# Measuring the (in)security of Palestinian civil society websites

Alexei Abrahams
TaSC Project, Harvard University

Etienne Maynier
Amnesty International

**Abstract**

Civil society organizations (CSOs) are reemerging as the central reference of the Palestinian struggle at a time when cyber threats to civil society are on the rise worldwide. We develop a web scanning tool to gather security data on websites and web servers, finding Palestinian CSOs neglect even basic precautions like encrypting web traffic or keeping software updated. Why? Evidence suggests this neglect cannot easily be explained by technical or financial constraints. Widening our scan to include Israeli organizations, and non-Palestinian organizations allied with the Boycott, Divestment, and Sanctions (BDS) movement, we find similar security lapses, suggesting insecurity is neither unique to Palestinian CSOs nor does it necessarily decline as organizations enter into contentious politics. Our results underscore the sociotechnical nature of cybersecurity, while encouraging greater vigilance from CSOs.

**Keywords:** Cybersecurity, information security, civil society, Israel-Palestine conflict

We would like to thank Wendy Pearlman, Diana Greenwald, Christopher Parsons, the organizers and participants of Harvard University's Political Violence Workshop (April 2022), the organizers and participants of a session of the Middle East Studies Association annual conference (October 2020), two anonymous referees, and the editor, for their very helpful feedback. This research has been done in a personal capacity and does not represent the views of Amnesty International, nor those of Harvard University. All errors are our own.

Amidst widespread disillusionment with the Palestinian Authority and the Oslo process, Palestinian civil society over the past decade has been reclaiming the mantle of resistance. While the PA's security cooperation with Israel in the West Bank continues to deepen, Palestinians have increasingly organized protests outside PA jurisdiction, in Area C or even East Jerusalem.[1] Civil society organizations (CSOs), wary of co-option, have increasingly found alternative means of funding their projects (as Catherine Herrold argues in this special issue). In the diaspora, the Boycott, Divestment and Sanctions Movement (BDS) has gained allies far and wide.[2] Recently there has even been talk of revitalizing the Palestine Liberation Organization (PLO) and sidelining the PA.[3] For the first time since Oslo's birth in 1993, it appears Palestinian civil society will once more be the central reference of the Palestinian struggle.

The landscape of power, however, has changed since the end of the Cold War in ways that present Palestinian civil society with both new opportunities and challenges. Prominently, information technologies have emerged over the past three decades to form a sociotechnical infrastructure to which societies worldwide are increasingly interfaced. With some skill, otherwise weak actors can subvert this infrastructure, lending them 'reverse structural power.'[4] Indeed, since the start of the Arab Spring a decade ago, there has been a growing understanding that the ability of civil society to effectively challenge state and corporate authorities is importantly tied up with its existence online.[5] Protest movements now routinely rely on social media to broadcast their grievances and demands, galvanize citizens, and coordinate the time, place, and nature of protests. Independent news agencies and think tanks publish articles on the web that challenge status quo narratives. Activists coordinate bilaterally with each other on their mobile devices, even across vast geographic diasporas.

The majority of these communications, however, travel over infrastructure maintained by precisely the same authorities that civil society actors seek to challenge. A growing body of scholarly evidence confirms that authorities around the world exploit their 'man-in-the-middle' position to throttle, divert, intercept, and monitor civil society communications, while hacking and implanting malware on the devices of journalists and human rights defenders.[6] Palestinian civil society, among others, is arguably a 'most likely' target of such digital repression. Within the occupied Palestinian territories, for example, the layout of communications infrastructure implies a high likelihood that Israeli authorities can intercept and tamper with internet traffic.[7] Israeli technology companies such as NSO Group, moreover, are closely tied to Israeli military

---

[1]Dana El Kurd, *Polarized and Demobilized: Legacies of Authoritarianism in Palestine* (Oxford: Oxford University Press, 2019).
[2]Nathan Brown and Daniel Nerenberg, "Palestine in Flux: From Search for State to Search for Tactics," *Carnegie Endowment for International Peace* (2016). Available from https://carnegieendowment.org/2016/01/19/palestine-in-flux-from-search-for-state-to-search-for-tactics-pub-62486. Omar Barghouti, *BDS: Boycott, divestment, sanctions: The global struggle for Palestinian rights* (Chicago: Haymarket Books, 2011).
[3]Marwa Fatafta and Alaa Tartir, "Why Palestinians Need to Reclaim the PLO," *Foreign Policy*, 2020. Available from https://foreignpolicy.com/2020/08/20/palestinians-reclaim-plo-palestinian-authority-democracy/.
[4]Lennart Maschmeyer, "What is Cyber Power?" (2021).
[5]Larry Diamond, & Marc F. Plattner (Eds.), *Liberation technology: Social media and the struggle for democracy* (Baltimore: Johns Hopkins University Press, 2012). Philip N. Howard and Muzammil M. Hussain, *Democracy's fourth wave?: digital media and the Arab Spring* (Oxford: Oxford University Press, 2013). Manuel Castells, *Networks of outrage and hope: Social movements in the Internet age* (Cambridge: Polity, 2012).
[6]Marc O. Jones, *Digital Authoritarianism in the Middle East* (2021). Margaret E. Roberts, *Censored: distraction and diversion inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018). Nils B. Weidmann and Espen G. Rød, *The Internet and political protest in autocracies* (Oxford, UK: Oxford University Press, 2019).
[7]7amleh, "Connection Interrupted: Israel's Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights" (2018), available from: https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf.

intelligence and are often implicated in cyber attacks on civil societies around the globe.[8] That the same technologies might be directed against Palestinian civil society seems a strong possibility.[9]

Are Palestinian CSOs secure? In contrast to the attacker-centric paradigm ubiquitous in the literature, we focus on the defender, looking for weaknesses in Palestinian civil society's digital infrastructure. By identifying lapses and loopholes, we hope to empower Palestinian civil society to proactively improve its cybersecurity. In so doing, and in the spirit of this special issue, we join the recent trend within Palestinian politics "away from ultimate ends and towards immediate means,"[10] emphasizing what Palestinians can do to take the initiative and be protagonists in their own story.

We proceed by creating a web scanning tool to gather security data on Palestinian and Palestine-allied CSO web infrastructure. In simple terms, the scanner is a computer program that scans websites and web servers, checking to see if the CSO web administrators have implemented basic security precautions: are web browser sessions automatically encrypted? Is the website's software up to date? Is the website protected from distributed denial of service attacks? And so on. We gather security data on the websites and web servers of 228 Palestinian CSOs, 73 non-Palestinian CSOs affiliated with the BDS movement, and a benchmark sample of 30 Israeli think tanks and 56 Israeli news agencies. Our dataset – the first of its kind (not only for Palestine, but worldwide) – paints a troubling picture of insecurity, encouraging a shift of attention for both researchers and Palestinian CSOs, and raising puzzling patterns worthy of future study.

We find that Palestinian civil society web infrastructure scores poorly in absolute terms on multiple security dimensions. Many CSO websites do not forcibly encrypt web traffic, instead allowing or even insisting on plaintext communication. Almost no CSOs are equipped with protection from distributed denial of service (DDoS) attacks. Many websites and web servers run out-of-date software. Indeed, a major takeaway of our analysis is that Palestinian CSOs could substantially improve their web security simply by keeping their software updated. Researchers, meanwhile, should perhaps shift their attention from the fascinating but rarefied dangers of cutting-edge 'zero-day' attacks to the more first-order question of why civil society organizations chronically neglect their cybersecurity.[11] While our data merely constitutes the starting point for that investigation, it does cast doubt on a few potential explanations.

Firstly, security negligence is not the result of technical constraints. For all of the weaknesses we identify in Palestinian web infrastructure, technological solutions have already been invented – often years ago. Secondly, security negligence cannot be easily explained by financial constraints. For example, it has been almost a decade since it became both free and easy to encrypt web traffic, yet many Palestinian CSO websites continue to communicate via plaintext. Likewise, DDoS protection is freely available for civil society, but almost no Palestinian CSOs avail themselves of it. Similarly, much of the outdated software that Palestinian CSOs are running can be updated for free. Thirdly, security negligence is not a phenomenon idiosyncratic to Palestinian civil society. We extend our scan to include Israeli think tanks and

---

[8]Amos Barshad, "Inside Israel's lucrative — and secretive —cybersurveillance industry," 2021, Available from https://restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline.

[9] Indeed, as we discuss below, evidence has begun to emerge that this is the case.

[10]Brown and Nerenberg (2016).

[11]Nicole Perlroth, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, (New York, NY: Bloomsbury Publishing, 1st edition, 2021). Bill Marczak and John Scott-Railton, "The million dollar dissident: NSO group's iPhone zero-days used against a UAE human rights defender", *The Citizen Lab* (2016).

news agencies, which score better on most metrics – but not much better, and still poorly in absolute terms. Finally, the contentiousness of an organization's politics does not seem to predict a concomitant degree of security preparedness. We extend our scans to non-Palestinian, BDS-affiliated organizations, which have arguably more reason to anticipate hostility than the average charity or sustainable development organization in Palestine, yet, according to our scans, are no more prepared. While the explanation for negligence thus remains elusive, it seems evident that the insecurity of Palestinian and Palestine-affiliated civil society is as much a social matter as a technical one, inviting attention from social scientists as well as computer scientists.

**Civil Society, Surveillance, and Cybersecurity**

Citizens lacking institutionalized channels for the remediation of grievances will tend to form organizations through which they can seek redressal *extra-institutionally*.[12] These 'civil society' organizations (CSOs) are often incubators for contentious political action and are, consequently, the targets of state repression or co-option. Surveillance is integral to both of these strategies, as is well known to scholars of the Middle East. Atia and Herrold document how the Moroccan government finances civil society in order to have full surveillance and control over it, while Western funding to Palestinian NGOs is generally conditional on projects being de-politicized and 'upwardly accountable.'[13] Herrold finds the culture of co-option, repression, and surveillance of NGOs in Egypt has grown even more stifling in recent years under the Sisi regime.[14]

Over the past decade, as civil society has become more and more interfaced with digital technologies, governments have stepped up hacking and remote surveillance – the digital counterpart of the human spies and informants of yesteryear. Civil society increasingly relies upon the internet to communicate with audiences and coordinate with peers, yet these digital activities tend to be hosted on and/or traverse infrastructure controlled by some of the same authorities civil society seeks to challenge. A growing literature across the global south has documented governments abusing their 'man-in-the-middle' positions to frustrate, surveil, and intercept civil society communications. During times of political unrest, for example, many governments are known to throttle internet traffic.[15] In a more fine-grained version of this, governments are also known to block or limit access to certain websites.[16] More actively, numerous investigations by watchdog organizations like Citizen Lab or Amnesty International have proven that states hack the digital devices of activists and human rights defenders to surveil and repress them.[17] Within the Middle East, for example, Citizen Lab and Amnesty International

---

[12]David A. Snow, Sarah A. Soule, and Hanspeter Kriesi (Eds.), *The Blackwell companion to social movements*, (Malden, MA: John Wiley & Sons, 2008), Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups, Second Printing with a New Preface and Appendix* (Cambridge, MA: Harvard University Press, 2009).

[13]Mona Atia and Catherine E. Herrold, "Governing through patronage: The rise of NGOs and the fall of civil society in Palestine and Morocco", *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations*, *29*(5), 1044-1054 (2018).

[14]Catherine E. Herrold, *Delta Democracy: Pathways to Incremental Civic Revolution in Egypt and Beyond* (Oxford, UK: Oxford University Press, 2020).

[15]Tina Freyburg and Lisa Garbe, "Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa", *International Journal of Communication*, *12*, 3896-3916 (2018). Jan Rydzak, Moses Karanja, Nicholas Opiyo, "Internet Shutdowns in Africa| Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries," *International Journal of Communication*, *14*, 24 (2020).

[16]Margaret E. Roberts, *Censored: distraction and diversion inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018).

[17]Amnesty International, "Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks" (2021), available from: https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks. John Scott-Railton, Bill Marczak, Siena Anstis, Bahr AbduRazzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless

have confirmed cases of digital surveillance of human rights defenders in the UAE, Saudi Arabia, Egypt, and Morocco.[18]

To make headway in the face of repressive surveillance, CSOs must attempt to protect themselves from surveillance and/or disguise their activities to appear innocuous to authorities. Writing on Egyptian civil society, Catherine Herrold argues that instead of drawing attention to themselves by agitating openly for human rights or democratization, CSOs in authoritarian states should emulate the behavior of some Egyptian CSOs that publicly claim a more mundane mission ('sustainable development') while quietly folding democratic processes into their daily community engagement.[19] Conversely, Barton Gellman, in his reflections on Edward Snowden and the American surveillance state, argues that if a government could perfectly surveil civil society, it would always be able to frustrate and foil social justice reform.

All that remains to be recognized is that cybersecurity helps civil society evade state surveillance and preserve its reformative potential. By keeping communications encrypted end-to-end, and keeping software updated to block known attack vectors, civil society can substantially frustrate the state's attempts to surveil their devices, maintaining operational secrecy long enough to achieve their aims.

Despite the evident importance of civil society's cybersecurity, data collection and analysis remain scarce and piecemeal. One recent study explains the data vacuum by arguing that there are really two global cyber conflicts in progress: a 'high-end' conflict, roughly corresponding to inter-state cyberwarfare and corporate espionage; and a 'low-end' conflict, in which citizens and civil society organizations are primary targets.[20] Since governments and corporations can generally pay top dollar, cybersecurity professionals focus on the 'high-end' conflict, creating a skewed data environment that frustrates awareness of the 'low-end' conflict. Relatedly, James Shires argues that cybersecurity has tended to be conceptualized as security *for* the state *from* anarchic actors such as criminals or terrorists.[21] Thus, cybersecurity professionals focus on the security of the state and big corporations not only because those actors pay the best, but also because cybersecurity is imagined in a state-centric way. A growing alliance of civil society actors, however, has undertaken a "moral maneuver" over the past two decades to recast cybersecurity according to a more human-centric paradigm.[22] Within this new paradigm it becomes possible to think of cybersecurity as being *for* civil society *from* the state.

Within this new space, however, many investigations follow the paradigm of threat reporting, not security assessment. Organizations like Citizen Lab and Amnesty International, for

---

VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware" (2019), available from: https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife.

[18]Marczak and Scott-Railton (2016). Bill Marczak, John Scott-Railton, Adam Senft, Bahr AbduRazzak, and Ron Deibert, "The Kingdom Came to Canada - How Saudi-Linked Digital Espionage Reached Canadian Soil" (2018), available from: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil. John Scott-Railton, Bill Marczak, Ramy Raoff, and Etienne Maynier, "Nile Phish - Large-Scale Phishing Campaign Targeting Egyptian Civil Society" (2017), available from: https://citizenlab.ca/2017/02/nilephish-report. Amnesty International, "Morroccan Journalist Targeted with Network Injection Attacks using NSO Group's Tools" (2020a), available from: https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools, Amnesty International, "German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed", (2020), available from: https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed.

[19]Herrold (2020).

[20]Lennart Maschmeyer, Ron Deibert, and Jon Lindsay, "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society", *Journal of Information Technology & Politics,* Vol 18 (2020).

[21]James Shires, *The politics of cybersecurity in the Middle East* (2021).

[22]Ibid.

example, conduct deep investigations of specific malware binaries deployed against civil society actors; specific incidents of penetration of civil society devices; or specific attack infrastructures used by state actors targeting civil society. While such reports commendably draw attention to the plight of civil society in the global south, their overriding model of policy change is not to directly empower civil society to steel itself against attack, but rather to prompt Western policymakers to intervene, for example by regulating the surveillance technology market, bilaterally censuring abusive governments, or setting international standards and norms.

Threat reports, moreover, are not the products of representative sampling, but emerge from an uneven and opportunistic selection process.[23] Indeed, as one of the coauthors can confirm firsthand, a primary consideration that determines whether or not an investigation proceeds is *novelty*. The hunt for novelty in turn leads to a preoccupation with so-called 'zero day' attacks, a particularly rarefied category of cyber attack that leverages bugs in computer code that software developers themselves have not yet discovered (Perlroth 2021). The literature's preoccupation with novel attack vectors centers the conversation on technological problems with technological solutions. Cybersecurity is sociotechnical,[24] however, relying not only on software developers to follow safe coding practices, but also on end users to be vigilant about running software updates, enabling encryption, using hard-to-guess passwords, adjusting default settings on apps, and so on.

Is civil society vigilant about cybersecurity? Most of what we know pertains to one particular sector: news media. Especially in the wake of the Snowden revelations of 2013, there has been a growing awareness of cyber threats against journalists, prompting scholars to ask if their cybersecurity practices have likewise evolved. Across the board, interviews suggest that journalists often do not yet follow best practices.[25] Interviews reveal several possible causes for this, including a lack of training or institutional support for digital security, along with issues with the usability of security tools. McGregor and Watkins (2016) find that journalists do not feel the need for information security unless they are working on a topic perceived of interest to nation-state actors, a perception that is not aligned with existing knowledge on state surveillance.

While illuminating, these studies are limited on several fronts. Firstly, they rely purely on self-reported cybersecurity habits, without conducting independent security assessments. The only paper that transcends this limitation is Marczak and Paxson (2017), which is also the only paper that extends interviews beyond journalists to civil society more generally.[26] The authors interview thirty subjects in the MENA region, including but not limited to individuals employed at news media organizations. They then conduct a security assessment of their personal computers and mobile devices. Tellingly, and consistent with our findings below, they find that

---

[23]Maschmeyer, Diebert, and Lindsay (2020).

[24]Matt Goerzen, Elizabeth Anne Watkins, and Gabrielle Lim, "Entanglements and exploits: Sociotechnical security as an analytic framework," *9th USENIX Workshop on Free and Open Communications on the Internet, FOCI 19* (2019).

[25]Jennifer R. Henrichsen, "Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies," *Digital Journalism*, 8:3, 328-346 (2020). Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui & Ronald Deibert, "The Information Security Cultures of Journalism," *Digital Journalism*, 8:8, 1068-1091 (2020). Philip Di Salvo, "Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protection," *Digital Journalism* (2021). Susan E. McGregor, Elizabeth A. Watkins, "'Security by Obscurity': Journalists' Mental Models of Information Security," *ISOJ* Vol 6:1 (2016). Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner, "Investigating the computer security practices and needs of journalists," *24th USENIX Security Symposium (USENIX Security 15)*, pp. 399-414 (2015).

[26]Bill Marczak and Vern Paxson, "Social Engineering Attacks on Government Opponents: Target Perspectives," *Proceedings on Privacy Enhancing Technologies*, *2* (2017), 172-185.

their interviewees tend to run outdated software, fail to encrypt their hard drives, and fall short on best practices to defend against social engineering ('phishing') attacks.[27]

Next, these studies concentrate on individuals, but ignore the cybersecurity of organizations.[28] McGregor et al. (2015) highlights that the institutional support (or lack thereof) on digital security plays an important role in the difficulty to adopt security practices. This is further affirmed by Crete-Nishihata et al. (2020), who find that employment status plays an important role in the adoption of security practices. These studies, however, are based on individual interviews and not on organizations. Studying CSO cybersecurity at the organization level can provide a more accurate picture of its security level, as a successful attack against an organization may lead to compromise of members and their individual devices.

Relatedly, these studies ignore web security, even though civil society organizations, and particularly news organizations, tend to maintain websites. Since the early days of the Internet, compromising and modifying websites (a practice known as "defacing") has been favored by so-called "hacktivists" groups or others with political motives, including actors ranging from the Anonymous movement to the Syrian Electronic Army.[29] More recently, there have been more and more cases of compromised websites by nation-state actors in order to infect websites with malicious code and attempt to compromise selected visitors.[30] Web security is thus a key aspect of digital security for organizations with a large online presence.

Finally, these studies primarily focus on the West. We found one article whose interview subjects were Hong Kong journalists, and a single article interviewing Turkish journalists.[31] This latter article, along with Marczak and Paxson (2017), were the only such studies we could find that addressed Middle Eastern subjects, despite the ubiquity of cyber attacks against Middle Eastern civil society documented in threat reports referenced above. On Palestine, meanwhile, the literature is completely silent. This silence, as we shall now see, is particularly conspicuous given that Israel has both the means and motive to target Palestinian civil society.

**The resurgence of Palestinian civil society**

Since the early years of the Palestinian refugee crisis, Palestinian civil society has been embroiled in contentious political action. In exile, under the umbrella of the Palestine Liberation Organisation (PLO), Palestinian militant groups launched attacks against Israel from Jordan, Lebanon, and Syria, and even targeted Israelis abroad.[32] After 1967, within the occupied territories of Gaza and the West Bank, Islamic community organizations and charities cultivated dense grassroots loyalty networks before ultimately sprouting militant wings in the 1980s

---

[27]Another important, threat-centric study of social engineering attacks on civil society is Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda, "A look at targeted attacks through the lens of an NGO," *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 543-558 (2014).

[28] Samarin et al (2020) review the structure of a single, multinational NGO (the International Committee of the Red Cross), and offer some thoughts on security practices. Nikita Samarin, Alisa Frik, Sean Brooks, Coye Cheshire, and Serge Egelman, "Conducting Privacy-Sensitive Surveys: A Case Study of Civil Society Organizations," *arXiv preprint arXiv:2003.08580* (2020).

[29]US Army website defaced by Syrian Electronic Army hackers - We Live Security https://www.welivesecurity.com/2015/06/09/us-army-website-hack/.

[30] See for instance : OceanLotus: New watering hole attack in Southeast Asia by We Live Security https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/.

[31]Lokman Tsui and Francis Lee. "How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom," *Journalism* (2019). Bora Ataman and Barış Çoban, "Counter-surveillance and alternative new media in Turkey," *Information, Communication & Society* 21, no. 7 (2018): 1014-1029.

[32]Peter Krause, *Rebel power: Why national movements compete, fight, and win* (Ithaca, NY: Cornell University Press, 2017). Wendy Pearlman and Boaz Atzili, *Triadic Coercion: Israel's Targeting of States That Host Nonstate Actors*, (New York, NY: Columbia University Press, 2018).

(Hamas, Islamic Jihad).[33] During the First Intifada, grassroots organizations across the occupied territories coordinated protests and strikes, battering the Israeli economy and ultimately provoking peace negotiations in the early 1990s.[34]

With the signing of the Oslo Accords (1993), and the promise of an impending peace with Israel, power shifted from civil society to the Palestinian Authority (PA), a proto-government apparatus staffed disproportionately by PLO returnees.[35] Especially following the Fatah-Hamas schism of 2007, the PA has declined into an increasingly authoritarian enforcer of Israel's security, under whose reign Palestinian civil society has been substantially tamed and defanged.[36] Not unrelatedly, the occupied territories have likewise experienced an infusion of aid from Western countries, delivered either directly into PA coffers, or granted to civil society organizations earmarked for development projects and charitable activities.[37]

Growing disillusionment over the status quo, however, along with the rise of the Boycott, Divestment, and Sanctions (BDS) movement,[38] has led many prominent voices to call for the dismantling of the PA, the restoration of the PLO, and, by implication, a recentering of power back into the hands of Palestinian civil society.[39] Indeed, recent years have witnessed increased protest activity in the Occupied Territories and East Jerusalem, particularly in areas beyond the PA's jurisdiction.[40] As Palestinians disentangle themselves from the Oslo proto-government model, they are reverting to a model where civil society organizations are once more coordinating and leading contentious political action.

Like other civil societies, Palestinian civil society's online presence has expanded with the rise of the digital age.[41] As we shall see below, many Palestinian CSOs maintain websites and social media accounts to advertise their activities and seek donations.[42] The BDS movement maintains a central website to provide updates on victories and new initiatives, and to connect new recruits with allied organizations near them.[43] Palestinian activists and advocates may be found on Twitter, Facebook, and YouTube, drawing attention to the Palestinian struggle. There are even organizations like 7amleh (The Arab Center for Social Media Advancement) that exist to monitor issues "related to Palestinian digital activism," train Palestinian activists to do "digital campaigning," and advocate for greater "digital rights."[44]

As we have seen with other civil societies, however, the promises of Palestinian digital activism are bound up with threats and dangers. Firstly, within the occupied Palestinian territories, the underlying digital infrastructure is Israeli-owned. Traffic in and out of the

---

[33]Milton-Edwards and Farrell (2010).
[34]Wendy Pearlman, *Violence, nonviolence, and the Palestinian national movement*, (Cambridge, UK: Cambridge University Press, 2011).
[35]Alexei Sisulu Abrahams, "Not Dark Yet: the Israel-PA principal-agent relationship 1993-2017," Chapter 7 in *Proxy Wars*, edited by Eli Berman and David Lake (Ithaca, NY: Cornell University Press, 2019).
[36]El Kurd (2019), Amaney Jamal, *Barriers to democracy: The other side of social capital in Palestine and the Arab world*, (Princeton, NJ: Princeton University Press, 2009). Benoit Challand, *Palestinian civil society: Foreign donors and the power to promote and exclude*, (New York, NY: Routledge, 2008).
[37]Jeremy Wildeman and Alaa Tartir, "Unwilling to change, determined to fail: Donor aid in occupied Palestine in the aftermath of the Arab uprisings," *Mediterranean Politics* 19, no. 3 (2014): 431-449. Tariq Dana, "The structural transformation of Palestinian civil society: Key paradigm shifts," *Middle East Critique*, *24*(2), 191-210 (2015). Atia and Herrold (2018).
[38]Atia and Herrold (2018), Bargouthi (2011).
[39]Fatafta and Tartir (2020).
[40]El Kurd (2019).
[41]Miriyam Aouragh, "Everyday resistance on the internet: the Palestinian context," Journal of Arab & Muslim Media Research, Volume 1, Number 2, 26 November 2008, pp. 109-130(22).
[42] 7amleh (2021), "Needs Assessment of Palestinian Civil Society Organizations' Digital Perfomance," 7amleh (2021), available at https://7amleh.org/2021/10/18/7amleh-released-a-survey-of-the-digital-activity-of-palestinian-civil-society-organizations.
[43]https://bdsmovement.net.
[44]https://7amleh.org/about.

territories passes through Israeli-controlled switch points, while traffic within the territories runs along infrastructure that was inherited from the Israelis.[45] Within the West Bank, moreover, areas that fall under total or partial Palestinian jurisdiction (Oslo areas A and B) are archipelagoed by Israeli-controlled areas (Area C). This means that Palestinian communications hopping from one 'island' of control to another must pass through Israeli-controlled infrastructure. Thus, both within the West Bank and at the exit nodes of both Gaza and the West Bank, Israel has opportunities to intercept and tamper with Palestinian traffic.

The dangers to Palestinian civil society inherent to this architecture of control are amplified by the formidable cyber capacities of Israel itself. Israel is home to a vibrant technology industry and startup culture symbiotically intertwined with military intelligence. Talented young hackers, conscripted straight out of high school and trained in state-of-the-art army signals units, feed forward into the private sector even while retaining backward ties to the military.[46] Surveillance technologies developed by veteran-staffed Israeli firms like NSO Group, and exported to regimes like Saudi Arabia, are regularly implicated in attacks on civil society members.[47] In November 2021, it was confirmed that such technologies have been turned against Palestinian activists[48] – a revelation that fits perfectly within Israel's established modus operandi of surveilling Palestinians as a means of anticipating and foiling militancy.[49] Within the Palestinian territories, 7amleh has also recently published several reports raising concerns about facial-recognition surveillance and censorship on social media.[50]

In such a dangerous online environment, it makes sense to ask whether Palestinian CSOs are taking precautions to keep their infrastructure secure.

**Data**

To gather data on Palestinian civil society cybersecurity, we decided to narrow our focus in this study to websites and web servers. Web security, it should be emphasized, is just one among several dimensions of cybersecurity. A Palestinian CSO could and should be concerned about hardware hacks (when their digital devices fall into the hands of authorities, for example at checkpoints, border crossings, or during raids), remote mobile hacks, and social engineering ('phishing') attacks (the likeliest vectors in Frontline Defenders' recent investigation). But web security is an excellent starting point. CSO websites and web servers are internet-facing, and as such can be attacked remotely by anyone with internet access. From an attacker's perspective, they constitute low-hanging fruit, and so securing web infrastructure should concomitantly be a priority for the defender. By the same token, we can infer something about a CSO's overall

---

[45] 7amleh (2018), Helga Tawil-Souri, "Digital Occupation: Gaza's High-Tech Enclosure," Journal of Palestine Studies 41 (2012), 27-43.

[46] Barshad (2021).

[47] See threat reports mentioned above.

[48] Front Line Defenders, "Six Palestinian human rights defenders hacked with NSO Group's Pegasus Spyware," (2021), available from https://www.frontlinedefenders.org/en/statement-report/statement-targeting-palestinian-hrds-pegasus.
Jack Khoury and the Associated Press, "Palestinians Say Israeli NSO Spyware Found on Three Senior Officials' Phones," Haaretz (2021), available from https://www.haaretz.com/israel-news/tech-news/palestinians-say-israeli-nso-spyware-found-on-three-senior-officials-phones-1.10375992.

[49] Bergman, Ronen, *Rise and kill first: the secret history of Israel's targeted assassinations*, (London: Hachette UK, 2018).

[50] 7amleh, Facial recognition technology and Palestinian digital rights, (2020a), https://7amleh.org/2020/05/21/facial-recognition-technology-and-palestinian-digital-rights; 7amleh, Systematic Efforts to Silence Palestinian Content On Social Media, (2020b), https://7amleh.org/2020/06/07/systematic-efforts-to-silence-palestinian-content-on-social-media.

cybersecurity posture from its web security – if it runs an insecure website or web server, chances are it is negligent of its security on other attack surfaces, too.

From a research perspective, meanwhile, websites are easy to find, enumerate, and scan remotely. By contrast, assembling a list of civil society mobile devices and personal computers would be far harder and more ethically dubious. Marczak and Paxson (2017), for example, conduct in-person examinations of the personal computers and mobile devices of thirty individuals, but only after obtaining their consent. Obtaining consent and conducting in-person meetings, however, is costly and limits the size and scope of such studies. Web scanning, on the other hand, is free, fast, and automatable, implying scalability and facilitating broader claim-making.

*Web Scanner*

We developed a web scanning tool that extracts information directly from any given website and enriches those results with data from external databases. This tool, while by no means constituting a formal security assessment, yields a variety of data highly relevant to measuring a website's security posture and, by extension, the security of the organization as a whole.

More specifically, the scanner extracts the following information:

- Geolocation of the website
- If the website allows HTTPS, and if it makes it mandatory for visitors
- If the website is using an up-to-date framework
- If the websites uses HTTP Security Headers
- If the server hosting the website has any known software vulnerability issue
- If the website has protection against distributed denial of service attacks (DDoS)

*Geolocation of the website*

A website has to be hosted on a physical server somewhere. In order to assess the possibility of surveillance by foreign nations (especially Israel) over the visitors of a website, we identified the country where the website is hosted. In order to do that, we relied on the free IP geolocation database provided by the American company Maxmind.[51] While this geolocation is not very precise at the city level, it is reliable at the country level, which allows us to assess the possibility of foreign surveillance.

*HTTPS*

Whenever users visit a website in their browser, they are sending data to and receiving data from a remote server. The *lingua franca* by which the client and server communicate is a universally recognized protocol known as HTTP. Since the data generally hop across many intermediate nodes between the client and server, there is ample opportunity for malicious actors with access to these intermediate nodes to intercept, read, and modify the data – a so-called 'man-in-the-middle' (MITM) attack. As described in the previous section, Israel likely has a MITM position on internet traffic passing in and out of Gaza and the West Bank. In the case of the West Bank, it probably also has an MITM position on traffic passing through Area C. It is therefore wise to assume that traffic is being intercepted and that plaintext HTTP is being read. To counter this eavesdropping, traffic can be encrypted. The HTTPS protocol – 'S' standing for

[51]MaxMind - https://www.maxmind.com/en/geoip2-services-and-databases.

secure – was invented for precisely this end. Although HTTPS has now been available for two decades, its adoption massively increased following the Snowden revelations, an extensive campaign by the Electronic Frontier Foundation, and the creation of the free 'Let's Encrypt' service.[52] By 2016, 50% of recorded page loads used HTTPS, and in 2020, more than 80% of Chrome page loads used HTTPS.[53] Assessing whether the websites in our dataset are configured to allow HTTPS sessions – or better yet, to insist on HTTPS and refuse insecure HTTP sessions – is a baseline security metric.

*Using an up-to-date framework*

Nowadays most websites are typically not built from scratch, but rather draw upon third-party templates or frameworks. Some of the most popular of these Content Management Systems (CMS) are WordPress, Drupal, and Joomla. WordPress, for instance, was used to create 37% of Internet websites in 2019 according to W3Techs.[54] As such, website security critically depends on the underlying security of the CMS. Just as with software for desktops or mobile devices, CMS companies regularly announce updates and patches after weaknesses are identified by the security community; but website managers are not necessarily attentive to these updates. Accordingly, we scan our list of websites and identify if they use WordPress, Joomla or Drupal by requesting pages specific to these tools. If they do, our tool then tries to identify their version by checking pages known to display the version or by comparing specific pages with a database of known pages for different versions of Wordpress; Joomla or Drupal. If the version is successfully identified, we then check if they match the latest secure version released or if they use an older version. One limitation of the tool is that we are only considering these three most important CMSs, there is a long list of similar tools that are way less common, developing a tool to identify them and their version would be a research project in itself, so we focused on the three major ones.

*HTTP Security Headers*

The HTTP protocol now includes several headers that can be used by websites to increase their security. Using them is recommended as a best practice for websites, so it makes an interesting metric to know if the website is respecting standard security practices. Our tool is checking for the following headers:

- *Strict-Transport-Security:* indicates that a website should only be accessed using HTTPS.
- *X-Frame-Options:* indicates whether a browser should load this website in an iframe. When enabled, this option can protect a website against clickjacking attacks.
- *Content-Security-Policy:* defines rules over the execution of Javascript in the websites, increasing security against cross-site-scripting attacks

*Known Vulnerabilities on Server's Software*

When software vulnerabilities are discovered by the security community, they are indexed by the MITRE organization under the name 'Common Vulnerability and Exposure'[55] (CVE), and publicly disclosed with details on the nature of the vulnerability and the affected software versions. These vulnerabilities are classified by criticality using a score named Common Vulnerability Scoring System (CVSS), allowing us to only focus on critical and high

[52] https://letsencrypt.org/.
[53] https://transparencyreport.google.com/https/overview?hl=en.
[54] https://w3techs.com/technologies/details/cm-wordpress.
[55] https://cve.mitre.org/.

vulnerabilities. The Shodan[56] internet scanning platform regularly performs internet wide scans and identifies versions of software hosted by websites, matching them to the CVE database. For each website in our dataset, we identify the server and query Shodan to list known vulnerabilities of the software running on these servers.

*DDos Protections*

Distributed Denial of Service (DDoS) is a type of cyberattack in which a website server is deliberately and maliciously overwhelmed by requests from a large network of computers under the attacker's control. Multiple techniques exist to protect a website against DDoS. A common approach is to use a caching platform to protect the website from malicious requests. Three organizations in particular offer free and robust DDoS protection services to civil society websites: Cloudflare through project Galileo;[57] Google through project Shield;[58] and the Deflect project of Equalitie.[59] These free services are among the best DDoS mitigation solutions available to civil society websites. For each website in our dataset, we detect whether it has availed itself of any of these three DDoS solutions.

*Intrusiveness of our web scanner*

It is important to make sure our web scanning tool does not create any issue on the website, either because of the type of requests made or the number of requests. The requests done by our tool do not attempt to exploit any specific vulnerability, they only browse pages in the same way a standard visit on the website would. When a browser is visiting a website, it loads all the needed resources (images, stylesheet etc.) to display the page, which creates as many requests to the website. This creates traditionally 10 to 20 requests to different pages of the website. Our tool performs 4 to 10 requests to the website, which is less than a normal visit by a browser. It is thus highly unlikely that our tool would have any impact on the website during the scan.

*Identifying websites to scan*

With our web scanning tool in hand, the next task is to assemble lists of CSO websites to scan. There is unfortunately no central registry of Palestinian CSOs, so we built a list of Palestinian civil society websites by drawing on three data sources. Firstly, we downloaded the Open Think Tank Database, a freely accessible spreadsheet listing think tanks from around the world.[60] Secondly, we scraped the ABYZ News Links website to obtain lists of news agencies from around the world.[61] Finally, we scraped arab[dot]org, a website purporting to aggregate NGOs by country for the Middle East and North Africa region.

The resulting sample of 228 Palestinian CSOs is listed in the first column of Table 1. While around 8% of the sample are news agencies, the majority (92%) are NGOs listed by arab[dot]org as focusing on advocacy, development, education, civil rights, and sustainability. The West Bank is the single largest represented territory, with 45.6% of organizations, followed by East Jerusalem (26.8%) and Gaza (16.7%). A handful were located in Israel or abroad, while

[56] https://shodan.io.
[57] https://www.cloudflare.com/galileo/.
[58] https://projectshield.withgoogle.com/landing.
[59] https://deflect.ca/.
[60] https://onthinktanks.org/open-think-tank-directory/.
[61] http://www.abyznewslinks.com/.

a further 5% (all news agencies) are likely operated within the Palestinian territories but do not appear to have a physical address.

As discussed earlier, we are particularly interested in Palestinian civil society organizations that would plausibly draw cyber attacks or surveillance. As several scholars have argued, however, many of the Palestinian CSOs founded since the start of the Oslo period are largely de-politicized conduits for foreign aid – professionalized, bureaucratized, and more upwardly accountable to their donors than downwardly accountable to Palestinian citizens.[62] Many of the 228 organizations in our list of Palestinian civil society websites may fit this mold. While Herrold (2020) argues that organizations may hide their political activities behind the veneer of innocuous neoliberal economic agendas, it makes sense to identify additional organizations that are more overtly confrontational and political.

The Palestinian Boycott, Divestment, and Sanctions (BDS) movement is definitely politically contentious and antagonistic, and has drawn sharp rebuke from Israel and many of its allies.[63] Organizations affiliated with the BDS movement, both Palestinian and otherwise, should therefore plausibly be the targets of cyber attack and espionage. From the BDS national movement website we scraped a list of 73 organizations worldwide that are allied with the BDS movement (the website lists 77 websites, but only 73 were functioning at the time of our scan - October 2020).

For comparison's sake, we also drew a sample of Israeli think tanks and news agencies from the former two sources. The list of Israeli media from ABYZ News yielded 56 functioning sites, while the Open Think Tank database yielded 30 Israeli think tanks with functioning sites. The final breakdown is displayed in Table 1.

[62] Atia and Herrold (2018), Dana (2015), Challand (2008), Jamal (2009).
[63] Barghouti (2011).

**Table 1: Civil society websites scanned**

| | | Palestinian civil society organizations | Non-Palestinian organizations BDS allies | Israeli organizations |
|---|---|---|---|---|
| Total | | 228 | 73 | 86 |
| Activity | NGOs / Think Tanks | 210 | 73 | 30 |
| | Media websites | 18 | 0 | 56 |
| Region[64] | West Bank | 45.6% | 0% | 0% |
| | Gaza | 16.7% | 0% | 0% |
| | East Jerusalem | 26.8% | 0% | 0% |
| | Israel | 0.9% | 0% | 100% |
| | Abroad | 1.3% | 100% | 0% |

We scanned these websites during the October 2020 - March 2021 period, while preparing this manuscript. The resulting cybersecurity dataset helps us see at a glance whether these organizations implemented cybersecurity best practices across the range of metrics described above.[65] This dataset is, to the best of our knowledge, the first of its kind for Palestinian civil society, and possibly for civil society more generally. Developing such a tool required not only technical efforts, but also interdisciplinary collaboration to identify relevant cybersecurity metrics and to make meaningful social scientific interpretations from the data. We believe it serves as a proof of concept that data of this kind can be feasibly gathered.

**Results**

*Insecurity of Palestinian CSO web infrastructure*

The first column of Table 2 summarizes cybersecurity statistics for our sample of 228 Palestinian CSOs. In absolute terms, the security of these organizations leaves a lot to be desired. Firstly, Palestinian CSO websites do not follow best practice for protecting visitors to their websites. Of the 228 Palestinian CSO websites scanned, we found that 133 (58.3%) allow plain-text (unencrypted) sessions; indeed, only 60 of these (45.1%) even allow secure sessions. Only 95 websites (41.7%) insist on secure (https) sessions, and only 13 websites (5.7%) enforce strict transport security (STS). Taken together, these results imply that for a majority of Palestinian CSO websites, visitor sessions may be easily monitored or modified by state authorities, even possibly including malicious payloads.

A similarly perplexing result holds for the website CMSes. For 83 of 228 websites, our tool was able to identify the CMS on which the website was built. Of these, we found that 55

[64] Here we are referring to the 'brick and mortar' location of the CSO, and not to the location from which the website is hosted.
[65] Due to ethical considerations, we are not publishing the dataset, but are happy to share it with researchers or civil society organizations on a case-by-case basis.

(66.3%) were using outdated versions of WordPress (45), Joomla (5), and Drupal (5). Using outdated software is dangerous, since software updates often patch publicly disclosed security vulnerabilities that can otherwise be exploited by attackers.

Of the 228 websites, 47 (20.6%) are hosted on servers located within Israel (4) and the occupied Palestinian territories (43), implying that Israeli intelligence services could gain physical access if necessary. Almost all of the other sites are hosted in the United States (44.3%) and Europe (32%), most notably Germany and the United Kingdom – all nations with robust intelligence sharing partnerships with Israel. Given this kind of geography, it is difficult to imagine how any of these websites could sustainably host content deemed unsatisfactory to Israeli interests.

Just one of 228 Palestinian websites has availed itself of DDoS protection. This means that, when necessary, adversaries could overwhelm these sites with traffic and put them temporarily out of service.

Finally, the underlying servers of 52 (22.8%) websites have at least one vulnerability rated 'high' or 'critical.' While the most common of these vulnerabilities was disclosed a year earlier, in 2019, some were disclosed as far back as 2006. The average number of years since disclosure was roughly 7.5, implying that over one in five Palestinian CSOs have been serving their websites from insecure servers for the better part of a decade.

**Table 2: Comparing security of Palestinian, BDS, and Israeli websites**

| | **Civil society websites** (news agencies, think tanks, CSOs) | | |
|---|---|---|---|
| | **Palestinian** | **BDS** | **Israeli** |
| Allow https sessions | **68.0%** (155/228) | **74.0%** (54/73) | **74.4 %** (64/86) |
| Force https sessions | **41.7%** (95/228) | **54.8%** (40/73) | **54.7%** (47/86) |
| Up-to-date CMS* | **33.7%** (28/83) | **27.5%** (11/40) | **43.5%** (10/23) |
| X-Frame-Options | **13.2%** (30/228) | **5.5%** (4/73) | **8.1%** (7/86) |
| Strict-Transport-Security | **5.7%** (13/228) | **19.2%** (14/73) | **5.8%** (5/86) |
| Content-Security-Policy | **1.3%** (3/228) | **1.4%** (1/73) | **7.0%** (6/86) |
| DDoS protection** | **0.4%** (1/228) | **9.6%** (7/73) | **17.4%** (15/86) |
| No high/critical CVEs*** | **77.2%** (176/228) | **78.1%** (57/73) | **81.2%** (70/86) |

*For technical reasons, the CMS version for each website could not always be identified.
**We only detected the use of Cloudflare, Google Cloud, or Deflect for DDos protection, three solutions offered for free to civil society but that do not together constitute an exhaustive list of DDoS mitigations.
***This number is calculated by querying the Shodan API (https://shodan.io).

*Explaining the insecurity of Palestinian web infrastructure*

What explains these security lapses? We now consider and cast doubt upon several possible explanations.

Firstly, one might wonder if perhaps there do not yet exist technological solutions to the security issues listed above. But by this point in the essay we know that this is not the case. For example, many Palestinian CSOs use plaintext HTTP, but the secure protocol HTTPS has existed for over two decades. Palestinian CSOs use outdated, vulnerable software, but updates exist for which vulnerabilities have been patched. Palestinian CSOs lack DDoS protection, yet DDoS protection is available, for example through CloudFlare. Nor can one claim that Palestinians organizations are unaware of these solutions; indeed, many Palestinian organizations have implemented them even as many have not.

Secondly, one might suppose that these cyber insecurities are idiosyncratic to Palestinian organizations or to the unique circumstances in which they find themselves. To dispel this notion, we scanned our sample of 86 Israeli think tanks and news agencies, and our sample of 73 non-Palestinian BDS-affiliated organizations. Columns 2 and 3 of Table 2 list the results. While it is evident that Israeli think tank and media websites outperform Palestinian CSO websites on most security metrics, in absolute terms Israeli security statistics are still deplorable. To take just one example, 74.4% of Israeli websites allow encrypted web traffic, which is only marginally higher than Palestinian CSOs (68.0%). Encryption of traffic for merely three in four sites is in any case underwhelming. As for (non-Palestinian) BDS-affiliated organizations, the differences with Palestinian CSOs are negligible. In summary, the cyber insecurity we observe in our data is by no means peculiar to Palestinian CSOs or their unique circumstances.

Thirdly, one might speculate that Palestinian CSOs want to secure themselves but cannot afford to financially. Indeed, in this special issue, Catherine Herrold's essay clarifies that many Palestinian CSOs operate under substantial financial constraints. Without financial data for the CSOs, we cannot easily adjudicate on this point. Table 2 suggests that Israeli organizations systematically outperform Palestinian organizations on web security, consistent with the story that Israeli organizations are better funded than their Palestinian counterparts. On the other hand, our sample of Israeli news agencies and think tanks is not immediately comparable to the variety of Palestinian NGOs we sampled. To compare 'apples to apples,' in Table 3 we restrict our attention to Palestinian and Israeli news agencies. Perhaps more so than CSOs in general, news organizations rely on their websites as the primary point of contact with their readers, so their web security is of particular interest.[66] The side-by-side comparison in Table 3 is far from definitive, but leans slightly in favor of Israeli news sites. Palestinian and Israeli news organizations enforce HTTPS at similar rates. Palestinian sites outperform Israeli sites on keeping their CMSes up-to-date, but the difference is not statistically significant (we could identify the CMS version for only two Palestinian sites). Palestinian news sites fare worse on DDoS protection, and their web servers run more vulnerable software.

**Table 3: Web security of Palestinian versus Israeli news organizations**

[66] Alexei Abrahams, "The Web (In)Security of MENA Civil Society and Media," POMEPS Studies (2021).

| | **News websites** | |
|---|---|---|
| | **Palestinian** (17) | **Israeli** (56) |
| Allow https sessions | **76.5% (13/17)** | **75.0% (42/56)** |
| Force https sessions | **47.1%** | **53.6% (30/56)** |
| Up-to-date CMS* | **100% (2/2)** | **25% (3/12)** |
| X-Frame-Options | **17.6% (3/17)** | **7.1% (4/56)** |
| Strict-Transport-Security | **0% (0/17)** | **7.1% (4/56)** |
| Content-Security-Policy | **0% (0/17)** | **7.1% (4/56)** |
| DDoS protection** | **5.9% (1/17)** | **17.9% (10/56)** |
| No high/critical CVEs*** | **70.6% (5/17)** | **83.6% (47/56)** |

*For technical reasons, the CMS version for each website could not always be identified.
**We only detected the use of Cloudflare, Google Cloud, or Deflect for DDos protection, three solutions offered for free to civil society but that do not together constitute an exhaustive list of DDoS mitigations.
***This number is calculated by querying the Shodan API (https://shodan.io).

**Table 4: Regional comparison of Palestinian CSO web security**

| | **Palestinian civil society websites** (news agencies, think tanks, CSOs) | | |
|---|---|---|---|
| | **West Bank** (106) | **Jerusalem** (61) | **Gaza** (40) |
| Allow https sessions | 67.0% | **70.5%** | **65.0 %** |
| Force https sessions | 39.6% | **49.2%** | **30.0%** |
| Up-to-date CMS* | 33.3% (15/45) | **47.1% (8/17)** | **14.3% (2/14)** |
| X-Frame-Options | 13.2% | **19.7%** | **5%** |
| Strict-Transport-Security | 3.8% | **11.5%** | **2.5%** |
| Content-Security-Policy | **0.9%** | **1.6%** | 2.5% |
| DDoS protection** | 0% | 0% | 0% |
| No high/critical CVEs*** | 77.4% | **77.0%** | **77.5%** |

*For technical reasons, the CMS version for each website could not always be identified.
**We only detected the use of Cloudflare, Google Cloud, or Deflect for DDos protection, three solutions offered for free to civil society but that do not together constitute an exhaustive list of DDoS mitigations.
***This number is calculated by querying the Shodan API (https://shodan.io).

In Table 4, we break down our Palestinian CSO sample by region. Here we find that Palestinian organizations based in (East) Jerusalem score better than those in the West Bank, which in turn outperform organizations in Gaza – an ordering that certainly tracks the economic fortunes of those three regions. Together, Tables 3 and 4 are broadly consistent with the interpretation that better resources lead to better security.

The security loopholes in question, however, can be patched for free. For example, failure to encrypt web traffic is not the result of pecuniary limitations. On the contrary, the HTTPS protocol has been around since May 2000,[67] and in 2012 the Let's Encrypt project was started to make HTTPS deployment a free and fairly seamless process.[68] Indeed, several Palestinian websites we scanned (including Bir Zeit University's website) evidently responded to this drive, as can be ascertained from their website security certificates. Similarly, DDoS protection through Cloudflare, Google Cloud, and Deflect, is offered free-of-charge for civil society organizations. Updating WordPress and other CMSes is likewise free, and there exist free updates (or free alternatives) to all of the other outdated software running on Palestinian CSO web servers. If financial constraints are indeed to blame, it cannot be the solutions themselves but perhaps the cost of hiring staff or consultants with the requisite skills that proves prohibitive.

[67] https://tools.ietf.org/html/rfc2818.
[68] https://letsencrypt.org/.

Finally, one might speculate that Palestinian CSOs are insecure because they are not as yet engaged in politically contentious action, and therefore see no need to protect themselves. This would echo, for example, the 'security by obscurity' argument advanced in McGregor and Watkins (2016). This also relates to the question of financial constraints: if a resource-constrained organization has little reason to expect cyberattacks, it might very well de-prioritize cybersecurity in its budget decisions. Our web scans cast doubt on this explanation, however. Firstly, the cross-regional comparison in Table 4 runs contrary to this logic. If one had to rank these regions in terms of intensity of Israeli repression, Gaza would be the most repressed and Jerusalem the least. Gazan organizations should therefore be the first to anticipate hostility and the first to take security precautions, but instead we find they are the least prepared while Jerusalem is the most. Our web scan of BDS-affiliated organizations in Table 1 adds further doubt. BDS-affiliated organizations have good reason to anticipate hostility, and yet their web infrastructure appears to be no more prepared for attack than 'ordinary' Palestinian CSOs. Indeed, over five years since the BDS movement's main website suffered a DDoS attack, we find that just 9.6% of BDS-affiliated organizations have availed themselves of DDoS protection.[69] Only a quarter of BDS-affiliated organizations run websites with up-to-date software. And the websites for one in five organizations are hosted on web servers running out-of-date software for which high/critical vulnerabilities are publicly known. The decision to openly engage in contentious political action, it would seem, does not prompt these organizations to adopt a higher degree of security vigilance. That many of these BDS-affiliated organizations are located in economically stable countries only adds to the puzzle of their insecurity.

What, then, explains the insecurity we observe? Two possibilities present themselves, which could form the premise of interviews in follow-up studies. Firstly, as suggested by an anonymous reviewer, there may be a prevalent lack of digital awareness or literacy, such that CSOs are simply unaware their web infrastructure is vulnerable. The definition of digital literacy has evolved over time, from the ability to understand information with the help of computers to a multidimensional definition including a combination of competences. Previous research from other contexts suggests that educational attainment and income help determine digital literacy, which could potentially explain the digital insecurity of Palestinian civil society.[70] On the other hand, Palestinians have long been aware of Israel's surveillance efforts, most notoriously their tactic of leveraging Palestinians to inform on each other.[71] While we find it implausible that Palestinian civil society failed to anticipate that surveillance might also have a digital dimension, clearly lack of digital literacy would make it hard to thwart such digital surveillance.

Alternatively, two readers of this paper have advanced a second explanation, in which Palestinians recognize the risk of digital surveillance but regard any effort to resist it as futile, in view of the prowess of their adversary. This 'rational fatalism' explanation has been advanced in other contexts, and it resonates with what we know anecdotally.[72] Clearly, however, neither one of these theories can be firmly established without follow-up interviews with the organizations themselves.

---

[69] eQualitie, "Deflect Labs Report #2 : Botnet Attack Analysis of Deflect Protected Website bdsmovement.net", (2016) available from: https://equalit.ie/en/deflect-labs-report-2.

[70] Nataša Urbančíková, Nataliia Manakova, Ganna Bielcheva, "Socio-Economic and Regional Factors of Digital Literacy Related to Prosperity," *Quality Innovation Prosperity*, 21, p. 124-141 (2017).

[71] See Bergman (2018), among many other examples.

[72] Xie, Wenjing, Amy Fowler-Dawson, and Anita Tvauri, "Revealing the relationship between rational fatalism and the online privacy paradox," *Behaviour & Information Technology* 38, no. 7 (2019): 742-759.

**Concluding remarks**

Why, in the face of a formidable cyber adversary, and with a long history of being the targets of surveillance and repression, do Palestinian CSOs (and their foreign, BDS-affiliated allies) fail to take basic cybersecurity precautions? Our essay offers no clear answer but articulates this question pointedly for future research. Resource-constrained organizations cannot treat everything as a priority, and cybersecurity may up until now have been something of an afterthought. But with the collapse of the Oslo process, Palestinian CSOs and their allies appear to be emerging once more as the vanguard of the Palestinian struggle at a time when cyber attacks against civil society are on the rise around the world. The ability of the Palestinian movement to plan and act clandestinely will be key to achieving the power shifts requisite for leveraging a just peace for all. Cybersecurity is an important part of resisting surveillance and ensuring the movement's integrity. In this paper we scripted a web scanning tool to gather security data on the websites and web servers of Palestinian CSOs. Our dataset suggests that Palestinian CSOs and their allies in the BDS movement exhibit substantial lapses in their cybersecurity posture. While this paper merely articulates the insecurity puzzle, it is clear that the answer(s) must be sociotechnical, beyond the bounds of computer science, and in the ken of sociology and political science. It is true, of course, that cybersecurity vulnerabilities are typically just 'bugs' in computer code, and that updating the software to eliminate these 'bugs' is likewise a mere technical exercise. But it should be clear at the end of this paper that the mere existence of a software update hardly guarantees it will be taken onboard; the mere existence of encryption hardly guarantees it will be used; and so on. Making sense of the internal calculus of civil society organizations on matters of cybersecurity, and indeed security more generally, should be a priority for future research.