AI, Surveillance and Data Colonialism in West Asia: Algorithmic Extraction and Geopolitical Vulnerability

*Alam Musheer[*] and Zainab Khan**

Abstract

West Asia faces dual surveillance threats. Multinational tech corporations extract behavioral data from hundreds of millions of residents. State actors weaponize algorithms to target populations during conflict. This research shows how surveillance reshapes power dynamics across the region. Drawing on data colonialism theory, documented cases from Palestine, Syria, Yemen, Lebanon, and Iraq demonstrate specific mechanisms of algorithmic surveillance that create asymmetric vulnerabilities. Facial recognition systems, content moderation algorithms, NSO-type spyware, and predictive enforcement tools let external actors monitor and influence West Asian populations with no legal constraint. Surveillance in West Asia isn't just privacy invasion. It's structural extraction that enriches foreign corporations while weakening regional sovereignty and enabling conflict escalation. The paper proposes policy frameworks for digital autonomy, regional cooperation, and international accountability. The research bridges security studies, technology law, and international relations to show how algorithmic systems become tools of geopolitical control in conflict zones.

Keywords: surveillance, data colonialism, West Asia, algorithms, geopolitics, digital sovereignty, privacy, security, corporate extraction, algorithmic warfare

[*] Research Scholar, Faculty of Law, Jamia Millia Islamia, New Delhi. *alammusheer342@gmail.com*

ISSN: 3108-0405 (O)

Introduction

On August 9, 2021, Israeli forces struck Gaza. Israeli forces attacked Gaza on August 9th, 2021. The use of facial recognition systems to identify civilians in video footage and match them with databases. Use of facial recognition systems to identify civilians from video footage and match with databases. One man had been tracked for weeks by surveillance camera footage, mobile phone location data and algorithmic matching. He was arrested later in the month without a warrant or court order. He was monitored just because of being near suspected members of the resistance group by his family.

This shows the working of surveillance in West Asia. Not some vague privacy invasion, but it's important that they're specifically extracting the information that can lead to conflict escalation and displacement.

There are three levels of surveillance which are interconnected. The big tech companies of the world gather data in huge quantities. Between Palestinians, Syrians, Yemenis, Iranians, Lebanese, WhatsApp records all messages. Facebook knows every pause while you scroll, every like and every share. Smartphones send geographical data to Google, Apple, Amazon. Meta uses 500 million user actions every day in the Middle East. Amazon's regional financial systems, hospitals, government offices are important to them. The Chinese companies Alibaba, Huawei and TikTok run parallel systems. Data is continuously exported, to processing centres in the US and China that are run by corporations, who are responsible to publics in the West Asian region, but not to the public.

This data is then at scale processed by algorithms. They forecast behavior, detect dissidents, categorize populations by threat, and put together targeting suggestions. Content moderation regimes silence Palestinian voices and reinforce Israel’s. Content moderation regimes stifle Palestinian narratives and amplify Israeli perspectives by their opaque training decisions. Predictive policing algorithms are directed at neighbourhoods. These facial recognition systems rank users in order of security threat, according to social networks and

previous behavior. Algorithms are not used to simply process existing data. They actively make what is possible: who can move, who can be heard by whom, which communities are subject to force.

The systems are used in conflict by state and non-state actors as weapons. They carry out targeted killings, forced disappearances, systematic torture, and displacement campaigns with the outputs of surveillance. Devices can be surveilled at a lower level, using third-party tools such as NSO's Pegasus. Collecting and processing with algorithms and weaponizing by states are conducted in parallel with no legal control.

Legislation specific to surveillance is lacking in all West Asian countries except for isolated initiatives in the UAE, Egypt and Israel. International law has no meaningful impact on cross-border surveillance. Multinationals work with terms of service that are incomprehensible to residents, and they can't read or comprehend nor negotiate. The consequence is that the extraction and control are systematic and run with almost complete impunity. There has been no meaningful consent from any citizen of the West Asian country. There was no judicial scrutiny of the legitimacy of the use of surveillance. There are no restrictions on collection or use.

This article delves into two interrelated aspects. First, how surveillance systems pose threats to individual privacy, group rights and state security that are not always experienced concurrently. Second, how algorithmic reliance leads to geopolitical vulnerabilities exploited by external powers in a conflict, and how these external powers can influence the conflict's results in regions without any formal power. The study is based on real examples from Palestine, Syria, Yemen, Lebanon and Iraq. It turns to data colonialism theory and its application to West Asian scenarios, where surveillance and armed conflict, along with the competition of the big powers intertwine, displacing human beings in the process. The paper suggests feasible policy frameworks based on regional digital independence and strategic cooperation, along with international accountability mechanisms, which the countries of the west Asian region can effectively embrace.

In fact, the surveillance problem is not confined to the west of Asia. The distinctive and urgent nature of this intersection is the specific one with the current conflict, humanitarian disaster, great power rivalry and historical disparities in access to and control of technology. This article deals with that configuration and what it portends for the future of the region and the global south in general.

Surveillance Infrastructure in West Asia: The Three Layers

Corporate Extraction Systems: The Data Pipeline

The tech giants are multinational and constitute the backbone of the region's life. Meta has 380 million users in the region, which amounts to almost half of the total population. That's because millions of people have their primary communication channel at the hands of Meta – WhatsApp for messaging; Facebook for community updates; Instagram for information on movements. 90 per cent of all internet searches take place on Google in the region, and it catches each and every research topic, second and every moment of curiosity. Amazon offers cloud infrastructure to the regional financial systems, hospitals, government etc. Loss of Amazon's servers means loss of power grids, loss of patient records, loss of transactions, etc. There are parallel collection systems by Chinese companies such as Alibaba, Huawei, Tencent, TikTok, and Baidu. Telegram-style apps, such as Telegram, are different. These are the electronic nervous systems that make West Asian society tick.

These platforms are able to gather behavioral data efficiently. When someone uses WhatsApp, it saves metadata related to the communication: with whom, when, where, for how long, etc. This is the social graph, NOT the content of the messages. Social graph: Network of relationships. Facebook monitors people's browsing habits by inserting tracking pixels on millions of sites. Google is gathering data from Android devices, search results, watching patterns on YouTube, contents of Gmail. They can describe social networks with great accuracy: who knows what, who trusts what, what communities are linked, what communities are not linked. They trace political orientations by the affiliations people participate in and content they consume. They index

ISSN: 3108-0405 (O)

health data using queries and health conversations. They represent economic vulnerability in terms of shopping habits and employment seeking.

It's an extraction that takes place without any genuine consent from the residents. The terms of service say they allow for collection, but they're written in English, thousands of pages, and can change at any time without notice to users. Palestinian resident on WhatsApp doesn't read the terms of use. She doesn't understand metadata collection versus data encryption. These are the only options she has when it comes to practicality. Her family meets, information passes, and jobs come and go. When someone chooses to not wear a mask, they are essentially choosing social and economic isolation. The data goes out to the processing centers in the US and China. Behavioral data from West Asia travels to VA, CA, Beijing, SHANGHAI. In Silicon Valley and Shenzhen, engineers develop algorithms without any context from or reference to the West. Companies return results to the region by recommending content for citizens to learn, deciding who to credit and who to deny it, and who to target and track with predictive targeting.

In fact it is the actual data colonialism which is going in this present age. Unlike Historical colonialism removed minerals, agricultural products, labor from colonialized lands, transformed them in colonial hubs and gave back manufactured products to the colonized people at a profit to the colonial powers. Data colonialism takes information from the Global South, runs it through US and Chinese tech centers, feeds the algorithmic products that inform decisions into the Global North and China, and centralizes profits in the Global North and China. The mechanism is the same. The geographic location remains the same. The power relations remain the same. The only thing that has changed is the use of resources from minerals to information. Corporate surveillance is harming without government involvement. However, there are many partnerships. US intelligence agencies made connections, both formal and informal, with major tech companies and were able to gain access to data. Microsoft is a cloud services provider to the U.S. Department of Defense. Amazon gives infrastructure to intelligence in the United States. Google offers location information and search history. These are true facts that

have been uncovered in response to FOIA requests and whistle blowing and which are not conspiracy theories. Israel formed a wide-ranging tech tie-up for monitoring. Facial recognition systems are a saleable technology that Israel makes to companies to be used in Palestinian areas. Israeli military and Israeli security funds Israeli surveillance companies. Saudi Arabia and UAE have invested in surveillance via their PIFs. These investments are about corporate and state surveillance. These investments are about the corporate and state surveillance. They fuse together the interests of the corporation and the state.

State Surveillance Deployment: Conflict and Control

West Asian governments deploy surveillance systems tailored to conflict and security goals. The scale and sophistication vary dramatically based on state capacity and resources.

Surveillance systems are used in the west Asian states in conflict and security purposes. The scale and sophistication can range greatly depending on the capacity and resources available to the state. Israel has the most advanced surveillance systems in the Middle East. Facial recognition is used to monitor Palestinians in occupied territories. Biometric databases collect images of the face, fingerprints and iris scans at checkpoints, arrests, and collection. People are tracked by location via cell phone signals, GPS and by passing through checkpoints. The system receives images from CCTV cameras, persistent surveillance by drone and images from the monitoring at checkpoints. Algorithms create risk scores that tell who is free to roam, who has some restrictions, who will get arrested. These scores are self-fulfilling. High-risk people are watched more, and therefore there is more evidence that they are high-risk, and their scores are increased.

There is very little or no surveillance in Palestine because of its infrastructure and lack of resources. The Palestinian Authority carries out some monitoring in the Palestinian Authority territories, mainly on political opposition and security threats. Palestinians are subject to total monitoring by Israeli monitoring apparatus, foreign intelligence agencies watching the conflict and

by international actors. It is completely asymmetric. One population which has advanced surveillance technology against another population which does not have the same technology.

On the other hand Saudi Arabia and UAE spent heavily on surveillance devices to monitor domestic dissidents and regional players. They have facial recognition at airports and in public areas. Mobile networks are directly connected to security agencies, allowing mass surveillance of communications as they happen. These systems are aimed at political opponents, human rights activists, Islamic activists, and anyone suspected of being an Iranian sympathizer. Amnesty International and Human Rights Watch reported systematic surveillance to allow activists to be detained, tortured, and disappeared in both countries.

In the midst of the conflict, Syria's surveillance has rapidly expanded. The government has implemented facial recognition systems in Damascus and in government-controlled areas and is monitoring telecommunications via government-controlled providers. Opposition areas do not have the ability to monitor the situation but have to do so from a variety of angles: monitoring by the Syrian government's intelligence services, by the Turkish army in northern Syria, by Russian troops, and by international actors. In contested areas of Syria, multiple actors of the state are able to monitor a resident, but they are not accountable to any law. The powerful alone can perceive what is being tracked.

Iran uses surveillance systems geared towards Internet control and communication surveillance. The government runs the "National Information Network", a huge infrastructure designed to direct all Internet traffic through it for full monitoring and filtering. The filtering and blocking of communication platforms and websites which are regarded as threatening is carried out in real time by authorities. They observe what VPNs are used and act against users trying to avoid observation. They monitor social media activity and arrest activists based on their online speech and content. Iran's system is unique in its comprehensiveness. It attempts to make internet activity

impossible without state knowledge therefore it has the most advanced surveillance system in the middle east.

Lebanon has a unique pattern of fragmented and scattered surveillance mechanism. Multiple state and non-state actors conduct surveillance in different territories according to their own method and procedure. Hezbollah conducts surveillance in those areas which is under their jurisdiction and control. Lebanese security services conduct surveillance in government areas. On the other hand, Israeli surveillance is also there because of the imminent threat of Hezbollah as anticipated by the Israeli authority. Palestinian and other refugee populations face surveillance from multiple directions. Civilians navigate overlapping surveillance regimes with no legal protection.

Yemen's humanitarian collapse fragmented surveillance capacity again because of its limited resources and infrastructure in terms of wealth and technology. The internationally recognized government conducts limited surveillance. Houthi rebellion conducts their own surveillance in controlled area which is roughly one-third of Yemen's total land area, mostly concentrated in the north and west part of Yemen. Saudi coalition forces conduct extensive surveillance including aerial surveillance, signal intelligence, and human intelligence. UAE forces conduct their own surveillance operations in southern Yemen. Civilians caught between these multiple authorities face overlapping surveillance regimes with no legal recourse. A Yemeni displaced person moving between territories faces surveillance from multiple actors with contradictory goals and no accountability mechanism.

Iraq, still rebuilding after conflict, operates with limited surveillance capacity. But international forces (US-led coalition, Turkish forces, Iranian forces) conduct surveillance in different regions. Sunni majority areas, Shia-majority areas, and Kurdish areas have different surveillance regimes. Civilians navigate this fragmentation with minimal legal protection.

Third-Party Surveillance Tools: Democratizing Surveillance

NSO Group which owns Pegasus spyware is an example of surveillance technology that extends beyond state and corporate boundaries and allows for surveillance without home-grown capacity. NSO is an Israeli company that develops advanced spyware software for government buyers. Upon purchase, Pegasus can take advantage of vulnerabilities in mobile platforms to allow users to gain total control of their device: to listen in on calls, read SMS messages, monitor real-time geolocation, read photos and documents, remotely trigger microphones and cameras for stealthy surveillance.

In 2021, the investigation by the Pegasus Project revealed a pattern of systematic targeting in West Asia based on leaked lists of targets. NSO, the company, has been accused of targeting journalists and human rights activists in Palestine who were documenting Israeli security operations. Saudi Arabia bought Pegasus licenses and employed the tool to spy on activists who have been critical of the regime, including members of families of the murdered journalist.

Jamal Khashoggi who was living in exile. Iran bought Pegasus, and it targeted opposition figures both within and outside Iran. Lebanon specifically attacked civil society activists. Turkey sought to attack Kurdish groups. UAE's attacks on human rights defenders. Targeting wasn't accidental or incidental. Pegasus was bought by governments to carry out targeted surveillance of their political opponents.

According to NSO, tools are only sold in relation to terrorists and criminals who are committing serious crime. As does the government purchaser, who makes the same claims in support of his purchase. The evidence clearly illustrates something else: systematic targeting of political opponents, journalists, lawyers, and human rights defenders. They are not criminals per se. They are individuals which governments wanted to keep an eye on and to control people for political reasons. NSO has sold licenses to at least five governments in the region in West Asia. The company says it has no way to

ISSN: 3108-0405 (O)

influence the use of the technology once sold by the government. This is not a reality, and it is convenient politically. NSO could be able to monitor and track usage patterns and sales. It has chosen not to explicitly.

One type of unique surveillance software that can be used is sophisticated spyware that is available to states and more affluent actors who don't have the technical expertise to create the software themselves: These are known as Pegasus. It opens up the capacity for surveillance among rich countries who have budgets for costly tools. But it centralises power in the hands of the rich.

The Pegasus or like tools are acquired by the states in the region who are fighting for supremacy. All the states of the West Asia have got Pegasus or similar tools. The state can now be held responsible for device level surveillance even in states that do not have highly developed indigenous technical skills. Other tools work exactly the same. Candiru is another Israeli company, which is developing and selling spyware worldwide. The German company FinFisher offers similar products. Russian companies offer SORM compatible systems integrated with telecommunication. Chinese companies are selling facial recognition and mass monitoring systems. The world market for surveillance technology is complex, lucrative, and expanding. West Asian governments are purchasers of capability as well as participants as developers/exporters (such as Israel, UAE, Saudi Arabia).

Algorithm-Driven Geopolitical Vulnerabilities

Predictive Surveillance and Conflict Targeting

Algorithms forecast futures, not merely process data! Predictive policing is a technique used to predict the geographical area where crimes may occur and focus policing there. Feedback loops are formed through over policing because this produces evidence of criminality. Algorithms for counter terrorism identify people who are expected to commit attacks. The algorithms used in refugee aid decisions. Algorithms for refugee humanitarian aid. Predictions shape reality. Predictive systems that identify people as threats, using social networks and behaviour, are being developed by Israeli companies in

Palestinian territories. It identifies family members of suspected resistance fighters and marks them as such. It foresees locations of protests based on previous data on where protests have happened and how social media has been used. It is a family based algorithmic threat assessment detention targeting. The algorithms contain military intelligence security logic that has been developed over years, and they are capable of making decisions without human intervention, 24/7.

The Syrian regime employs the same methods to distinguish opposition protesters from non-protesters in advance of the outbreak of violence. Instead of reacting to protests, they anticipate that they will arise and focus their surveillance on this area. Saudi forces are spying on people suspected of supporting the Houthis in Saudi Arabia. These systems do not require the utmost in accuracy. With an error rate of 70 percent, a system still suppresses political opposition to organizing levels.

It's a plain and straightforward process: The algorithm identifies that someone is a high-risk user, based on the networks they use and how they behave, and they are targeted by security forces, questioned, arrested or even shot. Family and community become aware of the danger. Opposition disappears. The algorithm was successful because it was able to trap would-be dissenters in advance. This is prevention become the control. It sees dissent as threat, not opposition. It does not say organized opposition success is absent, it says repression. Algorithms reinforce this by predicting future state control patterns based on their encoding of past patterns. Arrest history is used in risk assessments in the future. More opposition = more threat = more surveillance = more threat evidence = more threat. The algorithms will be given occupation logic. They utilize automation to control patterns.

Content Moderation and Information Warfare

Meta removes approximately 12 million pieces of content weekly using automated detection. These systems operate at scale making human review impossible. Facebook has three billion users. Even thousands of content

ISSN: 3108-0405 (O)

moderators can't manually review what billions post. Meta deploys algorithms trained to recognize policy violations. These algorithms cascade across billions.

Meta trained algorithms on English-language data using primarily English-speaking moderators.

They encode language biases and Western norms. Arabic content receives different treatment than equivalent English content because the algorithm learned English violations first and retrofitted that learning to Arabic. Cultural context disappears in translation.

During May 2021's Gaza conflict, Meta's systems demonstrated this bias. They removed Palestinian solidarity content faster than Israeli advocacy content. Studies showed Palestinian voices suppressed disproportionately. Hashtags like #GazaUnderAttack got throttled in recommendation algorithms. Palestinian journalists' posts were removed while similar Israeli posts remained. This wasn't intentional policy. It was algorithmic bias from training data and design choices made without Palestinians.

Palestinians use Facebook to organize, coordinate aid, share news, communicate when infrastructure fails. Meta's algorithms suppress this. Israelis use the same platforms. Meta's algorithms amplify Israeli perspectives. Neither results from intentional policy. Both platforms claim neutrality. The algorithms embed asymmetry. Neutrality for English speakers isn't neutrality for Arabic speakers.

Content moderation isn't traditional surveillance of private communications. It's algorithmic governance determining whose speech reaches whom. It shapes what populations learn, what movements organize, what narratives spread. During conflict, this becomes information warfare. Meta shapes conflict dynamics without accountability. A California company determines whose voices Palestinians hear. That's power.

ISSN: 3108-0405 (O)

Data Dependency and Strategic Vulnerability

Foreign companies are crucial to the digital infrastructure of countries in the West Asian region, exposing them to strategic vulnerability. Telecommunications are channelled through the U.S. systems in Pakistan. Palestine's banks are dependent on Israeli infrastructure. Foreign cloud providers are essential to Saudi energy. The government systems in Iraq are completely reliant on foreign hosting. Foreign business control now plays a role in territory control.

Amazon Web Services shuts down tomorrow, and so do critical infrastructure all over the region. This isn't because Amazon wants to weaponise this, it's because concentration brings about consequences. In one company failure, sanctions and business decision, millions are impacted without their choice. In the Syrian 2012 conflict, internet was taken down in the country. This is the subject of disagreement: It was Syria's military action, or an accident, or a technical failure. In either case, Syria didn't have control of its own internet. Political actors in the region and outside used connectivity as a weapon. With the return of internet, other infrastructure providers controlled it. Syria's dependency on the outside of the state obligated external actors to be able to leverage it.

This vulnerability is present in the region. Cloud services run in the US, Europe, or China, are critical infrastructure, including power, water, hospitals and telecommunications. The systems are built with redundancies and resiliency, but there is one basic requirement, that West Asian infrastructure is dependent on foreign companies to continue their service. Countries, that use Amazon Web Services, lose access to AWS if a US sanction includes AWS. A company can decide that a country is violating its terms of service and restrict access to the country. Where a government compels a firm to respect a preference for a particular country, the company will have to decide which country's law to obey. This gives coercive leverage over the other nation. State A can try to limit access to cloud computing to State B. Business disruption is a threat that can be used with negotiations. Competitors can bully companies

to give preference to some governments over others. There is no equivalent alternative for west Asian countries. Independent infrastructure development involves capital, expertise and institutional capacity that are focused in Global North companies. It takes several years to develop and billions of dollars to pay for. It needs to provide training for technical workforce and developing institutional capacity. In most West Asian countries, they do not have the capacity to establish 100% autonomous infrastructure. This vulnerability is being tackled by data localization policies. India requires that certain sensitive information be stored within India. Data transfers from the EU are restricted in Europe. Similar policies are proposed by Palestine.

However, localization policies have their own issues. Localization makes it easier for governments to spy on their own citizens: localized data makes it easier to spy on citizens in their own country. It decreases competitiveness and costs if companies must duplicate infrastructure and services in every country. It opens possibilities for the government to interfere with services. The infrastructure is dependent on countries they cannot control, algorithms which they have no understanding of legislation in other countries and companies' profit motives. This is a vulnerability that is not going away from the digital economy. This vulnerability persists as a permanent feature of the digital economy.

Privacy and Security Implications: The Dual Vulnerability

Privacy Erosion Without Legal Remedy

Privacy in West Asia has collapsed significantly particularly with the advent of advanced technology. Governments around the globe are conducting mass surveillance without paying any attention to privacy laws or meaningful oversight. Corporations extract data under unreadable, non-negotiable terms most of the times without the consent of the users. Individuals left with no practical remedy for state or corporate surveillance.

India's surveillance law provides a regional model. The Indian Constitution establishes privacy as a fundamental right under Art 21 (Puttaswamy v. Union

ISSN: 3108-0405 (O)

of India, 2017). But the application of this Article is only limited to Indian territory and citizens of India. It protects no Indian nationals whose data is stored on US servers or monitored by foreign governments. An Indian citizen's WhatsApp messages on US servers fall outside Indian jurisdiction. An Indian activist monitored by a foreign government has no Indian legal remedy.

There is almost no protection for surveillance under Palestinian law. Palestine cannot fully exercise its sovereignty to regulate digital rights. Under Syrian law, surveillance is not classified as security as it is a civilian protection issue. Yemeni law is split along rival lines. Post-conflict in Iraqi law. Surveillance is regarded as a security affair in Lebanese law. Legal protection related to surveillance in West Asia is very low levels.

Foreign tech companies are not responsible for any privacy violations to the residents of West Asia and cannot be sued by them in local courts. They don't have the power to force governments to disclose surveillance. They are unable to use algorithms to learn about profiling or to debate assessments. There is no remedy under international law. The UN Human Rights Committee's privacy comment (2015) provides principles but no enforcement power. There is no court order requiring Meta to turn over data. No court convicts NSO of targeting individuals. There is no court compensation in relation to surveillance.

Consequences are unequal exposure. The state regularly monitors civilians. Corporations are systematically watching consumers. Individuals can't surveil either. It's not a neutral monitoring. Vulnerability is focused in those who are being monitored, while power is focused in those who monitor. No Palestinian activist can keep track of Israeli surveillance on her. A Syrian oppositionist can't see what the government knows about him. A Yemeni refugee can't know who's tracking her movement.

Security Implications: The Paradox

Surveillance also imposes security risks, in addition to security claims. Governments defend surveillance because it's needed to counter-terrorism. Surveillance systems make targets, however. Identities, locations and networks are documented, and conflicts become personal. Tracked person(s) are the victims of revenge killings. Displacement campaigns are effective: algorithms target opposition supporters and focus force on them. Conflict becomes territorial to eliminating certain people. With Israeli surveillance, precision targeting in the Gaza Strip and the West Bank is possible. Targeting is accurate as they were identified, tracked, networked and threat level assessed by surveillance. Through network analysis, Syrian surveillance was used to detain and torture opposition activists. Saudi surveillance enables arrest of dissidents. Not to cause hypothetical harm, but to cause documented harm by algorithmic profiling.

The advocates don't often recognize the vulnerabilities associated with surveillance. Millions of residents' data are leaked from hacked corporate databases. Out-of-control facial recognition systems enables criminals to monitor anyone. A stolen metadata is used to identify activists for silencing. The loss of governments' control over surveillance systems gives their enemies a tracking capability. NSO has sold Pegasus to governments that have lost control of it. Pegasus was taken, ransomed. Government surveillance systems can be used against dissidents and are now essentially tools of criminal extortion.

Surveillance is a paradox, as it costs to 'secure' and simultaneously it is an insecurity. Residents monitor and forecast lose security. Those with mapped networks become less secure. The algorithms driving the flagging of threats are opaque, which makes those flagged less secure. If they don't know who is watching them, or how their information is being used, they aren't as secure.

ISSN: 3108-0405 (O)

Case Studies: Algorithmic Surveillance in Conflict

Palestine: Precision Targeting and Forced Displacement

Palestinian surveillance is a multi-scalar process. Israeli military has satellites, drones, facial recognition and informants to always keep a watch on Palestinian territories. Palestinian security services carry out the partial surveillance of Palestinian areas under their control. The United States, through formal agreements of cooperation, provides intelligence information to Israel for monitoring purposes, based on satellite data and technical support.

This combination enables precision targeting. Israeli forces on 10 May,2021 attacked Gaza, killing a senior leader of the Palestinian Islamic Jihad. The strike was on the identified location at the identified time. It was preceded by weeks of surveillance including tracking by cell phone, drone and informant information. Target ID, location, tracking, and precision weapons were used to locate and kill the target. The overall tendency is the systematic displacement. Escalating surveillance, restriction and forced displacement occurred in Sheikh Jarrah and other areas. Neighbourhoods are ranked by security threat, and force concentration is justified using algorithms. Maps opposition family networks for targeted detention and harassment for surveillance. Monitoring, restriction of movement and military force impose complete pressure to move out.

Palestinian resistance is based on some limited technology and encrypted communications. The Israeli military experimented with surveillance for decades, even creating military surveillance. Over the years, Israel has created military grade surveillance. Palestinian groups are employing older technologies and operational security. Israeli technological advantage allows them to foresee and anticipate Palestinian movements. Pre-planned protests are broken up by pre-positioned forces. Operations are disrupted by the arrest of key members before they go into action. This is code and data warfare. Surveillance feeds directed at data. Focusing data on military operations. These Operations further enable displacement particularly in those area where the Israeli oversight and surveillance is the most. The effect of this mass Displacement can be observed in the politics. Algorithms are not trigger pullers

ISSN: 3108-0405 (O)

or bombers. They form with the direction and location of the force. They are known for their accuracy which results in more civilian deaths and displacement.

Syria: Mass Surveillance and Humanitarian Displacement

Syria's conflict began in 2011 due to political unrest. The government escalated from police response to systematic surveillance and eventually leads to crackdown and arrest. Syrian intelligence authorities had increased and expanded surveillance systems throughout the conflict. By 2015, government forces surveilled opposition areas through informants, signal intelligence, facial recognition in cities, biometric and by the aid of artificial intelligence.

Surveillance enabled systematic disappearances and detention of the people along with their leaders and social activists. Activists were arrested and detained for uncounted duration without charges or trials. Independent documentation shows tens of thousands disappeared and others were arrested at unknown places. Torture was being used as a systematic tool to crackdown protest. Surveillance has helped the authorities with this precision and accuracy. Without opposition network mapping, arrests couldn't happen systematically. Without telecommunications surveillance, authorities couldn't identify coordination. Without informants, they couldn't locate specific individuals.

As the war progressed, several factions gained monitoring capabilities in various regions. Throughout the war, several groups acquired the capacity to monitor in different territories. Turkish troops monitored Kurdish and opposition groups in the north of Syria. Opposition areas had Russian advisers monitoring them. All parties were monitored by international actors. Syrians in disputed areas were subjected to the watch of several state actors without any legal protections.

The security implications are far-reaching. Syrians are incapable of gathering for political organization without exposure. They are not able to organize

ISSN: 3108-0405 (O)

resistance without risk of arrest. They have nothing to plan a future with, if they don't know who they are being watched by. Opposition movements were always fearful that all their meetings were watched, all their communications were tapped, all their plans were known.

The humanitarian effects are dire. People from a conflict zone fled into the interior, where they were under surveillance. More than half of the population of Syria lived in displacement in 2016.In 2016, more than half of Syria's population was living in displacement, either internally within the country or as refugees. Surveillance by systematic threat (not just direct violence). Those who fled for their lives from bombs also from extensive monitoring that rendered normal life impossible. Students are not allowed to attend University while on a security list. Children are not allowed to be fed by a parent in the case of movement restrictions. In contested territory, families can't keep homes under multiple surveillance directions.

Yemen: Surveillance and Humanitarian Crisis

Yemen is facing the worst humanitarian crisis in the world. More than 300,000 people were killed by violence, disease and starvation as a result of the conflict between government troops, Houthis and Gulf troops. It displaced 4 million internally and generated 3 Million refugees. The disaster is quantified in dead bodies and refugees. Surveillance is a limited aid, limited mobility, impossible choice. The uneven focusing of surveillance technology. The Saudi-UAE coalition forces use advanced technology, such as satellite surveillance, persisting drones, and SIGINT. The capacity of the government forces is constrained. The Houthis have fewer. This asymmetry determines conflict. Saudi troops monitor movements very accurately, forecast supply lines and strike convoys. The opposition forces work in the dark of technicality and are in a quandary, when they know they are being monitored but they cannot do anything about it. Humanitarian NGOs in Houthi regions are subject to surveillance, which limits their mobility and activities. NGOs would not be able to get aid to move without coalitions. They cannot put in place supply chains if they're not monitored. They need to be exposed to organize.

ISSN: 3108-0405 (O)

Surveillance only provides an information advantage, not a security advantage. Saudi forces have been failing to achieve military goals in Yemen over and over, even though they are well-supplied with surveillance. The campaign was a long one without a clear win. However, surveillance meant precision targeting resulting in more civilian casualties. Indiscriminate bombing is less precise than being able to hit targets that are under observation. Precision focuses on fatalities on specific population groups. Humanitarian consequences are dire. Camp residents are monitored and controlled. Aid organizations are subject to restraints on surveillance. Movements are monitored. Surveillance does not stop people needing human aid. It constrains response. If NGO's cannot operate freely, they cannot reach people. If there is a population that can be displaced, they cannot obtain safety. The surveillance system turns into a weapon of conflict, not a tool for security, but a tool for humanitarian. chokepoint.

Discussion: Surveillance as Geopolitical Instrument

These cases show surveillance as geopolitical instrument, not just security technology. It's structural extraction and control, not just privacy invasion. Algorithms let external actors influence outcomes where they have no formal authority.

Traditional geopolitical frameworks inverted. Power used to flow from military might, territorial control, economic dominance. Now it flows from data infrastructure and algorithms. Meta shapes conflict narratives reaching billions. US intelligence surveys populations without declaration of war. NSO enables governments to eliminate opponents. Chinese tech monitors at a large scale. Turkish surveillance reaches neighbors. Iranian surveillance controls its population.

None openly claim this power over West Asia. Meta claims neutrality and infrastructure role. US intelligence claims necessity and legal authority. NSO claims no control over client behavior. Chinese firms claim commercial service provision. Turkish authorities claim security threats. Iranian authorities claim

ISSN: 3108-0405 (O)

national security. But concentrated power is the outcome regardless of claims. Those controlling algorithms shape outcomes for those subjected to them. That's power.

Geopolitical consequences are vulnerability and dependency. West Asian nations can't conduct independent foreign policy with monitored communications. They can't develop opposition movements with tracked dissidents. They can't pursue autonomous security with externally controlled systems. They depend on foreign infrastructure controlled by foreign powers. They depend on decisions made in Silicon Valley, Beijing, Moscow, Tel Aviv about what technology is sold.

This is colonialism without territorial control but with structural dependence. Data flows outward to Global North and Chinese processing centres. Decisions flow inward through algorithms designed without regional input. Profits flow out. Control concentrates. Regional autonomy is getting erode day by day due to this mass surveillance. Actors accountable to West Asian publics don't shape West Asia's future.

Building Digital Sovereignty: Implementable Policy Frameworks

Addressing surveillance requires policy at multiple levels: domestic, regional, international, and technical.

Domestic Policy: Legal Frameworks and Institutional Capacity

West Asian nations need surveillance-specific and strict legislation establishing rights and liability. Indian Supreme Court in 2017 has established privacy as a fundamental right under Art 21 and thereby guarantees its protection from violation at the hand of government. In response to this government has drafted detailed regulation in terms of the Digital Personal Data Protection Act 2023 and IT Amendment Rules, 2026 which further strengthen the right of privacy. This works because constitutional protection and statutory regulation reinforce each other. The protection must specify what

ISSN: 3108-0405 (O)

data collection governments can authorize and also the utility of that data, under what authority, with what oversight, and for what purposes.

Palestine, Syria, Yemen, Lebanon, and Iraq do not have specific surveillance law regulations and frameworks. It takes political will in conflict situations and very few resources to build these. International technical assistance and capacity building would help to facilitate development. A comprehensive surveillance law would define which and how much information is being collected, who can be subject to surveillance, who can have access to surveillance information and under what conditions, judicial review and approval processes for surveillance, the independent bodies that look over surveillance, the lifespan of data before it is destroyed, and what limits would exist for foreign governments accessing citizen information. Further strict compliance to these rules and regulations for all the actors who would be involved in all these acts would meet out the purpose of legislation.

In countries or regions where states have weak capacity, the implementation of these frameworks will not be ideally realised. But they set legal standards to limit government action, set up mechanisms of accountability for violations, and give individuals and organisations a basis for contesting surveillance in court and by law. Legal frameworks matter most when they're weak exactly because they provide leverage for those without power.

Regional Policy: Coordination and Standards

There should be cross-border surveillance standards coordination in West Asian countries. The more countries that enforce a regional accord to ban NSO Pegasus and another spyware, the more effective it will be. A region becomes less appealing to vendors of surveillance equipment if they restrict the use of facial recognition in public areas. If they needed to have their data stored outside the country and limited outside-of-country transfers, they diminished the access to their population's data by foreign governments. Coordination is not enough to achieve complete compliance, but it does increase the cost of

monitoring the vendors and reduces the profitability of regional markets for the monitoring vendors.

Specific regional agreements should include bans on certain types of surveillance, allow certain types of facial recognition use by government agencies, determine where the data of citizens should be kept, the conditions for government agencies to access data from other governments, and how to simplify the process of requests from other governments that are lawful, while also requiring governments to report the frequency of their operations of surveillance. These agreements would be negotiated in bilateral treaty agreements between two countries and multilateral treaties between more. Implementation involves the need for enforcement and definite penalties for infringement It requires the kind of regional commitment that's difficult to achieve when nations have divergent security interests and political conflicts.

International Policy: Binding Frameworks

A new and comprehensive international surveillance law should be adopted by the West Asian countries together. The current legislation which was drafted for different period of time is not adequate for the digital age challenges. According to the ICCPR, Article 17 guarantees privacy in principle, but the protection is left to individual countries. The UN Human Rights Committee has given no guidance on the enforcement of surveillance. The Budapest Convention on Cybercrime was negotiated before mass surveillance became commonplace. These are international documents that give general principles but there are no provisions of any enforcement, penalties, or provisions for mandating compliance.

In West Asian countries there should be collective advocacy for binding privacy standards that set international rules for government surveillance so that countries should be held legally accountable when they violate privacy rights of citizens without reasonable justification in other countries which further can be classified as third country liability.

ISSN: 3108-0405 (O)

There should be a corporate liability for companies if the company aids, in any manner whatsoever, governments or any public authorities to spy on users or helps in violating privacy of users without just cause. The surveillance by the government should be made public, subject to public debate and must be justified by law and should not compromise on the fundamental right of privacy. Further governments should not spy in countries without getting permission to do so from the other country in which it is intended to spy or surveillance and hence it must obey extraterritorial limit. There should be a court that has the power to hear cases of violations of privacy and to order remedies (international tribunal jurisdiction). This means there is a lack of political will in West Asian countries to do this. Global South countries need to coordinate with each other so that they can reach at a substantial result to cope with the challenges and issues of surveillance. It requires willingness to challenge powerful states and corporations. It requires sustained commitment and dedicated will-power over decades to do so.

Technical Solutions: Building Alternatives

There are technical solutions that, when implemented, will diminish the scope of surveillance, but it is easy to impement. When metadata is shared with state actors, end-to-end encryption prevents content surveillance. Open-source software eliminates the need of proprietary algorithms as it is open to everyone to audit and know the vulnerabilities before they are exploited. Regional data infrastructure minimises foreign surveillance by keeping data in the region rather than being transmitted to data centres in the United States and China.

However, there are genuine problems to be overcome in implementation. Governments don't like encryption, because they can't do spying. Open-source software involves having local skills to audit code and maintain the systems without the need for external support. Decades of investment and commitment are needed to develop regional infrastructure.

End-to-end encryption of government communications and key infrastructure, deployment of government systems that are gradually moving to open-source

ISSN: 3108-0405 (O)

software with regional teams source coding, investment in regional cloud infrastructure for government and essential services data storage, training programs to build regional technical expertise in cyber security and data protection, and building regional standards for surveillance-resistant design principles for technology systems would all be appropriate realistic implementations. These all pose both political, technical and financial difficulties. Together they represent steps toward technical autonomy without pretending complete independence is possible.

The Realism of Implementation

In a globalized economy, which relies on connected technology systems, it is impossible to achieve complete digital sovereignty. International infrastructure and international technical expertise will be needed for decades by the countries of West Asia. This dependence isn't unique to West Asia. All parts are dependent on international technology in some fashion. However, the extent of sovereignty is of vast significance. To decide what to rely on and to secure good terms is of course preferable to being made to rely on something by others. Deal making with foreign technology companies and governments is preferable over taking whatever they offer. It is better to have alternatives and redundant systems, than solely other people's systems.

To implement realistically, sustained political will from leadership is needed even in the face of security demands, international support (both material and human) and the willingness of countries that wish to support autonomy to provide technical assistance and capacity development, regional cooperation, and willingness to coordinate across countries with competing interests, long-term perspective and commitment, and a recognition that perfection is not achievable, and incremental progress is more important than waiting for perfection. All these are currently missing in adequate amounts. They will take a lot of effort and mobilization to build. It seems difficult at this moment but with the collective efforts and hard work it can be achieved.

Theoretical Implications: Surveillance and Geopolitical Power

This analysis shows how algorithmic surveillance functions as geopolitical instrument in conflict zones. Existing scholarship and literature emphasize on individual privacy and state security. This work depicts how surveillance is a structural power which enable external actors to influence outcomes.

Data colonialism theory which was developed for African and Southeast Asian contexts also applies directly to West Asia. Mechanisms are almost identical which includes extraction of informational resources, processing in external centres, deployment to shape behaviour. Context differs but structural logic remains the same.

Surveillance is not merely a security tool but can be at any point of time be used a powerful projection. Control over information systems and data in the digital age equivalent to physical control over populations. Surveillance infrastructure is inherently geopolitical and therefore shall be observed through the global lens. It's not neutral technology but a powerful tool which can a used to devastate a nation.

Conclusion: Surveillance as Choice, Not Fate

West Asia faces unprecedented surveillance pressure particularly due to inadequate infrastructure and framework. Multinational corporations extract data from hundreds of millions of the users. State actors thereby use this data to weaponize algorithms. Third-party tools along with the State actors enable comprehensive surveillance and spy. Due to the absence of specific laws all actors are working at their own whim and caprice. External actors control West Asian futures. This appears inevitable, like technology's natural outcome.

Tech companies like other corporate chose profitable extraction of data of its users over protection of their privacy. Governments also chose surveillance over rights as it allows more and accurate control over the citizens. As far as the International law is considered it frequently chose security over privacy the

of people as also intended by the International law. Surveillance firms chose sales over ethics. Specific actors made specific choices with alternatives available. These choices can be contested and changed.

Building digital sovereignty requires acknowledging stakes: not just individual privacy but collective autonomy, not just rights protection but geopolitical power, not just technical security but political self-determination. Surveillance isn't a technical problem. It's political.

West Asian nations have tools such as domestic legislation, regional coordination, international advocacy and technical alternatives. But they lack political will and resources to cope up with the challenges of surveillance. At the same time, one can anticipate that international support, regional cooperation, and domestic mobilization could shift possibilities towards building surveillance system which is beneficial for both government and citizens. This isn't naive optimism but recognition that power shifts when actors coordinate.

Stakes are concrete in nature. Whether Palestinians can organize without targeting. Whether Syrians can rebuild themselves without external constraints and pressure. Whether Yemeni displaced people can survive without surveillance restrictions. Whether regional autonomy is possible in the age of conflict and data warfare. These questions matter for the Global South more than the other part of the globe. How West Asia responds shapes other regions.

Surveillance in West Asia isn't inevitable. Specific actors chose extraction, control, and domination. That choice can be contested. The process is complex and might takes years to come in its intended form. Resources are substantial and hence require proper methods and technique to allocate. Political commitment uncertain which is another hurdle in making a specific framework for Global South. But accepting total surveillance dependence is worse.

ISSN: 3108-0405 (O)

REFERENCES

Amnesty International. (2016). Syria: Extrajudicial executions and enforced disappearances in Syria. Retrieved from https://www.amnesty.org

Amnesty International. (2020). Surveillance of human rights defenders in Saudi Arabia. Retrieved from https://www.amnesty.org

B'Tselem. (2020). Surveillance and control: Israeli surveillance of Palestinians in the occupied West Bank. Retrieved from https://www.btselem.org

Chesney, R. (2018). The state of law and algorithm in the Middle East. Georgetown Law Technology Review, 3(1), 78–104.

Citizen Lab. (2015). Iran's cyber army: The inline censorship system of Iran's staterun internet service provider. Citizen Lab Research Report. Retrieved from https://citizenlab.ca

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1–33.

Cohen, J. E. (2019). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.

Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.

Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.

Davenport, C. (2019). Will the surveillance state recognize Islam? The digital governance of Muslim populations in the Middle East. Surveillance & Society, 17(3/4), 468–488.

Feldman, I. (2020). The Palestinian right to privacy: Surveillance in the occupied territories. Journal of Palestine Studies, 49(4), 42–55.

Forbidden Stories & Amnesty International. (2021). The Pegasus Project: Journalists, lawyers, and human rights defenders targeted with NSO spyware. Retrieved from https://www.forbiddenstories.org

Foucault, M. (1977). Discipline and punish: The birth of the prison. Pantheon Books. Human Rights Council. (2018). Report on surveillance and the right to privacy in the Middle East. United Nations Office of the High Commissioner for Human Rights, A/HRC/39/29.

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. Metropolitan Books.

Gürcan, E. C. (2019). Digital surveillance and algorithmic governance in the Middle East. Third World Quarterly, 40(10), 1845–1862.

Hildebrandt, M. (2015). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar Publishing.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). Digital citizenship and surveillance society: Rights and responsibilities in a digital age. Oxford University Press.

Human Rights Watch. (2021). Saudi Arabia: Sweeping use of NSO spyware against activists. Retrieved from https://www.hrw.org

Iliadis, A., & Russo, A. (2016). Critical data studies: An introduction. Journal of Documentation, 72(6), 967–974.

Kahn, L. M. (2021). Amazon's antitrust paradox. Yale Law Journal, 126(3), 564–907.

Khan, R. (2020). Digital colonialism and data extraction in the Global South. Global South Studies Review, 1(2), 145–168.

Kitchin, R. (2014). The data revolution: Big data, open data, data infrastructures and their consequences. Sage Publications.

Knockel, J., Crete-Nishihata, M., Marczak, B., Senft, A., & Deibert, R. (2015). Iran's cyber army: The inline censorship system of Iran's state-run internet service provider. Citizen Lab Research Report. Retrieved from https://citizenlab.ca

Lessig, L. (2006). Code: Version 2.0. Basic Books.

Lim, S. (2019). Surveillance infrastructure and state control in Palestine. Journal of Surveillance and Surveillance Studies, 17(1), 67–89.

Lyon, D. (2015). Surveillance capitalism: Monitoring and memory in the age of consumption. Policy Press.

Roberts, S. T. (2019). Behind the screen: Content moderation in the shadows of social media. Yale University Press.

Rozenfeld, B. (2022). The Pegasus Project: Israel's NSO Group and the global surveillance ecosystem. Stanford Center on Democracy, Development, and the Rule of Law Working Paper.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.