The everywhere border

Digital migration control infrastructure in the Americas

Mizue Aizeki, Laura Bingham and Santiago Narváez

STATE OF POWER 2023

tni
transnationalinstitute

In 2021, José Eusebio Asegurado, a farmer in El Salvador, was arrested by the Salvadoran National Civil Police for 'promoting human trafficking'. The basis for the arrest was a WhatsApp group chat that Asegurado and other migrants[1] were using to coordinate a caravan, which had been infiltrated by a police agent. According to the screenshots used to incriminate him, Asegurado's only participation in the chat was responding 'OK' to a migrant's message that he would be at a meeting point at around 5 o'clock. Police arrested Asegurado at the meeting point, telling him he was 'profiled' as a caravan organiser.[2]

The same day, the Salvadoran police also charged Fátima Pérez, a cook, and Juan Rufino Ramírez, a private security guard, with promoting 'human trafficking' based on messages on a WhatsApp group they had created to coordinate a caravan. Screenshots in Ramírez's case show him giving instructions to the 55-member group to meet at the bus station, and the prices of tickets to Guatemala. The police arrested Ramírez and Pérez the morning they were planning to leave.

These three arrests took place in the span of four hours. The then-US ambassador in El Salvador, Katherine Dueholm, promptly congratulated the General Prosecutor's office,[3] stating: 'I applaud the Salvadoran authorities who are taking action against those who want to deceive citizens with caravans and false promises. They promote only #UnViajeEnVano'—'a journey in vain'.

The arrests and Ambassador Dueholm's praise reflect the critical role of covert surveillance and data-driven 'smart' technologies in US migration-control practices operating deep within countries outside the US. Over the past twenty years, the US (and other wealthy countries) have made strides to externalise border-control regimes well beyond their actual territory. This often involves effectively enrolling agencies in other countries in migrant surveillance, policing, and exclusion.

The new digital infrastructure that enables border externalisation, however, is little understood. This digital infrastructure relies on both military-grade technology built by major weapons manufacturers and Silicon Valley innovation: inter-operable databases that share fingerprints seamlessly between police agencies across borders; biometric collection devices used by Mexican detention authorities to track migrants for US Customs and Border Protection (CBP); social media apps that serve as critical communications networks for migrants and surveillance tools for police; digital ID systems that enable access to essential services, but double as tracking devices.

Infrastructure—digital or material—has real sticking power; that's the point. Once a highway splits a community in half, a new permanence stifles the din of protest, and people move on. We use the term *digital infrastructure* to describe the establishment of a foundation that will be fundamental to how world powers will practise migration control; and, as it embeds itself, increasingly beyond challenge—a unified strategic intervention by powerful countries, with the US coveting the vanguard. While it may look like technological experimentation (like AI-powered robot dogs on the border) or one-off opportunistic data-grabs (like networks of international data-sharing agreements), the growth of digital border infrastructure is *by design.* This is enabled through joined-up digital technologies that settle into the kind of rigid, 'motiveless' permanence granted to other infrastructures, like submarine communications cables, protocols and servers that run the internet, an electrical grid or a superhighway.[4]

The profound implications of new infrastructures persist long after their creation, as is the case for the digital infrastructure deployed to police migrants in the so-called US 'backyard'. Its impacts are frequently rendered invisible. Governments promote border policing technologies as fundamentally safe, humane and non-violent while migrant advocates struggle to make visible the violence on the other side of this unseen 'borderland circuitry'.[5]

The implications range from digitally triggered violence and killings by local police in Central America to actions by the US, its allies and competitors in geopolitical contests over the control of global security. The US government and private industry have worked themselves into a largely covert entrepreneurial frenzy to own and control the migration policing interface of the future. Monitoring and control capabilities—a longstanding and routine part of US aid packages to fight organised crime—both expand domestic spying by partner governments for their own ends and serve US border externalization interests in controlling the movement of people and diverting them away from the US territorial border.

This essay will focus primarily on how digital infrastructure serves US interests. What do we know about this strategy and how it is already affecting mobility and human rights in the region? What are its historical foundations? What challenges lie ahead? It is impossible to answer these questions simply by dissecting the cruelty or provenance of any single technology, system or actor. We first need to understand the transnational motivations driving these incremental, more observable, facts on the ground. We need, in other words, to make visible the invisible digital infrastructure.

Digital infrastructure is key to border externalisation and a rise in unaccountable violence

Understanding border externalisation through the lens of digital infrastructure captures the true scale of border practices envisaged by the US (and its competitors and allies) as well as their envisaged permanence within the future world order. Digital border infrastructure feeds on histories of domination, control and atrocities in the name of transnational 'crime-fighting' projects, setting the stage for tremendous social costs.

First, as to scale, we are witnessing an escalation of US border imperialism and borderland violence[6]—both in terms of geographical reach far into national territories and the further extension of 'policeability' to an increasing number of individuals and groups through this digital infrastructure. This includes anyone an algorithm decides might be 'dangerous', those who might migrate, as well as humanitarian actors, migrant advocacy groups, and aid organisations. Scaling and the rapid growth it engenders is a quintessential property of digital technologies, regardless of their origin or application. The shifts to new targets under digital infrastructure are frictionless compared to earlier analogue-based border policing tactics. Asegurado, the farmer assisting migrants in El Salvador, was swept up in the US border externalisation dragnet with a simple 'OK' on a WhatsApp chat.

Second, as to permanence, advocates of digital borders in national capitals, industry and development agencies embrace the term 'digital public infrastructure' as a brand, to bestow (unearned) trust, normalisation and the inevitability of contested digital tools such as biometric IDs and payment systems.[7] Ceding the privilege of defining 'digital infrastructure' to actors with vested interests in current migration-control practices is reckless. Without a counternarrative that articulates their violent disposition, digital border externalisation tools—including widespread biometrics collection, real-time transaction data-collection in payment systems, and the confiscation of smartphones at the border—can easily be normalised as 'digital public infrastructure', rather than resisted.

The scale and enduring impact of the rapidly hardening digital infrastructure that fuels border externalisation calls for urgent transnational organising. As writers and activists, we have come together to resist the use of digital infrastructure in US migration-control policy in Mexico, Central and South America, and the Caribbean. We have only traces and not the whole picture. Building on the work of others, we weave all this together to show how the fusion of state and digital power to construct digital border infrastructure is neither humane nor safe: rather, it is increasing unaccountable forms of violence.

Convergence: Drugs war, border externalisation, digital infrastructure and the militarisation of US' neighbouring regions

Economic and political initiatives since the 1970s have driven relentlessly towards US investments in more militarised, criminalising, and digitised migration-control practices. Since 9/11, the US convergence of 'national security' with unauthorised migration has fueled an ever expanding border externalisation regime—currently there are 23 CBP offices and 48 ICE offices worldwide[8]—and consequently has provided an especially lucrative market for digital surveillance corporations.[9] Through programmes such as the Mérida Initiative and the Central American Regional Security Initiative, the US has tied aid to countries such as Mexico, El Salvador, Guatemala and Honduras to increased militarisation, policing, incarceration, and migration control.

Yet migration patterns to the US from Mexico, Central America and the Caribbean cannot be divorced from the practices and policies that the US employed for over a century to dominate countries in these regions. Decades of US practices and policies have fuelled economic, political, and environmental instability—key factors that drive migration to the US. Over the past 20 years the number of people migrating from Central America has more than doubled, the largest increases coming from Guatemala, Honduras and Mexico. The US-backed 'war on drugs' in Mexico and Central America has dramatically increased violence and instability.[10] In Mexico, the fight against organised crime has resulted in 350,000 deaths and more than 72,000 disappearances between 2006 and 2021. According to the World Bank, 60% of rural Central Americans live in poverty. While the largest contributors to the climate crisis are wealthy countries, these already impoverished populations suffer the most acute impacts of climate change. For decades, prolonged droughts together with natural catastrophic events such as hurricanes and floods have deeply affected Central America. The number of people facing food insecurity tripled between 2019 and 2021, affecting 6.4 million people. Asegurado, Pérez and Ramírez—like many others—are grasping for alternatives to this intolerable situation.

Rather than acknowledge these underlying causes, the US response has been to extend its border ever further. General John Kelly, former Secretary of the US Department of Homeland Security (DHS), stated, 'I believe the defense of the Southwest border starts 1,500 miles to the south'. Mexico has long been central to the US border-externalisation regime, and digital infrastructure plays an increasingly critical role. Tony Crowder, former director of CBP's Air and Marine Operations, shared Kelly's sentiment 'We have taught the Mexicans how to fish… [but] even though we have all this surveillance capability, we don't have enough, we need more'.[11]

While part of a continuum of US efforts to enlist Mexico in support of its regional objectives, this 'security and rule-of-law partnership' accelerated following 9/11. In 2007, the US shifted the focus of its drug war from Colombia to Mexico, Central America, and the Caribbean. Under this frame of securitisation, the drug war merged with the migrant-control regime. In 2008, the Mérida Initiative was launched—a bilateral partnership between the US and Mexico in the name of the US war on drugs. It initially provided financing for Mexico to purchase equipment for its military and police forces and for intelligence gathering. In 2013, Mérida was revamped to include four pillars, incorporating the creation of a '21st century US-Mexican border, while improving immigrant enforcement in Mexico and security along Mexico's southern borders'. Effectively an extension of US policy, some $3.5 billion has helped shape Mexico's migration-control agenda since 2008.

In 2014, *Programa Frontera Sur* further securitised Mexico's southern border by increasing the migration policing and deportation apparatus. Consequently, Mexico now has one of the world's largest immigration detention systems. Between 2014 and 2017, Mexico deported more Central Americans than the US Border Patrol. Doris Meissner, the former commissioner of the Immigration and Naturalization Service (INS, the predecessor to ICE and CBP), underscored the importance of Mexican migration control, explaining in 2017 the need to look at both US and Mexican data to assess the effectiveness of US border enforcement.[12]

Under these agreements, the US Department of Defense has provided training and sold millions in military equipment to Mexico, including an array of 'smart border' technologies provided by corporations such as Dev Technology, General Dynamics, Amazon Web Services, and NEC.[13] The CBP and ICE have provided training on intelligence-gathering, info-sharing, and migration policing. A key element of US support to Mexico has been to develop an infrastructure to collect and share data—such as biometric and biographical information, and criminal history—in a manner that interfaces seamlessly with US databases.

The digital infrastructure that tracks and catalogues migrants is central to US migration policy in Mexico. The US-backed Instituto Nacional de Migración (INM) strategy relies on this infrastructure as the primary means to control migration rather than sealing Mexico's southern border with Guatemala. Biometric collection is essential to making migrants more legible to the state. In 2011, the US provided four biometric kiosks to Mexico's southern border, and 117 additional biometric scanners the following year. Between 2018 and the first half of 2022, the Mexican government gathered and shared information on over 360,000 migrants in detention facilities.[14] Information from CBP reveals that Mexican authorities shared information from 10,000 humanitarian visa applications with DHS. The release of approximately 1,800 unregistered migrants from a shelter in Piedras Negras was conditional on the registration of their data.[15]

An 'Information Sharing Environment' that includes inter-operable data-sharing systems is central to achieving the objectives of the homeland security state.[16] 'Inter-operability' enables seamless connectivity between police, immigration agencies, foreign governments, and more.[17] Key forms of US-initiated digital infrastructure rely on widespread information-gathering and seamless sharing of data for surveillance across borders.

This vast amount of data-collection and sharing has been fuelled by unleashing the power of the carceral state—including the centrality of the 'criminal alien', 'gang member' and 'drug trafficker' as threats to national security—at all geographic levels of the US migrant-control regime. For example, the Biometric Identification Transnational Migration Alert Program (BITMAP) allows DHS and its partner countries to know where and when an individual arrives in the Western Hemisphere and their travel patterns before they reach the southwest US border. BITMAP is currently deployed to 18 countries, including Mexico. DHS also has a Criminal History Information Sharing (CHIS) programme that allows for the global sharing of biographic, biometric, and descriptive information on individuals deported from the US (e.g. alleged immigration, employment, family, and criminal histories).

The structural criminalisation of poverty in both countries is amplified with CHIS. According to the National Survey of Imprisoned Population in Mexico, conducted by the National Institute of Geography and Statistics (INEGI) in 2021, nearly 44% of the respondents declared having been imprisoned on the basis of false accusations or incriminations. Forty-two percent claimed they had been forced to plead guilty or to incriminate someone else. Nearly half of those who are jailed have not been convicted,[18] and nearly half of all convictions are for theft of under US$100.[19] This is the kind of data that feeds CHIS.

In another example, DHS is developing the Homeland Advanced Recognition Technology System (HART) to replace its current centralised biometric database, IDENT, through a contract with Peraton (a subsidiary of Veritas Capital, a private equity firm). Hosted by Amazon Web Services, HART will enable DHS to aggregate and compare biographical and biometric data on hundreds of millions of people across the globe. This includes so-called encounter data from police stops, facial recognition, DNA, iris scans, and voice prints—usually gathered without the individual's knowledge or consent. The massive HART database draws from widespread biometrics collection in all realms—for example, the US DOS INL's development of integrated DNA databases in Mexico and Central America in the name of combating trafficking or the proposed national biometric digital ID in Mexico. In this way, multiple state initiatives merge, and the power of the state to police, track and control migrants and all people under their watch grows exponentially.

While the Mérida Initiative formally ended in 2019, its approach has been sustained by the Mexican government. In 2021, the Mexican government increased the military by 46% and the National Guard dedicated to stopping migrants by 300%. In July 2022, President López Obrador committed $1.5 billion in smart border infrastructure over the next two years.

For US partner states, any technological and data-sharing channels that are financed and exported to them become assets—not just for monitoring migrants, but to advance multiple agendas of coercive power-building. This infrastructure can therefore end up fuelling violence and criminalisation, undermining the right to asylum, exacerbating inequality, and expanding the power of paramilitaries and the police, while privileging securitised neoliberal and corporate prerogatives.

The geopolitical nature of digital infrastructure

In their research on digital payment systems, Marieke de Goede and Carola Westermeier use the term 'infrastructural geopolitics' to stress the growing centrality of infrastructure to geopolitics and the ways in which US economic power is rooted in financial infrastructures (which, like migration control, are rapidly digitising).[20]

The global financial messaging network SWIFT is an example of infrastructure that is invisible to most people and yet plays a major role, as the writers describe, in reinforcing power relations of the post-war global order in which it emerged. Seventy years after the Second World War and fifty years since SWIFT's establishment, bank messaging routes flow through former colonial capitals and map onto a 'core' of Western countries, leaving large swaths of Latin America, Africa, and the Middle East in a permanent, but effectively invisible, economic periphery. Similarly, digital IDs, social media monitoring and infiltration, and data-sharing platforms are essentially component parts, nodes, or partially visible layers of deeper, longer-term geo-strategic digital infrastructure projects.

Extension of borders through digital infrastructure serves US political and economic goals well beyond the policing of human mobility. Geopolitical contests for control over infrastructures play out across several domains. Military establishments covet 'identity dominance', an objective that drove US forces to gather massive stores of biometric data in Afghanistan and Iraq as a weapon of war.[21] US digital services giants like Amazon and Google mastered 'platformisation' by building e-commerce (digital advertising, search, social media, etc.) infrastructure to dominate the digital economy. Often, public and private-sector interests converge, including in the form of public–private partnerships (PPPs) to build infrastructure. In each case, the true contest among states and corporate giants centres on control over the interface, or the most essential, invisible, infrastructural methods of digital communication and control. As Michael Kwet explains, 'Transnational "Big Tech" corporations based in the United States have amassed trillions of dollars and gained excessive powers to control everything, from business and labor to social media and entertainment in the Global South. Digital colonialism is now engulfing the world'.[22] The US quest for domination through externalised migration policing infrastructure goes hand in hand with its geopolitical and corporate designs for economic power.

These forms of infrastructural digital power pose unique challenges for documentation and ultimately for any form of systemic change. Challenges include blurred lines of responsibility, mission, and function; governments and corporate actors are seen or presented as passive conduits or intermediaries in digital public infrastructure; and infrastructures can easily appear to be 'ahistorical' and motiveless. In Mexico and Central America, migration control converges with ongoing US foreign policing operations (such as the war on drugs, and gang wars). We explore the several simultaneous effects of this complex merger: the turn to digital infrastructure; its relationship to violence and human suffering; and its foreclosure of accountability for these harms.

Digital border infrastructure in your phone: Information and Communications Technology (ICT) policing techniques along migration routes

Surveillance infrastructure is tangible in physical migration detention centres and in police arrests: mugshots, cheek swabs, confiscation of the detainee's mobile phone. The deepening integration of daily life, telecommunications and computers open extensive avenues for more covert, opportunistic surveillance of private communications and activity by users who rely on social media, mobile communication and messaging apps. The surveillance of mobile phones and social media ranges from overt disclosure requirements for visa and benefits applications to government listing and tracking of protesters and other 'undesirable' actors. Migrant surveillance is immersed in these control schemes where surveillance technology serves as a silent tool for government violence and repression.

This has had an impact on how migrants travel and keep safe, such as through safety in numbers. Travelling in caravans has therefore become both a survival and a protest strategy: sources of both physical and economic security and opposition to the economic policies that contributed to their displacement. Social media and messaging apps are key tools for the coordination of caravans and for migrants more broadly. Migrants use these tools to identify routes, look for shelter and food, communicate with their support networks, warn each other about risks, and coordinate travel. Governments as well as organised crime understand these dynamics and use these same tools to monitor and extort migrants.

On 5 June 2019, Irineo Mujica, from *Sin Fronteras*—a civil society organisation (CSO) dedicated to the protection of human rights of migrants in Mexico and the US, and which has supported multiple migrant caravans—was arrested in Mexico, falsely charged with human trafficking. Mujica appeared in the CBP's watchlist database published in 2019 that contained photos, names, professions, and other details of journalists, activists, and social media influencers both from Mexico and the US with links to the migrant caravan.

A DHS Office of Inspector General (OIG) report on the database and other surveillance practices found that CBP established electronic alerts (lookouts) on journalists, attorneys, and advocates who were connected by social media to the migrant caravans.[23] Those tagged by the lookouts were constantly flagged for secondary screening when entering the US, and interrogated about their work, organisation, family, education, and political leanings.

The weaponisation of such information had grim effects on the Mexican side of the border. According to *Sin Fronteras* activist Alex Mensing, after the CBP shared information gathered through lookouts with the Mexican government, other members from his organisation who assisted migrant caravans in the same period saw an increase in border scrutiny and death threats. Organising and supporting migrants threatens lucrative operations that depend on the criminalisation of migration across the region. Civil society assistance makes migrants less prone to kidnapping and extortion, which therefore reduces the income for organised crime linked to these activities, and, as a domino effect, bribes to authorities also drop, pitting the collective interests of such groups against activists and those providing humanitarian assistance.

Surveilling anyone who might pose a threat to the system has long been a generalised and systematic form of government control in Mexico. A leaked document from the NSO Group, the Israeli company that created Pegasus, revealed that 50,000 people were possible surveillance targets in Mexico. The list included opposition politicians, journalists investigating government corruption and extrajudicial killings, activists advocating the taxing of sugary drinks, judges, academics, and international experts who investigated the case of the enforced disappearance and extrajudicial killing of the 43 students, among others.

In 2022, mobile phones from two journalists and an activist who investigated abuses committed by the Mexican army were found to be infected with the malware Pegasus. In 2020, the Mexican government sought to create a SIM card registry that would link to the card owner's biometrics and other personal data. This would have intensified government digital surveillance via ICT infrastructure, and was opposed by civil society.

CBP internal documents show that government agencies across the border continually share information about the location of migrants, their origin, and the number of people in each group, even before they start to migrate. In 2018, US DHS agents infiltrated a WhatsApp group of Honduran migrants travelling in a caravan of about 4,000. These policing practices are also being reproduced by the Mexican government.[24]

Impact: Infrastructural violence and accountability deficits in globalised migration policing

Roberto M., a young man in El Salvador, was shot and taken away by police shortly after being deported from the US. The rural police officers who shot Roberto also threatened an eyewitness at gunpoint, telling him that Roberto was a gang member and if he revealed what he'd seen, the same would happen to him. Police in El Salvador receive data on gang-member affiliation from the US, and share these lists with neighbourhood-level police where deportees plan to live. These databases have been found to be problematic and unreliable.[25] Police departments confirmed that this information is used to target people: 'We think that if a person wasn't wanted in the United States, it must be because the deported person is bad'.

Violence can increasingly be tied to digital border technologies, particularly in combination with one another and with physical and environmental realities that envelop them. Studies show the effects of integrated fixed-tower surveillance on migrant mortality rates in Arizona's Altar Valley. Here, digital infrastructure merges with the ineffective yet longstanding US deterrence policy that purposefully makes migration routes more dangerous, on the theory that migrants would not risk the journey. The fusion of technology and policies that inflict deliberate harm produces these predictable results of increased migrant deaths.[26]

The story of Roberto M. and the witness to his post-deportation shooting and disappearance in El Salvador reflects another pattern of violence tied to information-sharing through digital infrastructures. The criminologist Ana Muñiz documents a 'cycle of violent policing, migration, more violent policing, detention, deportation, violent policing, migration, and so on', in which the labels themselves ('criminal alien' or 'gang member') become inescapable vectors of precarity.[27] Such labels channel individuals into a 'sort of statelessness' as constant, quantifiable scapegoats that provide an easy diversion for state security forces and corporations that produce and perpetuate the 'structural causes of violence'.[28]

Digital infrastructure merges not with a physical terrain, but with pre-existing social and political factors that make violence a foregone conclusion. Today's multipurpose digital infrastructure also permits the efficient incorporation of new undesirable criminalised categories, including 'caravan organisers' or 'migration promoters'—as in El Salvador's attempt to reform its penal code, criminalising the 'promotion of migration' on social media.

Challenges and way forward

We are interested in developing deeper knowledge about the political origins of these infrastructures to challenge the violence of global migration control systems. This essay only sets out the field of engagement. Far more collective work is required to document and design models of resistance to meet such challenges.

The diffuse and structural nature of power behind the seemingly ahistorical, and motiveless characteristics of digital infrastructures undermine classic approaches to accountability. Furthermore, the familiar national and international judicial avenues to hold perpetrators of these forms of indirect violence responsible—however imperfect or ineffective they may already be—are exceptionally ill-suited to the conditions at play in the migration policing context specifically, for several reasons.

First, the technologies *in use* such as biometric databases, and the *means of using* civilian technologies like social media and other ICTs, are simply not designed to respect or be held to democratic scrutiny; they are military-grade and converted for use in quasi-militarised spaces, by institutions permeated with military ideology. Nearly a third of CBP personnel previously served in the US military. Biometric surveillance technologies advanced by leaps and bounds within US military operations before being integrated with 'civilian' border policing. Private-sector military contractors play an integral role in this transition.

As journalist Annie Jacobsen documents, as part of the US military biometric data-collection in Afghanistan, Palantir Technologies served as a critical link between US intelligence operations to track and kill military targets and quasi-civilian policing operations like the piloting of rapid DNA samples from migrant families at the US border in 2019.[29] Today, the biometric kits used in Afghanistan, some still storing biometric data collected on the battlefield, are for sale on eBay.

Second, justice and oversight bodies are ill-equipped to serve their intended function in this ecosystem. Within criminal proceedings and investigations, the use of technologies that capture and record evidence of allegedly criminal activity or purport to biometrically match records are extremely difficult to challenge because of their scientific veneer and opaque data-collection and analysis methods, which leaves no practical room to impeach or exclude such evidence. The design of technologies that predetermine risk factors keyed to criminalised behaviour, including migration, contravenes the presumption of innocence. In the civil context, national-level justice mechanisms deny standing to non-nationals located outside the US who are victims of violations linked to digital surveillance.

Finally, there are huge incentives for both state and corporate power to hide violence. The political positioning of 'smart borders' as more 'humane' conceals the state's role in violence and insulates corporations from negative PR or constraints by participating in repugnant markets. Their task is made easy by rendering physical pain abstract rather than affecting real human beings,[30] and features of the data economy like the way corporates have helped the movement towards running government functions like private digital platforms.

Mitigation 'risk assessment' tools like data protection or human rights impact assessments provide cover, favouring the continuation of these business practices because firms undertake them voluntarily and face little or no consequences for a poor risk assessment. Unsurprisingly, these industry-led tools often fail to provide a means for real accountability; they reveal scant information that would be actionable if and when products do cause harm; and the burden of proving rights violations and finding an effective remedy after the fact is shouldered entirely by victims. The interests of powerful actors converge around a web of financial stakes in the system, leading to the aggressive harassment and potential silencing of activists as the case of Irineo Mujica and *Sin Fronteras* illustrates.

We need tools and methods for transnational cooperation to document, gather and share information safely, and organise. Fusing new understandings about how digital power functions within existing resistance movements transnationally, holds potential for challenges to the digital infrastructure of border externalisation.

We are in the initial stages of our collective effort to understand and expose this digital infrastructure. Through this analysis, we can begin to identify the interventions to start to tear it apart and break it down. Transnational organising against tech corporations offers opportunities for shared understanding and meaningful solidarity. This year, organisations in France and Kenya, with support from actors in other countries, sued biometrics giant IDEMIA for its failure to meet even minimum human rights standards of due diligence as it reaps billions in secret border security tech sales to low- and middle-income countries. This emerged from collaborative evidence-gathering and organising across borders.

As the US military establishment recognised decades ago: whoever dominates the field of externalised borders defines 'friend and foe' everywhere.[31] The faster the US establishes economic and political dominance over digital migration-control infrastructure, the greater its security in maintaining global digital power. Digital infrastructure serves multiple purposes at once, but the ultimate geopolitical function is raw, generalised power over global affairs. The tools examined here will 'contain' human life within spaces of catastrophic violence, by design.[32] This specific effect betrays the most fundamental commitments of international human rights and humanitarian law in the face of unprecedented challenges to human survival across most of the world. But this pernicious effect is also ruthlessly beside the point.

In reality, as facets of infrastructural power, the technologies that fix the 'calculation of who must live and who must die'[33] do not do so as an end in itself, but in the service of power and its reproduction in this digital age.[34] In this way the complicity of state and corporate actors in the production of violence is cast in the starkest relief. This geopolitical analysis is our starting point for building resistance towards transformation.

BIOGRAPHIES

Mizue Aizeki is Executive Director of the Surveillance Resistance Lab. For close to twenty years, Mizue has focused on ending the injustices—including criminalization, imprisonment, and exile—at the intersections of the criminal and migration control systems. Prior to the Lab, Mizue was a Senior Advisor at the Immigrant Defense Project (IDP) and the Project Director of the Surveillance, Tech and Immigration Project. Mizue is a co-editor of *Resisting Borders and Technologies of Violence* (forthcoming from Haymarket Books, Fall 2023).

Laura Bingham directs the Temple University Institute for Law, Innovation, and Technology. Prior to joining Temple Law, Laura served as senior managing legal officer with the Open Society Justice Initiative. She established and led a global program on data, technology, and human rights. Since 2017, Laura has taught courses on human rights and forced migration as an adjunct faculty member at New York University's Center for Global Affairs.

Santiago Narváez has been a researcher since 2016 at digital rights NGO "R3D: Red en Defensa de los Derechos Digitales" based in Mexico City where he researches how government surveillance is exercised and its impact on human rights. He has a degree in International Relations and a formation in data analysis.

Endnotes

1 We use 'migrant(s)' to refer to people on the move without differentiating between refugees, asylum seekers or economic migrants.

2 Cáceres, G. and Gressier, R. (2021, 14 May) 'Sting operation against migrant caravan arrests working-class migrants as human traffickers', *El Faro*. https://elfaro.net/en/202105/el_salvador/25479/Sting-Operation-against-Migrant-Caravan-Arrests-Working

3 Johnson, R. (2021, 15 January) 'Aplaudo a las autoridades salvadoreñas que están tomando acción contra quienes quieren engañar a los ciudadanos con caravanas y promesas falsas Solo promueven #UnViajeEnVano', Twitter. https://twitter.com/FGR_SV/status/1350133335549501443

4 de Goede, M. and Westermeier, C. (2022) 'Infrastructural geopolitics'. *International Studies Quarterly*, 66(3): 1–12. http://dx.doi.org/10.1093/isq/sqac033.

5 Muñiz, A. (2022) *Borderland Circuitry: Immigration surveillance in the United States and beyond*. Oakland, CA: University of California Press; see also Mijente, Immigrant Defense Project, NIPNLG (2018) 'Who's behind ICE'. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf

6 This lens also enables us to emphasise the connection to historical antecedents such as physical transit and trade infrastructure 'modernisation' projects, where the link to state violence is indisputable (e.g. railway construction projects and genocide of indigenous peoples in Sonora from 1880 to the 1900s). See Guidotti-Hernández, N. (2011) *Unspeakable Violence: remapping U.S. and Mexican national imaginaries.* Durham, NC & London: Duke University Press. We emphasise that this scale is no departure from the racialised logics that have defined border practices in this region for decades. See Rosas, G. (2006) 'The managed violences of the borderlands: treacherous geographies, policeability, and the politics of race'. *Latino Studies*, 4(4): 401–418. https://doi.org/10.1057/palgrave.lst.8600221

7 See, for example, Shivkumar, G., O'Neil, K. and Nordhaug, L. (2021, 30 August) 'How to bring digital inclusion to the people who need it most'. https://www.weforum.org/agenda/2021/08/4-reasons-you-should-care-about-digital-public-infrastructure/ ('[Digital Public Infrastructure (DPI)] refers to digital solutions that enable basic functions essential for public and private service delivery, i.e. collaboration, commerce, and governance. Think about our existing shared public infrastructure such as roads and education, but online: that's DPI in a nutshell'); Masiero, S. and Arvidsson, V. (2021) 'Degenerative outcomes of digital identity platforms for development'. *Information Systems Journal*, 31(6): 903–928. https://doi.org/10.1111/isj.12351; Massally, K. and Frankenhauser, C. (2022, 3 August) 'The right way to build digital public infrastructure: 5 insights'. https://www.weforum.org/agenda/2022/08/digital-public-infrastructure/

8 Aizeki, M., et al (2021) *Smart Borders or A Humane World*, https://www.tni.org/en/publication/smart-borders-or-a-humane-world

9 Andersson, R. (2018) *Illegality, Inc.: clandestine migration and the business of bordering Europe*. Oakland, CA: University of California Press, Miller, T. (2019), op. cit.; Akkerman, M. (2021) *Border Wars*. Amsterdam: Transnational Institute.

10 Paley, D. (2014) *Drug War Capitalism*. Oakland, CA: AK Press.

11 Miller, T. (2019) *Empire of Borders: The Expansion of the U.S. Border around the World*. London, New York: Verso.

12 Ibid, p. 177

13 Immigrant Defense Project, Mijente, and NIPNLG (2018), 'Who's Behind ICE: The Tech and Data Companies Fueling Deportations'. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf

14 FOIA request 330020322000471 directed to the National Institute of Migration. https://r3d.mx/wp-content/uploads/Oficios-y-anexos-471.pdf.

15 Watch CBP Intel (2019) 'Central American Caravans and Migration Crisis Flow - Update 32'. U.S. Customs and Border Protection. https://r3d.mx/wp-content/uploads/Central-American-Caravans-and-Migration-Crisis-Flow-Update-32.pdf.

16 Meissner, D., Kerwin, D.M., Chisti, M. and Bergeron, C. (2013) *Immigration Enforcement in The United States: a formidable machinery*. Washington, DC: Migration Policy Institute. https://www.migrationpolicy.org/pubs/enforcementpillars.pdf.

17 Woodward, J. (2005) 'Using biometrics to achieve identity dominance in the Global War on Terrorism'. *Military Review*; see also Jacobsen, A. (2021) *First Platoon: a story of modern war in the age of identity dominance*. New York: Dutton.

18 Angel, A. (2020, 15 December) 'Población en cárceles crece a ritmo récord en 2020: hay 14 mil reos más que al inicio del año', Animal Políitico. https://www.animalpolitico.com/2020/12/poblacion-carceles-crece-record-2020/#:~:text=Mientras%20que%20en%20diciembre%20de,de%20que%20cometieron%20un%20delito

19 Romero, O.A. (2014, 10 February) 'La criminalización de la pobreza y el sistema de justicia penal', Información Sididh. http://centroprodh.org.mx/sididh_2_0_alfa/?p=31418

20 de Goede, M. & Westermeier, C. (2022), op. cit.

21 Woodward, J. (2005) 'Using biometrics to achieve identity dominance in the Global War on Terrorism'. *Military Review*. https://www.rand.org/pubs/reprints/RP1194.html; see also Jacobsen, A. (2021) op. cit.

22 Kwet, M. (2021), 'Digital Colonialism'. https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire

23 DHS Office of Inspector General (2021) 'CBP Targeted Americans Associated with the 2018–2019 Migrant Caravan'. https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf

[24] LIS and R3D (2023 forthcoming) 'Uso de las tecnologías digitales en los contextos migratorios: necesidades, oportunidades y riesgos para el ejercicio de los derechos humanos de las personas migrantes, defensoras y periodistas'. www.r3d.mx/publicaciones.

[25] Open Society Justice Initiative (2019), *Unmaking Americans: insecure citizenship in the United States,* p. 102. https://www.justiceinitiative.org/uploads/e05c542e-0db4-40cc-a3ed-2d73abcfd37f/unmaking-americans-insecure-citizenship-in-the-united-states-report-20190916.pdf

[26] Chambers, S., Boyce, G., Launius, S. and Dinsmore, A. (2019) 'Mortality, surveillance and the tertiary "funnel effect" on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence'. J*ournal of Borderlands Studies*, 36(3): 443–468. https://doi.org/10.1080/08865655.2019.157086

[27] Muñiz, A. (2022), op. cit.

[28] Rosas, G. (2006), op. cit.

[29] Jacobsen, A. (2020), op. cit.

[30] Guidotti-Hernandez, N. (2011) *Unspeakable Violence: Remapping U.S. and Mexican National Imaginaries*. Durham & London: Duke University Press. Woodward, J. (2005), op. cit.

[31] Woodward, J. (2005), op. cit.

[32] Muñiz, A. (2022), op. cit.; Rosas, G. (2006), op. cit; Khan, J. (2019) Islands of Sovereignty: Haitian migration and the borders of empire. Chicago: University of Chicago Press.

[33] Rosas, G. (2006), op. cit.

[34] McCoy, A. (2017) *In the Shadows of the American Century: The Rise and Decline of US Global Power*. Chicago: Haymarket Books.