POLICY BRIEF | CIVIL SOCIETY

Harnessing Open-Source Intelligence for Palestinian Liberation

By: Tariq Kenney-Shawa · May, 2023

Overview

Open-source intelligence (OSINT) is revolutionizing the flow of information across the globe. Through a process of collecting, analyzing, and sharing publicly available content online—including cellphone videos, social media posts, and satellite images—OSINT analysts are exposing critical intelligence once monopolized by state authorities. From Syria to Ukraine, OSINT is used to uncover war crimes and human rights violations that might otherwise remain obscured. Against the backdrop of declining trust in media and government institutions, along with the growing threat of mis and disinformation, OSINT is proving to be an increasingly valuable tool in facilitating transparency and objectivity.[1]

However, despite the ostensibly accessible and democratized opportunities OSINT provides for sharing information, the benefits of the burgeoning industry do not impact everyone equally. For Palestinians, the rise of OSINT has come at a cost. This policy brief contextualizes the Palestinian struggle for liberation amid the global rise of OSINT. In doing so, it explains how OSINT has been leveraged both as a liberatory tool to hold Israel accountable for its war crimes and human rights

violations, and as a means of further oppression by promoting false Israeli narratives. While innovations of the digital age have exposed state violence, these technologies have also been co-opted by the same repressive forces. This policy brief recommends several steps that Palestinians, their leadership, and their allies should take in order to harness OSINT's potential as a tool for liberation and mitigate the risks posed by those determined to weaponize it.

Historical and Global Origins of OSINT

While OSINT has reached new heights in the rapidly evolving digital age, it is not a recent phenomenon. In the aftermath of Japan's 1941 attack on Pearl Harbor, the US established the Office of Strategic Services (OSS) to bolster more traditional intelligence collection. At the time, the OSINT process looked similar to what we see today, although far more painstaking. OSS analysts meticulously dug through newspaper clippings and poured over grainy images of enemy formations in search of critical intelligence. While OSINT took a backseat to more mainstream intelligence services, it has consistently provided accessible means of discovering and sharing information typically considered off limits to the general public.

It was the birth of citizen journalism and the social media generation—amid Iran's 2009 Green Revolution and the 2011 uprisings across the Middle East and North Africa—that brought OSINT back to the fore. As protesters took to the streets across the region, millions resorted to social media to organize, and OSINT analysts and citizen journalists broadcasted developments to the world. Likewise, when uprisings were suppressed by authoritarian states, like Syria and Libya, the constant flow of photos, videos, and satellite images allowed for near real-time updates from the ground.

OSINT has since demonstrated its value in investigations across the globe. Bellingcat, a collective of independent researchers and citizen journalists, exposed

Russia's role in downing Malaysian Airlines Flight MH17 over Ukraine in 2014 by analyzing call records and identifying Russian-backed separatists. In 2017, Human Rights Watch used satellite imagery to document ethnic cleansing in Myanmar. More recently, the visual investigations team at The New York Times uncovered and exposed the Russian army unit responsible for the massacre of Ukrainian civilians in Bucha with similar techniques.

The decentralized nature of the OSINT process offers a potentially unique opportunity for the marginalized and oppressed to challenge the narratives presented by governments and mainstream media in pursuit of truth and justice. However, while OSINT sharing gives journalists unparalleled insights from the ground and provides activists with new tools for accountability and mobilization, authoritarian regimes are quick to co-opt the new technologies for their own repressive purposes. Colonized Palestine is a case in point.

OSINT in Palestine

A Tool for Liberation

On May 11, 2022, Israeli forces shot and killed renowned Al Jazeera journalist Shireen Abu Akleh while she was reporting on their raid in the occupied city of Jenin. News of Abu Akleh's assassination, along with footage of the moment Israeli forces opened fire, spread rapidly across social media, eliciting shock and outrage across a region that knew Abu Akleh as a household name. Witnesses—including journalists who were at Abu Akleh's side when she was killed—reported that Israeli soldiers targeted them despite their clearly marked "PRESS" vests. Israeli authorities immediately denied responsibility, with then Israeli Prime Minister Naftali Bennett attempting to pin the blame on "armed Palestinians."

As eyewitness accounts began emerging and footage of the shooting circulated on social media, OSINT analysts across the globe combed through a deluge of

evidence in an effort to hold Abu Akleh's killers accountable. By geolocating the exact positions of Israeli soldiers during the raid using footage obtained from those on the scene, Bellingcat investigators determined that the bullet that killed Abu Akleh was fired by an Israeli soldier. The New York Times—which also leveraged spatial analysis, eyewitness accounts, and photos to rule out the possibility that Palestinian resistance fighters could be blamed—reached the same conclusion. A joint report by Al Haq and Forensic Architecture further validated these accounts by drawing on community access to confirm Israeli culpability—a conclusion that has since been corroborated by the UN, Al Jazeera, and even the Israeli military, albeit reluctantly.

Prior to the resurgence in OSINT, widespread recognition of the truth surrounding Abu Akleh's murder would have rested on the outcome of an Israeli investigation of its own military. Today, OSINT gives Palestinians an invaluable tool: the joint investigation carried out by OSINT teams around the world into Abu Akleh's murder proved a remarkable feat considering Israel's ongoing violations of Palestinians' digital rights and its crackdown on human rights groups.

However, glaring issues continue to put OSINT's liberatory potential at risk. Firstly, the investigation into Abu Akleh's murder showed that Palestinians continue to depend in large part on the good will of OSINT analysts abroad who enjoy unrestricted access to the online infrastructure on which they depend—infrastructure often denied to Palestinians. Secondly, Israeli OSINT analysts are attempting to suppress efforts to expose the truth by serving as purveyors of hasbara—Israeli state-led propaganda aimed at concealing Israeli crimes and distorting the reality of its military occupation and apartheid policies.

A Tool of Oppression

Over recent years, anonymous OSINT accounts such as Aurora Intel, Israel Radar, and ELINT News have cultivated large followings with their coverage of security

developments across colonized Palestine and the broader Middle East. Among their followers are journalists, DC-based analysts, and policymakers alike who regularly quote and re-share their posts to their respective audiences. However, many of these accounts source much of their information uncritically from the Israeli military, overreporting acts of armed resistance by Palestinians, and underreporting more pervasive Israeli structural violence. As a result, instead of the objective sources of information these accounts claim to be, they end up propagating Israeli hasbara, distorting the public narrative, and covering up the regime's war crimes.

One of the most prominent of these OSINT accounts is Aurora Intel. Founded in October 2018, Aurora Intel claims to be dedicated to "providing up to date news and intelligence to the masses." Since then, three anonymous contributors—"David," "Adam," and "Knish"—have provided nearly 24/7 coverage of colonized Palestine and the region from the UK, Canada, and Israel. As the Israeli regime launched its assault on Gaza in summer 2022—killing at least 49 Palestinians, including 17 children—Aurora Intel joined the torrent of OSINT accounts churning out updates on operational developments in nearly real time.

Emanuel Fabian, a former OSINT analyst-turned-journalist at the Times of Israel, is one of Aurora Intel's most frequently cited sources. On August 6, 2022, Aurora Intel and Fabian simultaneously reported that an airstrike in Gaza's Jabalia refugee camp had killed four children. As news of the strike spread and public outrage intensified, Israeli occupation forces immediately attempted to deflect responsibility. Without questioning or verifying the Israeli narrative, Aurora Intel and Fabian shared footage and infographics produced by the Israeli military that purportedly showed failed rocket launches by the Palestinian Islamic Jihad movement as evidence that Israel was not behind the civilian casualties.

Several days later, Israeli occupation forces acknowledged their responsibility for

a separate airstrike near Jabalia that killed five Palestinian children. However, neither Fabian nor Aurora Intel reported on the attack, despite having previously shared unconfirmed Israeli military intelligence that blamed Islamic Jihad for the civilian casualties. When questioned as to why a potential war crime acknowledged by Israeli military officials did not warrant mention, Fabian prevaricated, insisting that he could not share the news because the event was "still under investigation."

The inaccurate, biased reporting we see from accounts like Aurora Intel and analysts like Fabian are not an aberration. In fact, they are indicative of a wider, organized network of Israeli and pro-Israel OSINT analysts who operate as uncritical conduits of Israeli hasbara. By amplifying certain stories while ignoring others, regurgitating Israeli military talking points, and outright disregarding developments that reflect poorly on the Israeli regime, these analysts are in effect whitewashing Israeli war crimes.

Furthermore, many OSINT accounts are anonymous, making it impossible for their followers to independently verify their technical expertise or identify underlying biases. As a result, it is unsurprising that these ostensibly impartial sources of information do not add to a more comprehensive understanding of the roots of violence in colonized Palestine—the Israeli regime's interwoven systems of settler colonization, apartheid, and occupation.

Palestinians Under Digital Occupation

In theory, Palestinian OSINT analysts should be able to counteract Israeli disinformation campaigns by presenting the truth to a global audience. Indeed, one of the most appealing aspects of OSINT is that it permits just about anyone with internet access, situational knowledge, and training in open-source research techniques to participate in collective information verification processes. But under the Israeli regime's brutal military occupation, even life on the internet for

Palestinians is characterized by suffocating surveillance and obstructive barriers to access. Indeed, the Israeli regime took complete control of Palestinian information and communications technology infrastructure as early as 1967. Since then, it has controlled digital life in Palestine, preventing access to network technology, denying import requests for new telecommunications equipment, and closely surveilling online activity.

In addition to restricting access, the Israeli regime destroys critical infrastructure needed for basic energy resources, including electricity. In 2014, it bombed Gaza's only functioning power plant, plunging its two million residents into an energy crisis that persists to this day. Although the power plant has since been partially restored, it is incapable of providing energy to sufficiently power the besieged enclave. Under Israel's suffocating blockade and collective punishment tactics, Palestinians in Gaza are left to cope with daily rolling blackouts that often render it impossible to keep refrigerators running, let alone access the internet for extended periods of time.

When Palestinians do get online, internet connections are often excruciatingly slow. Indeed, Palestinian telecommunications networks in the West Bank have struggled to keep up on 3G since 2018, while Gaza still depends on an even less reliable 2G network. In July 2022, US President Joe Biden announced that the White House would work with Israel to bring 4G services to the West Bank and Gaza in 2023. However, almost a year since the announcement, no progress has been made. Slow download speeds and spotty internet connections force many Palestinians to buy Israeli SIM cards to access faster networks. While this does improve internet access for those who have the means, it only exposes Palestinians to heightened surveillance by the Israeli regime. Ultimately, under Israel's digital occupation, Palestinians simply cannot participate in an OSINT revolution that is entirely dependent on reliable and fast internet access, and the free flow of information.

What is more, Israeli occupation forces regularly target Palestinians for recording and sharing information that may implicate them in war crimes or human rights violations. In November 2022, they shot and killed Mufid Khlayel as he filmed Israeli soldiers firing live ammunition at Palestinian youth in Beit Ummar in the southern West Bank. Later that month, they arrested Palestinian activist Issa Amro after he posted footage showing an Israeli soldier throwing an Israeli activist to the ground and repeatedly punching him in the face in al-Khalil (Hebron). And in May 2021, Hazem Nasser, a photojournalist for Palestinian television network Falastin Al-Ghad, was interrogated and threatened by Israeli soldiers for filming settler attacks and police brutality in Jerusalem.

Since 2020, Israel has imprisoned at least 26 Palestinian journalists throughout the West Bank, charging many of them with "incitement" for merely documenting the events around them. Last year, the total number of Palestinian political prisoners reached 4,760. Many of them report being detained and interrogated for posts such as sharing photos of Palestinians killed by Israeli forces on Facebook.

While Israel's digital occupation has failed to deter burgeoning Palestinian-led OSINT initiatives outright, it has severely hampered their capabilities. For example, in the summer of 2021, Palestinian human rights organization Al Haq announced the establishment of a Forensic Architecture Investigation Unit that leverages OSINT techniques to monitor Israeli human rights violations. Their team later produced the aforementioned groundbreaking report into the killing of Shireen Abu Akleh that utilized special analysis to effectively recreate the moment journalists came under fire by Israeli forces.

In August 2022, Israeli occupation forces invaded Ramallah under the cover of night and raided the offices of Al Haq, along with five other human rights organizations that former Israeli defense minister Benny Gantz designated as "terrorist organizations." EU member states, UN experts, and dozens of human rights organizations rejected the supposed evidence Israel cited as justification for

the designations and raids; however, Israeli occupation forces doubled down on their threats to human rights organizations and staff throughout the West Bank. Unsurprisingly, the more effective these organizations become at exposing Israeli crimes, the more they become a target of Israeli retribution.

The Israeli regime is not alone in censoring Palestinians online. A September 2022 investigation by the Intercept found that Facebook and Instagram blocked or restricted posts and accounts that shared footage of the Israeli regime's May 2021 airstrikes on Gaza and attacks on Palestinians in the West Bank. Social media companies attempted to blame the mass censorship on glitches in artificial intelligence software; however, activists pointed out that Facebook regularly moderates content at the behest of governments.

In fact, Israel has its own government agency dedicated to submitting censorship requests. Its cyber unit, which operates out of its State Attorney's office, flags social media posts and requests their removal. According to its own data, 90% of these requests are granted across all social media platforms. High-ranking Israeli officials, including former defense minister Gantz, have gone as far as personally urging Meta and TikTok executives to moderate and censor social media content that is critical of Israel.

The Israeli regime's coordinated campaign against social media companies is difficult to withstand, and this is exacerbated by the complicity of Palestinian leadership in digital violations. As a result, Palestinians cannot exert legal or diplomatic pressure on social media companies, nor sovereignty over their digital infrastructure. Furthermore, the Israeli regime's highly developed technology sector has given it valuable soft power and an unparalleled relationship with leading social media giants. This means Palestinians must once again rely on the international community to hold Israel accountable for censorship and privacy violations.

What Needs to be Done

The rise of OSINT presents Palestinians with a unique conundrum. On the one hand, it provides relatively accessible and low-cost tools to document proof of Israeli regime war crimes and human rights violations that would otherwise go unreported. On the other hand, Palestinians are victims of the very technology they hoped would help them. By actively obscuring Israeli war crimes and fueling narratives that misrepresent the reality of Israel's occupation, Israeli analysts and their supporters have co-opted OSINT, transforming it from a tool of objectivity to one of distortion. Furthermore, Israel's digital occupation and constant surveillance often prevents Palestinians from dispelling Israeli disinformation.

OSINT alone will not stop Israeli war crimes and human rights violations, nor ensure accountability. However, by exposing Israel's crimes to the world, OSINT can be used as a liberatory tool in the pursuit of transparency, deterrence, and justice. Despite the many obstacles Israel has erected, OSINT has already served the Palestinian cause and will only play an increasingly important role in collective efforts to hold Israel accountable. However, without concerted efforts by the international community, technology companies, and activists to ensure equal internet access, combat disinformation, and challenge authoritarian surveillance, OSINT risks being further used as a tool of oppression.

Fundamentally, Palestinians should be able to access the internet reliably wherever they are. There are currently no international treaties or laws that explicitly affirm access to the internet as a human right. Yet, the US and several countries throughout Europe have domestic laws that do. Human rights activists and organizations, Palestinian leadership, and UN member states must support the official establishment and ratification of internationally recognized laws—like the 2021 UN Resolution on the Internet—that enshrine access to the internet as a human right. They should leverage these laws as a framework to demand the

Israeli regime relinquish its control over Palestinian internet infrastructure.

Furthermore, Israel must be held accountable for targeting reporters, citizen journalists, and human rights groups. Activists in the US should contact their representatives to demand the passage of HR 9291, which calls for an investigation and report on Israel's assassination of Shireen Abu Akleh. Voters in the EU should also call on their representatives to demand Israel cease targeting Palestinian human rights organizations with false accusations of "terrorism." In the absence of action in this regard at the state level, advocates should coordinate efforts with organizations like the Committee to Protect Journalists in calling for accountability and preparing Palestinian journalists with protective tools and training.

Finally, there are steps that can be taken immediately to empower Palestinians in the face of Israel's tightening digital occupation. Palestinian OSINT analysts and citizen journalists should be given access and funding for training and digital security courses that will allow them to more effectively leverage OSINT collection methods towards human rights, while maintaining their own safety and security. Organizations like Bellingcat and the Atlantic Council offer free or low-cost courses that have proven to be immensely valuable as foundational resources.

Advocates should also support Palestinian-led OSINT initiatives like the Al Haq and Forensic Architecture lab with additional funding and resources. Emerging applications like Sourceable are aimed at empowering citizen journalists with tools to immediately verify footage, photographs, and other open-source evidence in order to directly connect them with media and human rights organizations around the world. Deploying these tools in Palestine would enhance the flow of information, reduce the adverse impact of disinformation, and protect Palestinian citizen journalists from retribution by Israeli regime forces.

1. *To read this piece in French, please click here. Al-Shabaka is grateful for the efforts by human rights*

advocates to translate its pieces, but is not responsible for any change in meaning.

Al-Shabaka: The Palestinian Policy Network, is an independent, non-profit organization. Al-Shabaka convenes a multidisciplinary, global network of Palestinian analysts to produce critical policy analysis and collectively imagine a new policymaking paradigm for Palestine and Palestinians worldwide.

Al-Shabaka materials may be circulated with due attribution to Al-Shabaka: The Palestinian Policy Network. The opinion of individual members of Al-Shabaka's policy network do not necessarily reflect the views of the organization as a whole.