintaining their surveillance system, as per the 6 July 2015 leaks of Hacking Team emails. These emails document correspondence between Hacking Team employees and government or intelligence department officials, including Moroccan government officials. Confirming the test results of the Citizen Lab's findings, they revealed that the Moroccan High Council for National Defence (Conseil Supérieur de la Défense Nationale or CSDN) acquired the software in 2009, and the Directory of Territorial Surveillance (DST) in 2012. In 2015, the CSDN and DST spent EUR 140,000 and EUR 80,000 for spyware that can reach up to 300 and 2,000 targeted devices respectively.[50] The Moroccan Gendarmerie[51] was listed as an "opportunity" for Hacking Team's 2015 strategy with an expected revenue of EUR 487,000. The emails also revealed that the UAE-based Al Fahed Smart System is a usual intermediary between governments and the company.[52]

Morocco was also one of the countries in which the Citizen Lab found traces of FinFisher appliances in their 2015 update test. It was among those countries where the group was able to verify the location of the server: the CSDN.[53]

The Moroccan government did not respond officially to any of these allegations. However, in September 2015, after the publication of the Privacy International report *Their Eyes on Me*, the government filed a lawsuit against Hisham Almiraat, who participated in the report. He was charged with "threatening the internal security of the state." At the time of writing this paper, Almiraat's trial was adjourned until March 2016.[54]

48 Marczak, B. et al. (2014, 17 February). Mapping Hacking Team's "Untraceable" Spyware. *The Citizen Lab*. https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/#2

49 Blum-Dumontet, E. (2015, 10 July). Op. cit.

50 Ibid.

51 www.fiep.org/member-forces/moroccan-royal-gendarmerie

52 Currier, C., & Marquis-Boire, M. (2015, 7 July). A Detailed Look at Hacking Team's Emails About Its Repressive Clients. *The Intercept*. https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries

53 Marczak, B. et al. (2015, 15 October). Op. cit.

54 Free Press Unlimited. (2015, 18 November). These seven Moroccan human rights defenders are on trial. https://www.freepressunlimited.org/en/news/these-seven-moroccan-human-rights-defenders-are-on-trial

CASE STUDY 2: OCCUPIED PALESTINE

Surveillance has been one of the most integral tools to perpetuate the Israeli occupation of Palestine, and also to maintain the status quo of the Palestinian Authority (PA). It is a multifaceted complex structural system that starts with the layout of the telecommunication infrastructure in the West Bank and Gaza, to the Israeli military-academic-private security establishment of a surveillance industry, ending with cross-collaboration of the Israeli intelligence agency with the NSA and the PA.

Telecommunication infrastructure

The Oslo Accords of 1995 gave the Palestinians the authority to operate their own telephone, radio and TV networks, but assigned the allocation of frequency and infrastructure to a joint committee with the Israeli authorities. In 2014, the International Telecommunication Union (ITU) passed a resolution urging member states to take every effort in "facilitating the establishment of Palestine's own international gateway networks, including satellite earth stations, submarine cables, optical fibres and microwave systems."[55] However, the Israeli occupation continues to determine the shape, form and scope of the Palestinian telecommunication industry. Until this date, Palestinian telecommunications providers are still unable to set their own communication standards or independently import certain equipment, as Israel controls the allocation of frequencies and determines the scoping and scaling of Palestinian infrastructure. Helga Tawil-Souri, an assistant professor of communication at New York University, sums up the "independence" best:

> The majority of Palestinian Internet traffic is routed through switches outside the Territories. Even on the ubiquitous cellular phones, calls must touch the Israeli backbone. Paltel, Jawwal, Hadara and Wataniya rely on Israeli permissions for the placement, number and strength of routers and exchanges; the range of their signals and the equipment they can use is limited by Israeli restrictions; the allocation of their bandwidth is decided by the Israeli Ministry of Communication – not the Palestinian one.[56]

It was not until November 2015 that the Israeli government allowed the establishment of a 3G mobile network in Palestine, at the time that Israel was moving to 4G. Moreover, Israel only allowed the implementation of a 3G network in the West Bank, but not in Gaza.

In the Gaza Strip, restrictions on the telecommunication infrastructure are further heightened. Any landline call from Gaza is routed through the Israeli telecommunication infrastructure. The allocation of bandwidth; the placement, number and strength of internet routers or telephone exchanges; the range of cellular signals and the equipment used; and decisions about which new technologies are permissible or not are all limited by Israeli restrictions.[57] The infrastructural Israeli military surveillance apparatus over the Palestinian telecommunication companies is reflected through the text messages and phone calls that Gazans used to receive from the Israeli occupation forces warning them of impending bombs. The only fibre optic cable to Gaza is placed in Israel, which gives Israel centralised surveillance and switching powers. This control is also manifested in how Paltel and whatever Israeli firm it is dealing with must coordinate their operations with the Israeli occupation forces and the Israeli Coordination and Liaison Administration to the Gaza Strip.

The mechanism of Israeli surveillance over telecommunications starts with the dependence of telecoms infrastructure. This routing centralisation grants greater unchecked powers to the Israeli government to monitor the communications of Palestinians, and therefore to perpetuate control over their lives.

Surveillance establishment: IDF-private sector-academia

On top of the physical infrastructural surveillance apparatus, there lies a security-based establishment tightly connecting the Israeli military, the Israeli version of the Silicon Valley, and Israeli academic institutes. The high tech spy incubator of the Israel Defence Forces (IDF), Unit 8200, can be a dream destination for a 16-year-old with good coding and hacking skills. However, to be eligible

55 International Telecommunication Union. (2014). Resolution 99, Status of Palestine in ITU, Final Acts of the Plenipotentiary Conference, Busan 2014. https://www.itu.int/en/plenipotentiary/2014/Documents/final-acts/pp14-final-acts-en.pdf

56 Tawil-Souri, H. (2011, 9 November). Hacking Palestine: A digital occupation. *Al Jazeera*. www.aljazeera.com/indepth/opinion/2011/11/201111715155960l957.html

57 Tawil-Souri, H. (2014, 29 September). The Technological End Between the 'Inside' of Gaza and the 'Outside' of Gaza. *7iber*. www.7iber.com/2014/09/the-technological-end-between-the-inside-of-gaza-and-the-outside-of-gaza

for Unit 8200 recruitment, students need to graduate from Magshimim, a three-year school, partly funded by the IDF. In Magshamim students get to experiment with building surveillance gadgets and spying technology that the IDF may use in their military operations.

An inaccessible space, Unit 8200 is where most of the IDF spying activities take place. It is the equivalent of the NSA in the US or the UK's GCHQ. When in September 2014, 43 Israeli Unit 8200 veterans signed a public letter refusing to participate in its intrusive spying tactics against Palestinians, they were dismissed by the IDF.[58] The veterans alleged that the Unit gathers information on innocent Palestinians to suppress political dissent and create strife between different factions. Among this collected information were damaging details of Palestinians' lives they came across, including information on sexual preferences, infidelities, financial problems or family illnesses that could be "used to extort/blackmail the person and turn them into a collaborator." One veteran reported that during his training for Unit 8200 he was assigned to memorise different Arabic words for "gay".[59]

While the market demand for surveillance equipment is high in Israel, so is the supply. Israel is one of the biggest manufacturers of surveillance products in the world. In Gaza alone, the IDF uses unmanned aerial drones, closed-circuit TV cameras, sonic imagery, gamma detection machines, remote-controlled bulldozers and boats, black lights, unmanned miniature robots, electrified fences, electro-optic systems for night vision, aerostat balloons with 360-degree observation coverage, vibration sensors, among others, to control and surveil.[60] The Israeli company Elbit, managed by the IDF, is one of the largest defence arsenal suppliers in the world and the main supplier for the IDF surveillance and defence apparatus, reaching a revenue of USD 764.8 million in the third quarter of 2014 alone.[61] Israel is also one of the world's biggest exporters of surveillance equipment. In 2014, Elbit supplied the US Department of Homeland Security with a tower, erected with high-powered surveillance cameras, over the Mexican border in Nogales, Arizona. Elbit operates that tower as well. A 2015 report from Privacy International revealed that the two multinational Israeli-based companies Virent and NICE Systems were supplying surveillance systems to Colombia,[62] while the Israeli firm BlueBird Aero Systems sold drones to the Chilean army to surveil the territory of the Mapuche indigenous people in 2013.[63] In 2015 alone, Israel's cyber-security sales totalled around USD 4 billion, attracting 20% of the global private sector investment in the same industry.[64]

The close relationship between the Israeli military and the private surveillance sector is also infused by the mutual movement of intelligence specialists across both sectors. Investigating the intrusive ad injection industry, a report revealed that Superfish, a company that produces ad injectors, and Komodia, which creates encryption-breaking technology, were both owned by former Unit 8200 employees.[65]

Surveilling the web

The Snowden revelations reported a memorandum of understanding (MOU) signed between the NSA and the Israeli Sigint National Unit (ISNU) to formalise their intelligence sharing activities. The MOU establishes the sharing of collected raw data including "unevaluated and unminimized transcripts, gists, facsimiles, telex, voice and Digital Network Intelligence metadata and content."[66] The MOU attempts to safeguard the right to privacy of US nationals, but states that shared data includes collected operations against a particular foreign intelligence target.

58 Beaumont, P. (2014, 12 September). Israeli intelligence veterans refuse to serve in Palestinian territories. *The Guardian*. www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories

59 Reed, J. (2015, 10 July). Unit 8200: Israel's cyber spy agency. *Financial Times*. www.ft.com/intl/cms/s/2/69f150da-25b8-11e5-bd83-71cb60e8f08c.html

60 Tawil-Souri, H. (2014, 29 September). Op. cit.

61 Globes. (2015, 11 November). Elbit Systems third quarter profit up 50%. *Globes*. www.globes.co.il/en/article-elbit-systems-third-quarter-profit-up-50-1001080146

62 Privacy International. (2015, 2 September). New investigation reveals Colombia's spy equipment suppliers. https://www.privacyinternational.org/node/640

63 Derechos Digitales. (2013, 3 December). Is it a bird? Is it Superman? No, it is a "drone"! Surveillance and new technologies in Araucanía. https://www.derechosdigitales.org/6883/bird-superman-drone-surveillance-new-technologies-araucania

64 Reed, J. (2016, 12 January). Israel cyber-security expertise lures growing share of investment. *Financial Times*. www.ft.com/intl/cms/s/0/dfa5c916-b90e-11e5-b151-8e15c9a029fb.html

65 Fox-Brewster, T. (2015, 9 June). These Ex-Israeli Surveillance Agents Hijack Your Browser To Profit From Ads. *Forbes*. www.forbes.com/sites/thomasbrewster/2015/06/09/from-israel-unit-8200-to-ad-men

66 Greenwald, G., Poitras, L., & MacAskill, E. (2013, 11 September). NSA shares raw intelligence including Americans' data with Israel. *The Guardian*. www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents

In addition to using equipment to collect information on Palestinians, so as to control and monitor their movement to perpetuate occupation, the IDF is profiling Palestinian users on social media websites. The IDF contracts commercial social media monitoring companies to monitor the mass posts of Palestinians. Among the information that these companies provide are Arabic posts on protests or conversations that include trigger words like "boycott", "demonstration" or "AlQuds" (Jerusalem in Arabic) across social media websites and tools. The techniques that the company uses include creating fictitious profiles to circumvent privacy mechanisms and to be able to access private posts. Companies provide a combination of raw data and analysis of how profiles "feel" regarding the state or different Israeli bodies.

While it starts with profiling Palestinians, it then moves into incriminating them for things that they have shared or said on different platforms such as Facebook, Twitter and WhatsApp. In May 2015, Palestinian Omar Shalbi received nine months in prison under the charge of "inciting violence" for writing "resist the occupation" in many of his Facebook status updates.[67] Sami D'ias was sentenced to nine months in prison for the same charge for publishing the logo of the Popular Front for the Liberation of Palestine. "Inciting violence and terrorism" was the charge in November 2015 against Anas Al Khatib for publishing posts that included phrases such as "long live the Intifada" and "Jerusalem is Arab".[68] These are only a few of an unending list of cases, especially after the Israeli public prosecutor's announcement to actively detain Palestinians for incitement in May 2015. These cases are prosecuted selectively; despite reports on the rise of internet incitement against Arabs in Israel, not a single perpetrator has been subjected to criminal charges.[69]

67 http://v.gd/q8CYJi

68 www.raialyoum.com/?p=349302

69 Edelman, O. (2015, 13 October). Internet Incitement Against Arabs in Israel on the Rise. *Haaretz*. www.haaretz.com/israel-news/.premium-1.679990www.haaretz.com/israel-news/.premium-1.679990

DIGITAL SECURITY AND HUMAN RIGHTS NEEDS

After the Snowden revelations, digital security was a main priority in any discussion revolving around the future of the internet. The themes of most conferences addressing technology and public policy shifted towards the violations and the ethical human rights responsibilities of all stakeholders, starting with those involved in building the communications technical infrastructure, to the legislative landscape. This is not to say, however, that "digital security" is taking the same precedence over the priorities of users or civil society in the region, or elsewhere.

The Snowden revelations marked a phase where companies and developers introduced applications promising "secure", "private", "encrypted" communication as their edge. For example, by the end of 2013, dozens of mobile chat applications gained more attention, including ChatSecure, Surespot, RedPhone, Silent Phone, Silent Text, Telegram and Signal. New social media websites with different business models also surfaced, promising higher security and better data collection transparency and user privacy policies. Security experts – including Jacob Applebaum and Edward Snowden – all united in recommending the use of PGP encryption and Off The Record (OTR) to communicate safely and securely away from the radars of surveillance machines run by governments.

Media coverage heightened the debate. There were constant reports of privacy loopholes and surveillance backdoors in protocols, communication devices, applications and software. Research groups tracked the import and export of surveillance software to assist governments to crack down on dissent, journalists and marginalised groups. A large number of these governments are in the Middle East, spending big budgets on software from companies like FinFisher, Hacking Team, BlueCoat and Netsweeper.

Consequently, this phase also marked the intensification of a wave of digital security training and workshops with the aim to address the security needs of human rights activists, journalists and NGOs. While many started years ahead of Snowden's revelations, international human rights organisations began to actively compile manuals and guidelines targeting people at risk. These include, to name a few, the Digital First Aid Toolkit,[70] the APC Digital Security First Aid Toolkit for Human Rights Defenders,[71] Security in a Box,[72] Journalist Security Guide,[73] and Online Survival Kit.[74] While many of these manuals addressed a general audience, some were more specialised, aiming to target the needs of certain groups like LGBTQ communities in the Middle East.

Digital security movements in the Arab region

News about government surveillance of activists was not new in the Arab region. The unfolding Arab spring demonstrations in 2011 revealed evidence of the use of surveillance equipment and apparatus to crack down on opposition movements and groups demanding democratic reforms. For example, after revolutions erupted in 2011, many reports highlighted government-sponsored "spearfishing", soliciting account information of activists in countries like Bahrain and Syria. In Egypt, the day activists ransacked the State Security Headquarters after the fall of Hosni Mubarak in 2011, they found a contract between the Egyptian government and Gamma International to run FinFisher software, dating back to 2009. Local and regional media covered such events, and activists and civil society called for governments to be held responsible for the violations of constitutional rights.

Given the turmoil that followed 2011, advocacy to hold governments accountable for their human rights violations took a backseat. The Snowden reports expanded information on Arab governments' and intelligence departments' use of surveillance software and cooperation with other secret intelligence programmes. However, the lack of access to information limited Arab media to merely echoing what international media and research centres revealed without digging deeper into the extent of these violations and the details of the technical capacities of the state.

Training programmes directed at journalists, human rights defenders, NGOs and activist groups flourished in the region. The aim was to help activists in dangerous

70 https://digitaldefenders.org/digitalfirstaid

71 https://www.apc.org/en/pubs/digital-security-first-aid-kit-human-rights-defend

72 https://securityinabox.org/en

73 https://cpj.org/reports/2012/04/technology-security.php#3

74 wefightcensorship.org/online-survival-kithtml.html

and undemocratic zones secure their communications devices, and assess the risks of their data sharing and communication behaviours in the light of the powerful state-led programmes infringing on citizens' rights, including the right to privacy.

The Arab region should not be treated as one entity despite the commonalities between systems of governance and violations of human rights. Therefore, for the purpose of assessing digital security trainings and workshops and how effectively they respond to human rights needs in the region, the author chose Morocco and Occupied Palestine as case studies. In these two countries, the literature about state surveillance and how it translates in reality is the most available, thanks to the revelations of state-sponsored hacking attempts and persecution of activists for their private messages. We interviewed four digital security trainers and activists in the region, two residing in Palestine, one in Morocco and one in Egypt, to address the following main questions:

- How do you adapt the digital security programmes you provide to the internet's political and infrastructural realities in the countries where you lead these workshops?
- In your opinion, what is the role of the digital security manuals produced by international and regional organisations? What are their points of relevance to and departure from the digital security needs of the local context?

We believe that the perspective of the digital security trainers on these questions gives a better understanding of the contextual approach in addressing digital security needs, not only in the Arab region, but also around the world. They confirm that just as in physical security, digital security is a practice that should respond to the local legislative framework protecting human rights, and the reality of the threats that activists, journalists and marginalised groups face. In the following section, we will address each of these questions individually.

CONTEXTUALISING DIGITAL SECURITY CONSULTATION

The preceding overview of the most commonly violated human rights across the Arab countries confirms similarities of state mentalities to restrict freedoms. However, it also confirms the differences in tools that states use to violate the rights to free speech, assembly and privacy. While some states resort to the legislative framework to encode the legality of these violations by passing restrictive laws, others use the internet infrastructure, and some do both. In some examples, states violate human rights through arbitrary means without having to find the legal cover, as in the confiscation of devices or internet cut requests (for example, Egypt in 2011). Here we provide an overview of how digital security trainers incorporate the local realities of surveillance in their digital security consultation, mentorship or advice to different target groups. We categorised three variables according to which they design their digital security advice: (1) the country's legislative framework, (2) the internet infrastructure, and (3) communication behaviours.

We interviewed Rabeh and Haleem,[75] two digital security trainers from Egypt and Palestine, who have been engaged in various digital security trainings and consultancies for individuals and organisations around the region. These trainers were able to give their perspectives on the extent to which these trainings and tools correspond with the local legislation and local environment. The other two interviewees, Alaa and Nabeel, are both recipients of digital security trainings and advocates of digital security practices within their organisations. Alaa is a co-founder of a newly established media institute based in Morocco and a journalist. Nabeel is a co-founder of an institution that supports civil activism and mobilisation by Palestinians.

Legislative frameworks and surveillance realities

For Rabeh, Haleem and Nabeel it is important to understand the legislative realities and surveillance practices of the country before offering advice on digital security. In a country like Egypt, where any form of encryption is prohibited without a permit, Rabeh has to make a choice between visible and not-so-visible encryption, "especially, when there is a risk of devices being inspected by the airport authorities." Also, for Rabeh, if the government uses non-conventional tools to surveil, "activists have to be careful about their choices with tools promising secure communications, especially on their mobile. I try not to recommend Orbot web or ChatSecure, as they may produce suspicious traffic."

In Israel, private companies incorporating encryption in the software that they produce have to apply for a licence at the Ministry of Defence. According to the Control of Commodities and Service Law (1957), companies must submit an application including details of the prod-

75 For security purposes, this paper is using pseudonyms for interviewees.

uct and its encryption interface to get a licence. Special licences should be requested if companies are exporting their products to the Palestinian Authority.[76] This legislative framework grants the Israeli authorities unsupervised and non-transparent access to software sold to the PA. This reality is important for Haleem. When encryption is illegal or state-accessed, he provides advice on secure communication behaviours rather than encrypted tools and synchronous communication.

The upsurge in detention by Israeli authorities of Palestinians criticising the Israeli occupation has led Nabeel's organisation to incorporate this knowledge into their workshops about social media as a tool for civic mobilisation. "We integrated a small segment on basic concepts of privacy that groups should consider when using platforms such as Facebook. We developed a video that guides activists to the privacy features on Facebook to protect themselves from Israeli legal persecution." In their programme, Nabeel's organisation does not suggest certain tools for digital protection as they do not have enough technical knowledge of the available tools, their capacities and limitations. "Our advice is based on Facebook behaviours rather than tools," says Nabeel.

For Alaa, security was at the heart of their organisation strategy from the very beginning. The fact that their business model is subscription-based makes it very important to build a strong wall around their platform that will protect their clients' information and their content. The realities of the persecution of Moroccan citizens – for their Facebook posts, or activism in digital security – and facts about the software the government uses for surveillance have led them to develop a digital security guidebook for journalists to secure their practices in the field. However, these guidelines are flexible, depending on the sensitivity of the topic that they cover: "Journalists have to communicate their data through secure means if they are covering militants, for example," says Alaa.

Internet infrastructure

Studying the layout of the internet and landline infrastructure in the country where training is taking place is essential in planning the digital security consultation. For the digital security trainers that we interviewed, it is important to first know the international connections from which the country takes its internet, the different internet connection types prominent in the country, the variance in internet speed, and finally the extent to which the ownership of the internet backbone is centralised.

For Rabeh, you cannot just advise people to use Tor for secure navigation. It is essential to study the network speed that activists or organisations depend on, and provide a solution that will not hamper their communication. "The one-size-fits-all does not work, not only because of the political context but also the infrastructural one." For him, "the solutions that you apply on ADSL connections are different from those on 3G. Choosing between Tor and virtual private networks depends on the internet speed. Tor needs good speed!"

In Morocco, Maroc Telecom owns most of the internet backbone. This means that most internet traffic goes through this company that used to be government owned. After Maroc Telecom was privatised, the Moroccon government shares were reduced to 30%, which still gives it enough authority to access traffic on the network. This arrangement of the infrastructure gave the Moroccan intelligence department the power to host FinFisher servers on Maroc Telecom servers and infect groups like Mamfakinsh with malware to hack into their laptops. The fact that FinFisher is still running until this year means that the intelligence department has extraordinary powers to hack into activists' laptops. To test the extent to which the state is performing surveillance activities, the technical team at Alaa's organisation left one computer vulnerable. They later found a virus whose source was tracked to official entities. "We do not allow any journalists to use their personal laptops or phones in their investigations."

In Occupied Palestine, the arrangement of the internet infrastructure plays a big role in activists' understanding of what is realistically possible in achieving digital security. For one trainer, the understanding of infrastructure starts simply with the logistics of planning a workshop that addresses online organisation for civil movements. In Gaza, for example, the electricity cuts caused by Israel's stifling gas policies make it impossible to host a training or a workshop in a space that does not have generators. "Once you get that figured, then you start addressing the issues of digital security," says Nabeel.

For Haleem, it is very important to not only understand the layout of the infrastructure, but also explain the dependency of the Palestinian internet and phone network on the Israeli infrastructure in a digital security training. "Of course there is a baseline of digital security hygiene that is common in each country and should not be compromised," he noted. However, the consultancy that he

76 Waxman, M., & Hindin, D. (2015, 30 November). How Does Israel Regulate Encryption? *Lawfare*. https://www.lawfareblog.com/how-does-israel-regulate-encryption

provides depends on contextual risk assessment of any human rights group he works with.

For example, after evaluating the data storage risks that one NGO in Ramallah has, he suggested a multifold solution to ensure not only the virtual but the physical security of the data. This NGO documents the abuses of both the Palestinian Authority and Israeli occupation security forces, and sends this information to its Europe-based headquarters to use it as evidence in their international court trials against both authorities. Having only Israeli international connections feeding the internet in the West Bank means that the occupation state can monitor the internet lines without being subjected to legal accountability. Here you have to deal with the reality that any access to their documents will subject their sources and staff to arrests, which leads to the need for secure communication between the staff, sources and any external entity. The second layer of security comes from the history of the Israeli occupation forces in raiding NGO offices, confiscating computers, and blowing up data centres. It is essential in this case to suggest processes to securely, instantly and regularly move their data to their headquarters in Europe.

There are cases where NGOs use SMS as their main communication method. "We found out that their SMSs were moderated and filtered according to some words. In this situation, recommending a tool such as TextSecure[77] will draw attention to this group and make them under the spotlight." Instead of introducing new tools, Haleem suggested the use of manual agreed-upon encoded text while using the same medium to avoid persecution or more attention.

Communication behaviours and digital security

In order to lead users to adopt digitally secure communication practices, digital security advisers must not only assess the legislative and infrastructural context, but also communication practices. Most advisers we met with agree that understanding the context should go as local as understanding the NGO's communication processes, on top of the countries' legislative and infrastructural realities. Haleem mentions an example: "Some groups do not depend on emails for communication but Facebook messages." Therefore, for him, introducing email encryption as a tool for higher security is not useful in this situation.

Security advice should take into consideration the behaviours of activists and their assumptions on certain platforms. Rabeh mentions that many of the people he engaged with access the internet through public wireless rather than their home connections. "You can suggest all the secure applications in the world, but it won't matter if you are using them through a public network."

Haleem mentions another example where highlighting behaviours is more important than highlighting tools. Using a password manager to assist the good practice of creating separate passwords for different user accounts can still be a security threat if not followed by a change of different behaviours. Haleem asks, "So what if you use a tool like KeePass but still leave your laptop unlocked when you walk away from it? While you followed the good practice of not using a single password for all accounts, you gave easy access of all these passwords when you walked away from your computer."

For Alaa, his organisation is enforcing certain behaviours through technical limitations. For example, journalists are not allowed to use their personal email to communicate or their personal devices for their work. His organisation has also activated a local virtual private network (VPN) on which only work laptops can be registered. Setting up these systems for communications reduces insecure practices by design.

Beliefs around digital security and its impact on activism affect the adoption of secure practices. Raising awareness on digital security is a point of constant debate among Palestinian activists, according to Nabeel. Although many of these digital security tools were developed as an act of resistance by hacker movements, the dilemma for these activists is raising awareness on digital security risks without discouraging activism. If the tone used to address risks to privacy creates a sentiment of fear, it will discourage the use of tools for activism and limit the work space. "Some believe that they should treat the reality of occupation as it is, abusive and brutal, rather than try to follow techniques that will keep them out of trouble."

DIGITAL SECURITY HANDBOOKS: RELEVANT OR NOT?

Digital security advisers were asked about the relevancy of digital security guidebooks to the local human rights context in which they work. Haleem treats kits as references only: "I mix and match chapters from differ-

77 In November 2015, Open Whisper Systems replaced TextSecure and RedPhone with the messaging application Signal. This quote from Haleem refers to times when TextSecure still existed.

ent developed kits based on each needs assessment of the situation." Digital security is not about introducing tools, but practices. The following critiques on toolkits and guidebooks were common across the digital security advisers that we interviewed.

The need for context

All digital security advisers agreed that many of the digital security toolkits and guidebooks are application-focused. Very few address political context and individual differences when introducing tools. For Rabeh, some toolkits do a good job at framing the context through which users are working.

"The LGBT communities websites address the behaviours of these communities online, especially that dating websites are becoming an essential tool for them to meet." Rabeh mentions this example to reflect how toolkits should address certain behaviours of their target groups. He adds that once you are able to replace the specific target group in the toolkit text with any other group – for example, say "journalists" instead of "LGBT communities" – then you know that the toolkit is not contextual.

In order for a toolkit to be useful to the needs of the target group, a proper needs assessment survey should take place. This is how the Moroccan news organisation safeguarded their operations in and outside the office. The digital security training that Alaa participated in was not sufficient to draw up a whole strategy for the organisation without looking at the processes and practices of its work.

Context does not only mean the current national legislative environment, but can go down to situational instances. In Alaa's media organisation, for instance, in order to find a balance between efficiency and security, the guidelines for security provide room for flexibility, according to the topic that is being covered by journalists. While there is a base for using secure technology tools, Alaa's organisation attempts to only apply very rigid security practices if journalists are working on very sensitive issues.

Sometimes digital security manuals are counter-effective

Some of these manuals were not subjected to a security review pre-publication, as Rabeh mentioned. In some cases, the manuals jeopardised the security of organisations and activists that were identified as examples in such manuals. For Rabeh, connecting the name of an organisation or an activist to the privacy field without consulting them is a violation of their privacy, especially when an organisation does not announce its work in the privacy field.

Overly certain

The language of certainty in some training kits can be alarming for digital security trainers given all the findings of security holes – the SSL Heartbleed, for example.[78] Many of these manuals introduce tools with a cause-effect tone that directly connects usage and security. While introducing Tor for safe navigation, for example, Haleem lists all the controversy around it to prevent participants from blindly adopting it without keeping themselves updated on future developments. Rabeh does not speak with the same certainty about Signal on mobile phones when it comes to its desktop application. "We need to highlight risks using these tools, and differentiate between the security of protocols, mobile and desktop applications." Rabeh also alludes to the perception of absolute safety that these manuals sometimes create, and adds, "Encryption will not immunise you from torture."

Part of the problem is that some NGOs who develop these manuals lack the technical experience and end up with improper evaluations of the tools. For Rabeh, finding a 2015 toolkit that still recommends TrueCrypt,[79] for example, is problematic and does not reflect the recent developments in the file encryption field. The challenge for NGOs producing these manuals is the lack of dedicated staff for such topics to provide continuous updates on changes in tools and technologies in the field of digital security.

78 The Heartbleed bug is a security flaw in OpenSSL protocol versions 1.0.1 through 1.0.1f discovered in April 2014. The flaw affects the protocol that ensures the security of banking and chatting transactions and emails. The bug manipulates a server to extract information from its memory on the history of transactions. You can learn more here: www.businessinsider.com/the-heartbleed-bug-explained-in-one-cartoon-2014-4

79 TrueCrypt is a hard drive encryption tool for Windows. In 2015, TrueCrypt underwent a security audit that revealed flaws compromising security. "The flaws, which were apparently missed in an earlier independent audit of the TrueCrypt source code, could allow attackers to obtain elevated privileges on a system if they have access to a limited user account." See Constantin, L. (2015, 29 September). Newly found TrueCrypt flaw allows full system compromise. *Network World*. www.networkworld.com/article/2987436/newly-found-truecrypt-flaw-allows-full-system-compromise.html

RECOMMENDATIONS

These recommendations are curated from interviews that the research team conducted with four interviewees from Morocco, Palestine and Egypt. Addressing donors, NGOs and digital security trainers that are active in the field of securing privacy, the following recommendations were compiled:

To increase the effectiveness of digital security programmes, contextual research should take place, addressing the diverse human rights realities, not only at the country level but also at the level of the targeted group.

While violations of human rights in Arab countries have similarities, the intensity, consistency and fatality of violations are different from one country to another. In countries of crisis and war in the region, the physical security and privacy of citizens and activists may be a higher priority than their digital security practices. In countries where activists and journalists are facing forced disappearances and jail because of their political activities, digital security cannot be treated as key to security and safety. Some countries use legislative powers to restrict freedoms of anonymity or encryption. In this case digital security consultants have to assess the risks of using encryption for activists in their respective countries.

Seeking local specialised consultation strengthens the appropriateness of digital security advice to the needs and the political situation in the country itself. The customisation of digital security training should go as far as the targeted individual or organisation, because even within the same country, their digital security needs differ.

It is important to to factor in the layout of the internet infrastructure of the country when assessing risks to digital security and recommending tools or practices.

The infrastructural realities assist with understanding what is possibly achievable when it comes to online protection. It is essential to ask questions such as, for example, could Gazans ever be able to communicate securely using their phones or internet connections given the strong dependence of their network on the Israeli network? Or, are privacy workshops a priority in Gaza when electricity is so scarce?

Digital security trainings and manuals should be behaviours-focused more than tools-focused.

Risk and needs assessments are very important in developing digital security trainings and manuals. Many digital security trainings are based on the assumption that digital security is a priority for activists in countries where state surveillance exists. In countries of crisis or abusive human rights policy, physical security could take priority over digital security. As one activist said, "Digital security cannot protect you from torture."

On top of legislative and infrastructural realities, activist groups have developed different communication and organisation behaviours that suit their aims and environment. When planning for digital security consultation, the training entity should negotiate a middle ground of secure practices that do not restrict activists' and organisations' operations, and measure the risks that recommended practices and tools entail. Engaging activists in developing a privacy policy according to their surroundings is essential to achieve the adoption of more secure communication behaviours.

To ensure better adoption of practices, ongoing support and adaptation of advice should also be provided beyond the training or the consultation time frame. Variances in the needs of different organisations at different times should steer manuals and guidelines from the "assertive tone" of achieving safety by using tools, to guiding groups into the questions that they should ask when adopting tools or communication behaviours.

It is necessary to subject digital security manuals to technical and security risk audits prior to publishing.

It is very important for NGOs developing manuals and guidelines to consult technical security auditors before publishing their manuals. A scientific approach to introducing tools and explaining how they work is essential to avoid the blind adoption of tools and to focus instead on concepts that explain why they are secure. It is also important to test the certainty regarding a tool and emphasise the time factor of these tests in case the information becomes outdated in the future.

Internet and ICTs for social justice and development

APC is an international network of civil society organisations founded in1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs).

We work to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

www.apc.org info@apc.org

SUPPORTED BY THE EUROPEAN UNION UNDER THE EUROPEAN INSTRUMENT FOR DEMOCRACY AND HUMAN RIGHTS (EIDHR)

DIGITAL SAFETY IN CONTEXT: PERSPECTIVES ON DIGITAL SECURITY TRAINING AND HUMAN RIGHTS REALITIES IN THE MIDDLE EAST AND NORTH AFRICA
April 2016

ISBN 978-92-95102-60-6 APC-201604-CIPP-I-EN-DIGITAL-251

Creative Commons Licence: Attribution-NonCommercial ShareAlike 3.0 licence

Graphic Design: MONOCROMO