Between Chinese Surveillance and Israeli Settler Colonialism

Thursday 15 August 2024, by Palestine Solidarity Action Network (Date first published: 7 August 2024).

As Sinophone activists organizing across multiple continents, we are collectively working on educating our communities on Palestinian resistance and the global solidarity movement, as well as calling attention to China's complicity in Israel's occupation, apartheid, and war crimes against the Palestinian people.

Individually, we work in different spaces of Palestine solidarity organizing—on campus, at the workplace, in cities, or via publishing. We aim to provide grassroots education and updates through social media about Palestine solidarity—informing our audience in Chinese about "pinkwashing," colonial feminism, and other relevant topics. We have been translating poems by Palestinians and creating Chinese-language weekly overviews of new boycott or divestment actions from grassroots activists around the world. We are also organizing a campaign against Hikvision, a Chinese state-backed surveillance company complicit in the Israeli occupation, especially in the West Bank.

In this presentation, we will look at some of the connections between Chinese and Israeli institutions, though it's important to note that this overview is not comprehensive.

Ties Between China and Israel

There are extensive economic ties between China and Israel. China is Israel's second-largest trading partner globally and takes the lead in Asia. The Belt and Road initiative has significantly catalyzed China-Israel cooperation. Major Chinese companies like China Railway Engineering Corporation, China Ocean Shipping Company, Huawei, China National Chemical Corporation, and ZTE Corporation are actively investing in Israel, while others such as Huawei, Xiaomi, Lenovo, Geely, and SAIC Motor have set up research and development centers in Israel. Specifically for Huawei, it acquired two Israeli technology innovation companies, HexaTier and Toganetworks, in 2016 for $42 million and $150 million, respectively. In the electric vehicle industry, in 2022 and 2023, the share of Chinese brands in the Israeli electric car market exceeded 50 percent and 60 percent respectively. Chinese car sales outlets abound in Israel, represented by companies like BYD, Geely, Hongqi, SAIC Motor, Chery, and Hozon Auto. In the field of infrastructure, in 2021, the Chinese company Pan-Mediterranean Engineering Company (PMEC) constructed the Ashdod Port in southern Israel. China State Construction Engineering Corporation constructed Haifa New Port Terminal, a vital node port of the Belt and Road, and the first time that Chinese enterprises exported "smart port" technology and management to a developed country. China Railway Engineering Corporation led the construction of the Red Line in Tel Aviv, the first light rail project constructed by a Chinese enterprise in the high-end market of a developed country. The current cooperation between China and Israel involves ports, subways, highways, tunnels and other fields, and the amount of cooperation reaches billions of dollars.

Israel-China collaboration extends beyond traditional industries. For instance, Israel's military laser weapons have found applications in civilian fields such as medical beauty, laser surgery, and laser

beauty instruments. The Chinese company Juva Medical (□□□□) acquired a partial stake in the Israeli company EndyMed in 2014. This acquisition has facilitated the integration of Israeli medical technology into China's domestic home medical aesthetic instrument market. Asia now accounts for a growing share of the market, especially China and South Korea, while a significant portion of South Korean sales are sold to Chinese tourists through the duty-free store channel. Collaboration in the food and healthcare sectors is also flourishing. China's Bright Foods (□□□□) acquired Tnuva, an Israeli food-processing cooperative. Nanjing Xinjiekou Department Store Co.'s (□□□□) operations in Israel include Natalie, Israel's largest private medical care services company, focusing on in-home senior care and telemedicine, along with A.S. Nursing, Israel's fourth-largest in-home care company.

Deep ties also exist between Chinese and Israeli universities and other academic institutions. For example, Tsinghua University and Tel Aviv University established a cross-innovation center and organized summer laboratory training programs at the Technion-Israel Institute of Technology. Peking University and Tel Aviv University jointly enrolled doctoral students. Shantou University partnered with Technion to establish the Guangdong Israel Institute of Technology. These collaborations are some examples of Chinese university students engaging with Israeli institutions as if they were neutral, without recognizing that Israeli universities are complicit in the ongoing genocide, occupation, and oppression of the Palestinian people.

Interconnected Surveillance

We now explore a key method by which China and Israel collaborate to enforce settler-colonialism—through surveillance technology. Amnesty International's 2023 report, "Automated Apartheid," identifies how Chinese surveillance technology, through state-backed companies like Hikvision, targets West Bank Palestinians in everyday life and maintains a dehumanizing environment for them. These CCTV cameras alone cannot serve the purpose of surveillance with full efficiency: they are often embedded in a larger network of physical infrastructure, software, and data systems. For example, Hikvision cameras feed information into □□ (Wolf Pack), a database exclusively of Palestinians from the West Bank used by Israel, including data on permits, family members, addresses, license plates, and whether they are wanted by the authorities or not.

To understand how Hikvision and other Chinese surveillance companies developed their operations, we must look at the role Hikvision plays in maintaining surveillance and policing in the "Xinjiang" region of Northwestern China. Many of these methods are directly inspired by U.S. and Israeli counter-insurgency, and so we see imperialist states using and developing each other's techniques. Hikvision's parent company is the China Electronics Technology Corporation (CETC, □□□□□□□□□□), a significant player among China's central state-owned enterprises and a prominent military contractor.

CETC's involvement in Xinjiang is substantial. It was responsible for building the Xinjiang-wide Integrated Joint Operations Platform (IJOP), □□□□□□□□□, one of the main systems the Chinese Communist Party (CCP) uses for mass surveillance in the region. IJOP is supplied by the Xinjiang Lianhai Cangzhi Company (□□□□□□□□), which is a wholly-owned subsidiary of CETC. IJOP is a system that aggregates and assesses data streams from across the region, tracking patterns in movement and social networks. Specifically, as a Human Rights Watch report ("China's Algorithms of Repression," 2019) shows, the IJOP app is used to fulfill three functions: (1) collecting personal information, (2) reporting on activities or circumstances deemed suspicious, and (3) prompting investigations of people whom the system flags as problematic.

Under the government's "Strike Hard Campaign against Violent Terrorism" campaign (□□□□□□□□□□□□□□□), Xinjiang authorities have collected biometrics, including DNA samples, fingerprints, iris scans, and blood types of all residents in the region between the ages of 12 and 65. The IJOP app contains

facial recognition functionality for checking whether a photo on an ID matches a person's face or for cross-checking pictures on two documents.

They also collect massive amounts of personal information, from the color of a person's car to their height down to the precise centimeter, as well as their address, phone number, and school or workplace. In addition, authorities have required residents to give voice samples when they apply for passports.

All of this data is entered into centralized, searchable databases. Collecting these biometrics is part of the government's drive to form a "multi-modal" biometric portrait of individuals and to gather more data about its citizens. All of this data can be linked in police databases to the person's ID number, which in turn is linked to a person's other biometric and personal information on file.

Xinjiang authorities consider many forms of lawful, every day, non-violent behavior suspicious, such as "not socializing with neighbors, often avoiding using the front door." The app also labels 51 network tools as suspicious, including many Virtual Private Networks (VPNs) and encrypted communication tools, such as WhatsApp and Viber.

When the IJOP system detects irregularities or deviations from what it considers normal, such as when people are using a phone that is not registered to them, when they use more electricity than "normal," or when they leave the area in which they are registered to live without police permission, the system flags these "micro-clues" to the authorities as suspicious and prompts an investigation.

Another key element of the IJOP system is monitoring personal relationships. Authorities consider some of these relationships inherently suspicious. For example, the IJOP app instructs officers to investigate people who are related to people who have obtained a new phone number or who have foreign links. Dataveillance technology helps the Chinese settler-colonial state classify and segment its population. The software automates the detection of watch-listed individuals, placing all populations assessed in a color-coded stoplight system. Automated detection parameters, including discriminatory algorithms such as the "Uyghur alarm," contribute to the systemic ethno-racial profiling of individuals based on the phenotypes of Uyghur faces. IJOP's central system includes multiple sources, including CCTV cameras, some of which have facial recognition or infrared capabilities (giving them "night vision"). The IJOP system also receives information from some of the region's countless checkpoints and "visitors' management systems" in access-controlled communities.

City and town are turned into a maze of digital ethno-racial profiling with the help of checkpoints and thousands of surveillance hubs. Muslims are subjected to frequent ID checks and facial scans, as often as ten times per day at the checkpoints, which are built at nearly every jurisdictional boundary, such as shopping mall entrances, banks, hospitals, schools, walled residential areas, and city boundaries.

At some checkpoints, officers asked Uyghur young people to give them the passwords to unlock their smartphones. The officers then look at the spyware app Clean Net Guard, built by state contractor Landasoft. This app automatically scans smartphones registered to Uyghurs, searching through WeChat (the Chinese version of WhatsApp), Weibo (the Chinese version of X or Twitter), Douyin (TikTok), and other apps looking for thousands of flagged images and text associated with so-called extremist groups, Islam, and Uyghur political history.

In some cases, the security workers plug the phones into digital forensics tools built by companies such as the Chinese digital forensics state contractor Meiya Pico. These tools, referred to in Chinese as "counter-terrorism swords," run on Meiya Pico software that mimicks the systems built by the

Israeli company Cellebrite, which is one of the world's largest retailers of digital forensics tools.

This comprehensive, AI-assisted biometric and digital surveillance system that Hikvision supports, serves to bolster the oppressive "reeducation" system that explicitly targets and detains Uyghurs and other indigenous and ethnic minority groups in Xinjiang.

Even though surveillance is rampant in Xinjiang, it doesn't stop in Xinjiang; instead, it extends far beyond the province; it's a pervasive tool used against any dissenting voices in China. This reality is well-illustrated in Jialing Zhang's 2023 documentary, "Total Trust." The film exposes a digitally-driven authoritarian regime utilizing sophisticated technologies like big data analysis, biometrics, and facial recognition to monitor and control its populace and suppress dissent. Since the "709 Crackdown" in 2015, a nationwide effort to quash dissent, Chinese citizens, including lawyers, journalists, and activists, have faced arbitrary detention, torture, and imprisonment under vague charges of "subversion of state power." Technology firms collaborate with the government, which enables pervasive monitoring of citizens' communications, online activities, and movements through methods like phone tapping, monitoring chat logs, and the use of apps (especially VPNs), as well as the widespread CCTV coverage, and the mandatory use of ID cards to access public services and public spaces such as public transit and malls.

Hikvision cameras are also present in other parts of the world, from Myanmar to the United States. Hikvision is a multinational corporation operating in more than 190 countries. International exports have expanded to the point that they now account for more than 30 percent of its revenue. [1] It sells facial-recognition camera systems more cheaply than Japanese and Euro-American manufacturers. The United States has over 12 percent of all Hikvision camera networks outside China, second only to Vietnam (13 percent). In 2016, a Georgetown University study (*Guardian*,4/8/16) found that police departments were applying facial recognition to databases that were "disproportionately African American," meaning that cops could use facial recognition software to double down on existing targeted practices.

An Amnesty International citizen-led investigation called "Decode Surveillance NYC" found that New Yorkers living in areas at greater risk of racist stop-and-frisk policing were more likely to be exposed to invasive facial recognition technology. In the Bronx, Brooklyn, and Queens, the research also showed that the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras. [2] In 2021, the Surveillance Technology Oversight Project, S.T.O.P., (a group working against surveillance abuse, also part of the Ban the Scan campaign) found over 15,000 Hikvision internet-enabled cameras used by the NYPD in NYC. [3] This is after the 2018 ban of Dahua and Hikvision from being used by federal agencies. Many municipalities in the United States still use Hikvision cameras despite federal bans on Hikvision devices as a by-product of rising U.S.-China tensions. According to contract data reviewed by TechCrunch in May, at least a hundred U.S. counties, towns, and cities have bought surveillance equipment made by Hikvision and Dahua. They are able to do so because federal actions do not apply at the state and city level. [4]

Conclusion

The interconnections between these surveillance regimes show that the fight for abolition is global. Our call to divest from Hikvision is not to exceptionalize China's role in this violence, but to provide a rallying point for Sinophone communities around the world to do our part to resist the role of Chinese institutions in Israeli and other apartheid states. Protests are incredibly difficult in China, but Hikvision's transnational presence means we can identify targets to combat Chinese state-backed surveillance entities across the world. So, sign our petition, and organize people to protest at a Hikvision office to begin encouraging people to connect between different forms of state violence—exposing the collaboration between even rival state blocs. In February 2024, pro-Palestine

activists demonstrated at a Hikvision office in Vancouver. [5] Let us identify their other distribution sites and demand that they drop Hikvision.

Given the U.S. demonization of China, some may feel concerned about why we highlight China's complicity while Washington is the main country directly supporting the genocide of Palestinians with its weapons. We emphasize that our point is not that the United States and China have an equal responsibility in Israeli genocide. We are deeply enraged by an imperialist world order in which Palestine has never achieved justice, while the United States can continue arming the genocide without being sanctioned. We also understand that all businesses, no matter their country of origin, must cease to profit from genocide and occupation. We target Chinese companies not only because many of us have roots in China, but also because we are the direct object of the Hikvision panopticon because of our organizing at home and abroad.

The fight against neo-McCarthyism and Sinophobia in the West need not mean that we should defend another oppressive state. We hope our campaign against Hikvision, which is in continuity with the larger Boycott, Divestment, and Sanctions movement against Western and other companies, encourages a critical stance against all imperialisms. Let us look beyond what state officials are saying, and pay attention to the organic connections among people on the ground. Listen to the voices of solidarity between Palestinians and Uyghurs, and encourage these ties against common structures of repression.

Further Reading

Darren Byler, *In the Camps: China's High-Tech Penal Colony* (Columbia Global Reports, 2021).

Darren Byler, "How China's 'Xinjiang Mode' Draws from US, British, and Israeli Counterinsurgency Strategy," Lausan Collective, Oct. 2, 2020.

"Free Dzungarstan & Altishahr: Resources on Occupied Dzungarstan & Altishahr, aka 'Xinjiang,'".

Human Rights Watch, "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," May 1, 2019.

Promise Li, "China and Israel Have a Long History of Cooperating in Repression," *Jacobin*, Oct. 21, 2023.

Palestine Solidarity Action Network

Click here to subscribe to ESSF newsletters in English and or French.

P.S.

New Politics

https://newpol.org/issue_post/between-chinese-surveillance-and-israeli-settler-colonialism/

Footnotes

[1] Hangzhou Hikvision Digital Technology Co., Ltd., "2022 Half Year Report: January to June 2022." August 13, 2022.

[2] Amnesty International, "Inside the NYPD's Surveillance Machine."

[3] STOP: Surveillance Technology Oversight Project, "2021 NYC Hikvision Camera Census."

[4] Zack Whittaker, "US Towns Are Buying Chinese Surveillance Tech Tied to Uighur Abuses," *TechCrunch*. May 24, 2021.

[5] Jane Skrypnek, "B.C. Group Protests Global Company Supplying Surveillance Cameras to Israel," *Victoria News*. Feb. 27, 2024.