

Digital Fortresses

Mapping the infrastructure of coercion and control



1. Introduction

We live in times of growing coercion and control, where activism, resistance, and even existence are under threat in the face of state violence and repression. The infrastructure for this is increasingly digital. Migrants are swept up and imprisoned in border-patrol dragnets in US cities or in desert towns in Mali and their personal details recorded in transnational biometric databases. Fishing boats off the coast of Venezuela or wedding parties in Yemen are eliminated at the touch of a drone operator in Arizona. Activists holding up signs saying ‘I oppose genocide. I support Palestine Action’, and even for comments made on a Zoom call, are being charged with terrorism. This genocide continues to unfold in Occupied Palestine in which the names of journalists, teachers, health workers and even children are entered into databases, and an algorithm determines them to be a legitimate target for elimination.

Digitalisation has dramatically increased both the coercive scope of state agencies as well as its potential impact. This is facilitated by a physical and mobile infrastructure of data centres, databases, cables, mobile and home devices that penetrate every realm of our lives. It is an infrastructure that interconnects previously distinct areas of state power, reliant on a small coterie of private corporate actors, and embedded in physical landscapes and institutions that might well outlast those who dare to challenge it.

To examine this digital infrastructure, the Transnational Institute (TNI) and The Institute for Technology in the Public Interest (TITIPI) convened a diverse international group of 30 activists, researchers, and organisers working at the intersections of technology, militarisation, borders, and social justice. The workshop was in response to the recognition that many movements work reactively, responding to specific moments or advocacy opportunities, and thus sought to create space for broader conceptual connections across different arenas of resistance.

The workshop took place over two days in Amsterdam in March 2026, with support from Funders Initiative for Civil Society (FICS), in the historic Ru Paré building – a space rich with symbolic significance.¹ Named after Henrica Maria (‘Ru’) Paré, a prominent artist who organised resistance networks during Nazi occupation and saved Jewish children, the venue continues to work with marginalised communities in Amsterdam and embodied the workshop’s spirit of resistance and solidarity.

2. Analysis

Why look at digital infrastructure?

Civil society campaigners and researchers working in this area tend to focus on reacting to specific legislation or regulations or tackling a particular harmful tool, trying to block the latest power-grab by Big Tech companies or state over-reach, and limit potential human or environmental harm. The advantage of looking at digital developments through the lens of infrastructure is it enables us to analyse the physical and digital systems that permit this extension of coercive control and surveillance, to examine where they intersect and diverge and to identify the nodes and vulnerabilities that could allow for intervention.

For activists working to oppose US border militarisation, understanding it as an infrastructure helped make sense of the multifaceted beast of migration-control surveillance across a huge border, seeing it as far greater and more complex than a geographical line near the Rio Grande, extending 2,415 kilometres south of the US border and at the global level.² The design of this infrastructure is not

accidental but based on long-term plans by US military and security strategists who have sought to join up technologies, databases and devices through planned hardware and software development and through agreements such as biometric data-sharing partnerships with neighbouring countries.

In the US and elsewhere, the rationale for expanding digital systems of surveillance took off after 9/11 (Al-Qaeda's attacks on US buildings in September 2001) and the so-called 'war on drugs', and increasingly included migration management. Biometric data-sharing infrastructure was entrenched in Trump's first presidency, as well as the initiation of apps, such as CBP One, requiring migrants to share their personal data in order to apply for asylum and which is now used to encourage them to 'self deport'. The new Acting ICE Director, Todd Lyons expressed the direction of travel when he said: 'We need to get better at treating this like a business, like [Amazon] Prime, but with human beings'.

The app CBP One shows that by infrastructure, we are not just thinking about the cloud or data centres, but a 'production environment' like a factory, where every bit of software goes through a system controlled by a few small companies. In this sense, our personal devices (smartphones, computers, home appliances, electric vehicles) are not ours, but accessories of the clouds. Take Amazon Ring or Echo, for example, which are no longer just personal home security devices, but a network that covers 95% of the US population and has the potential to track and map devices in its reach.³

Nor is it simply about personal consumer items. This same production environment encompasses governments, including the military, public institutions and non-governmental organisations (NGOs), all of which are being encouraged to build systems in the mirror image of software production saved in clouds.⁴ Coercive state agencies are using this vast infrastructure and datasets in ever more expansive ways. The US Immigration and Customs Enforcement (ICE) biometric Mobile Fortify app, for example, is being to expansively analyse even random datasets, such as ad tech data, to identify 'target rich' areas to which to send officers.

The power of the infrastructure – and the ambition of many of its architects – is that it is interoperable, whereby datasets are shared and connected. This means that borders, prisons, military systems, and digital platforms are increasingly integrated through shared technologies, data systems, and corporate interests. These are also embedded in a political economy where the computational industry – in particular the Big Tech firms – have succeeded in capturing the operations of governments and public institutions in all spheres of public life, which enables them to facilitate connections and overlap processes in different civil, military and security contexts. It means that increasingly we are not talking about stand-alone tools or actors but an ecosystem or architecture. Resistance therefore requires a multi-pronged approach, but the many nodes also offer opportunities to connect different movements and campaigns and provide a variety of 'choke points' to target.

The difficulty with infrastructure is that it is often invisible to most people while to others it appears motiveless, purpose-free, apolitical or even as a public good. It is hard to see the human harm they inflict. Yet infrastructure is never neutral: it carries political meaning and reflects the power dynamics of its environment and funding sources.

BOX 1: Bezahlkarte – Germany's Asylum Seeker Payment card

In 2025, Germany introduced a new payment card to replace most cash-based benefit payments to asylum seekers. The stated rationale was to make it easier to distribute benefits, reduce the 'risk' of money being sent abroad or to traffickers, and cut down on paperwork for local authorities. This has in fact made it harder for refugees to access resources, limited their ability and autonomy to purchase what they need, and forced them into a few large supermarket chains who now capture all the income. It has become a system of racialised control. There have, however, been creative forms of resistance, with groups like the International Women* Space creating solidarity infrastructures that allow users of the *Bezahlkarte* to exchange vouchers purchased with the cards for cash.⁵

Mapping the Digital Fortresses

One way of understanding the digital infrastructure is through the metaphor of a digital fortress, which is increasingly constraining and limiting privacy, autonomy, exercise of rights and even people's right to life. It reflects how public interactions are increasingly militarised and securitised, with physical and digital boundaries becoming increasingly blurred and with digital infrastructure given systems of protection that citizens rarely enjoy. The physical nature of a fortress also draws attention to the physical infrastructure – cables, data centres, phones, and computers as well as the material components (minerals, plastics etc.) – that are involved in all digital infrastructure. As one workshop participant said, 'Data centres are the unsung heroes of uptime, engineered to withstand disasters both natural and man-made. In a world increasingly reliant on constant connectivity, these digital fortresses have become the system's last line of defence'.

During the workshop, there was an attempt to map the layout of these fortresses, to identify the architecture that illustrates the system of coercion and control. The aim was not to produce a technical map, but rather a political one that can reveal points of vulnerability and connection. Participants identified several key dimensions that could be mapped:

- Technical infrastructure: The physical and technical components of digital systems, including data centres, mobile devices, network infrastructure, and hardware.
- Corporate actors: The companies developing, deploying, and profiting from digital coercive infrastructure including intermediary companies that supply and enable them.
- Government actors: The state agencies and officials involved in designing, implementing, and regulating these systems.
- Financial flows: The funding sources, investment patterns, and economic interests driving the development of these systems.
- Data flows: The movement of data through these systems and who has access to it.

All these actors, in pursuit of their varied interests, have direct impacts on communities – and indeed maps based on their experiences of these impacts is critical to making sense of the infrastructure and making its harms visible. Every institution, no matter how powerful, is also dependent on others, most of all the workforce, consumers, academic partners, and investors, all of which are potential points of leverage against them. They are also dependent on systems, regulations and legislation that enable and at times constrain them. Together these provide a power map for activists navigating and challenging digitised security infrastructures, helping us share common frameworks and methodologies, build collaboration and prioritise targets and campaigns.

There are nonetheless challenges in mapping digital coercive infrastructure. Much of the infrastructure is deliberately opaque, complex, dispersed and rapidly changing. Mapping it can therefore be like trying to map a living organism—it is constantly changing and adapting. It may also distort realities if it is based on limited knowledge, reflects partial understanding, or makes structures seem more solid or more important than they are in practice.



Flipchart maps of digital infrastructures, March 2026

Blurred military and civilian worlds

The digital fortress is at its core a system of violence. This can be seen in the ways that the distinction between civilian and military technology is becoming increasingly blurred, in terms of the companies, the spheres of impact, and even the data that is used for new technologies. Everything is militarised. The Pentagon has declared cyberspace the ‘fifth domain of warfare’. Data that was never intended for military purposes, such as social media content, is now being used in military campaigns. Technology, such as drones, is also rapidly being applied to military use. Tech companies that relied on advertising to consumers are now winning massive military contracts from the Pentagon. Technology deployed in the genocide in Gaza is being repurposed to support the deportation of racialised people from the US. Digitalisation is increasing both the speed and scale of human rights abuses.

There has been an emergence of a digital-military-security-industrial complex, whereby commercial players are entering the military field, and military/security companies are moving into the commercial sphere. These involve some of the world’s largest and most powerful companies, such as Alphabet (Google), Amazon, Meta (Facebook) and Microsoft, the giant military companies (Lockheed Martin, Airbus) as well as newer players like Anduril and Palantir and Chinese corporate giants such as Hikvision, Huawei, and Dahua.

This militarisation of the digital sphere is not new and is in some ways embedded in its origins – as much modern computing originated in military research – but it has dramatically expanded and shifted to becoming the major focus of digitalisation in recent years. It embeds violence at the core of the system.

It also mirrors a blurring of public and private as tech companies secure a growing level of publicly funded military and domestic security contracts and the military and state security agencies (policing, border control etc) become increasingly dependent on privately controlled infrastructure.⁶

BOX 2: Power dynamics in digital security infrastructures

- Control over information flows: Infrastructure determines what information can flow, to whom, and under what conditions
- Logistical control over material and labour resources: Digital infrastructure is reordering supply chains, labour markets and the environment
- Extraction and exploitation: Digital infrastructure replicates and perpetuates patterns of colonial extraction, with data and computational power flowing from the Global South to the Global North
- Exclusion and inclusion: Infrastructure determines who is included in digital spaces and who is excluded
- Disproportionate impact on marginalised communities: All systems disproportionately affect marginalised and vulnerable populations
- Surveillance and monitoring: Interconnected infrastructure enables unprecedented forms of surveillance and social control
- Predictive control: Digital systems are moving from reactive to predictive forms of control
- Blurring of public and private: All systems involve increasing collaboration between government and corporate actors.

Convergence and control – Scaled up violence

The big picture is that digitalisation is facilitating the convergence among the control systems of the coercive arms of the state. Digital infrastructure serves multiple overlapping purposes (military, border control, corporate surveillance) and similar technologies are deployed across different applications. Paying attention to digital infrastructure, therefore, allows for a better understanding of the undergirding and overlapping workings of military, border, policing, surveillance, and other technologies by the state and its partners in everyday life.

As these technologies are deployed, they are further enmeshing systems, which will be very difficult to unravel even in different political environments. Technical standards and protocols, for example, are becoming increasingly standardised across different applications. Data systems are being integrated across different domains. Policy frameworks are being harmonised across different domains. This is accompanied by a corporate consolidation in which a small number of corporations are now controlling infrastructure across multiple domains – deciding how it is constructed and deployed and whom it serves.

This is reordering the entire economy, expanding the logistical power of specific security companies and embedding them deeply into the state, while transforming the relationship between citizens and the public and the state. Tech companies, for example, are now shifting their self-promotion from being consumer champions to being state champions and binding themselves to a national security project. Financial corporations, such as VISA's involvement in the German refugee welfare digital card (Bezahlkarte), are also embedded in the system, while academics and think tanks are marshalled through funding arrangements to support this project. This architecture is why infrastructure cannot be viewed simply as a few systems tools, but rather as an entire ecosystem that includes the corporations, investors and states that sustain, drive and fuel the supply chain of these technologies.

The nature of the burgeoning and interconnected digital infrastructure is that it allows for surveillance on a much bigger scale, with global implications. This system could be used for different purposes, such as protection, but it is overwhelmingly deployed in forms of violence or exclusion. This is evident in the way that border infrastructure can survey every movement in or near a border, yet seems incapable of preventing drownings (such as in the Mediterranean, the English Channel or en route to the Canaries), documenting and stopping violence of border guards, or improving human rights protections of vulnerable peoples.⁷

Panopticon – the vision of interoperable databases

The European Union (EU) has been involved in a long-term project to create a digital infrastructure that links and provides greater access to multiple databases, actors, and data flows, with severe consequences for basic rights, particularly in relation to migrants and marginalised communities. For more than 20 years, the European Commission has been working towards a common identity repository, focused on migrants.⁸ It started in 2003 with a fingerprint database for asylum seekers, EURODAC. This was followed by the Visa Information System (2011), Sharing Information System II (2013), and now the Entry-Exit System (2026), which is modelled on the US ESTA (Electronic System for Travel Authorization), and which requires everyone crossing a border to leave fingerprints and a facial image. It also stores and links to any formal or informal convictions. The EU is working on making these databases increasingly interconnected and linking them with law enforcement databases, thus intentionally conflating migration and crime, and making survival harder for people at risk of deportation and providing ever more possibilities for deportation (where a ‘crime’ might be attending a pro-Palestine protest).⁹

In terms of policing, the Prüm Convention allows police authorities to make one request of the databases in 30 countries. The US is requesting direct access to police databases with biometric data as a condition for access to its own Visa Waiver programme. This could include accessing 8 million images of refugees or migrants whose identity has been recorded by the police authorities, even if they have never been charged of committing any crime. Bahrain has already agreed to such a US deal, exemplifying how data that was hitherto controlled and restricted to one country is shared cross borders and turned into bargaining chips – by the US, in this case.

Once the access to private data is granted, usually for a specific purpose, there is little to stop it being used for others. The ‘Global War on Terror’ was initially used as the pretext for data-sharing, with the UN Office on Counter Terrorism legitimising this worldwide. With the rise of reactionary, anti-migrant governments, the focus is now on data on migrants and other travellers, and the scope is bound to extend to other arenas later. Health-related data in Kenya, for example, has been shared with US authorities,¹⁰ while digital data from Afghanistan, whose collection and storing were funded by Germany during the US-led occupation, ultimately ended up in the hands of the Taliban.

This is also facilitated by the increased reliance on private corporate contractors for data storage, sharing and analysis. Companies like Microsoft and Palantir, for example, are embedded in both the most aggressive forms of digital-based warfare and racist migration enforcement, but also in the operations of state welfare agencies such as the National Health Service (NHS) and His Majesty’s Revenue and Customs (HMRC) in the UK. Their data ‘services’, predicated on the violation of people’s right to privacy, intend to expand to accessing personal data containing intimate insights of our lives. These actors sell their services thanks to their power to combine and understand this data. The supposed barriers between our private data and weaponised harm are ready to be broken, if they are not already.

Dilemmas of Digital Public Identity (DPI)

The coercive uses of data present huge challenges whenever basic services require digital access. In countries across Africa, for example, there is a big push to promote Digital Public IDs (DPIs) in a continent where 850 million people lack any legal identity. Digital ID is said to offer the possibility to meet the UN Sustainable Development Goal (SDG) 16.9 and Africa's Agenda Title 2016, by providing a legal identity for all. It could also help low-income countries provide universal services at lower costs. This drive to DPI is being strongly supported by certain multilateral organisations as well as major donors such as the Gates Foundation.¹¹

However, a rushed or uncritical introduction of these systems may have adverse impacts on human rights, and cause social harms and further exclusion of those who are potentially being locked out of social protections. It could also embed racial or other bias inherent in algorithmic systems, for example through its dependence on legacy systems like those that exist in post-Apartheid South Africa. Issues of data misuse are also t, even if collected carefully, particularly for marginalised groups. For example, data on Rohingya refugees collected by the United Nations High Commissioner for Refugees (UNHCR) ended up being shared with the Myanmar government from which they had fled.¹² Similarly, databases may eventually be connected to other datasets that provide states and other actors much more intrusive insights into citizens and others than were initially imagined. In the context of countries across Africa, where there are often no formal legal frameworks to hold corporations accountable, the dangers are multiplied.

As a minimum, if DPI is adopted, it is important to ensure that certain safeguards are put in place and that it is not made mandatory or conditional for accessing services.

Prison Digital Infrastructure

Prison and incarceration present another frontier for digital surveillance technologies, with systems being pioneered for deployment both in prison and after release in terms of electronic monitoring and smartphone apps. The US, in particular, is relevant in this regard, as proportionally it has the world's largest prison population of 1.8 million people, far more than China on this measure.

Digital systems control every aspect of prison life from movement to communication. Cameras, audio monitoring, and other surveillance technologies physically track prisoners. Digital media is used to track their behaviour and to make money, forcing prisoners to pay for accessing books or media or even for sending messages to their loved ones. Print correspondence is scanned and a charge imposed for doing so. This is the beginning of the automatisisation of prisons that could even lead to replacing some prison officers with AI tools and robots.

For former inmates and others, there has been a boom in electronic monitoring smartphone apps, enabling continuous monitoring of people day and night. Migrants who have not been convicted of any criminal offence are compelled to use the SmartLINK smartphone app, developed by BI Inc, whose parent company is Geo Group, which runs private immigration detention facilities and prison systems in the US. There are even proposals to put chips under people's skin in the future, marketed and justified as a means to protect them, such as preventing cardiac arrest.

These systems interface with fingerprint, facial recognition, and other biometric systems used by increasing numbers of state authorities from policing to borders and migration to health and social security. Together they create a continuum of control that extends beyond prison walls, blurring the boundaries between incarceration, 'community supervision' and social welfare.¹³

In 2025, the US prison telecommunications industry had a revenue of US \$5.6 billion,¹⁴ most of which came from prisoners' family members, who are usually from the lowest economic strata of society. It's a transfer of wealth from the poorest people in the US to the private equity companies that own these prison telecommunication companies.

Border Digital Infrastructure

As mentioned earlier, border control is at the heart of how digital technologies are transforming coercion and control of people, particularly the most marginalised. Digital forms of border control are more pervasive and harder to challenge than physical barriers and are moving society towards forms of racialised control, in which political decisions are made about who is allowed to move and who is not.

A 'border industrial complex' of corporations is emerging using AI, biometrics, and data analytics to create these new forms of control.¹⁵ These include biometric border systems (fingerprinting, facial-recognition, and iris-scanning technologies used to track and control movement); predictive analytics (AI systems that attempt to predict and prevent migration based on various data points); digital identity systems (documents, ID and banking cards, and systems that control access to movement and services) and remote surveillance (satellite, drone, and other technologies monitoring borders from a distance). These are all reinforced by private and semi-private institutions, universities, and research facilities developing technologies and policies and using borders and refugee camps as testing grounds for new technologies.

Many of these systems are being trialled on Europe's borders, such as the Samos detention camp in Greece or the International Centre for Migration Policy Development (ICMPD) programmes in North Africa. The Samos camp has pioneered an elaborate system of surveillance cameras and drones, tracking all the detainees' movements, accessing their phones and data and feeding this into an AI-powered behavioural recognition system, hosted in a futuristic control centre in Athens.¹⁶ Indeed, the border between Greece and Turkey is now a prototype of modern borders where every type of camera, radar system, radio frequency spectrum monitoring, unmanned drones, and land- and water-monitoring vehicles feed into AI-powered systems that process this data in real time.

These systems are also being exported, including through border externalisation agreements, that impose digital coercive systems on states far away from the EU and the US. Any ethical concerns that the EU may claim are completely ignored when it comes to border and migration enforcement. Indeed, data is extensively taken from migrants and often without even the knowledge of asylum seekers demanding international protection.

Policing Digital Infrastructure

Digital technologies are also transforming police practices, creating new forms of surveillance and control that are much more pervasive and intrusive than traditional methods. These developments include:

- Predictive policing: AI systems that attempt to predict where and when crimes will occur
- Facial recognition and other biometric surveillance: Technologies used to identify and track people in public spaces
- Social media monitoring: use of social media platforms for surveillance and intelligence gathering
- Database integration: Systems that create comprehensive profiles of individuals based on multiple data sources.

Invariably these systems reinforce the systemic racism and discriminatory practices of policing, creating suspect populations that are more deeply surveyed and controlled.

3. Strategies

Infrastructural points of vulnerability

The enmeshed and emerging coercive digital infrastructure is not impregnable. It is important to understand the many points of vulnerability for intervention and resistance. Some of these dependencies or vulnerabilities include:

1. Physical presence: For all the hype about the cloud, this infrastructure requires data centres, cables, satellites, cell-phone towers and more, all of which can be places for resistance or disruption. The militarised nature of these structures – and the potential for them to be seen as ‘legitimate’ targets – have been seen in the US/Israeli war on Iran, where Iran responded by targeting data centres operated by Amazon Web Services in the United Arab Emirates (UAE) and Bahrain.¹⁷ Building infrastructure tends to be slower than popular mobilisation, as illustrated by the burgeoning resistance to new data centres across the US and elsewhere, which threaten to undermine the grandiose plans of AI hyper-scalers, and is fuelled by the costs of data centres to the local environment (water, air, energy). Campaigning could make this structural violence visible.

2. Technical dependencies: Infrastructure relies on specific technologies, protocols, or suppliers, all of which can be points of intervention as well as places where counter-surveillance can be marshalled. The recent EU digital wallet, for example, requires certain protocols and systems that users can use to reassert control. The parties seeking to use the wallet must, for example, identify themselves and maintain an interface with the wallet system.

3. Labour reliance: Data centres, AI development and weapons development all depend on and require labour participation, which becomes a crucial point of intervention particularly through the engagement of trade unions. Labour organising in Kenya around data work, for example, has achieved a ruling against sham employment by Facebook, as well as mandatory mental health care for content moderators.¹⁸ Similarly, tech development for migration enforcement and war has been increasingly challenged by tech workers through groups like No Tech for ICE and No Tech for Apartheid – although this has also faced fierce repression within the industry with organisers being targeted and sacked or laid off. Forming alliances with public-sector unions will become increasingly strategic as these digital surveillance services and tools become further integrated into state institutions and bodies.

4. Regulatory vulnerabilities: These systems are under-regulated, but nevertheless depend on specific regulatory frameworks or policies that can be points of leverage. Data-protection rules, impact assessments or human rights impact assessments are frustratingly bureaucratic and weak, but have also been a tool for communities in countries such as Kenya to challenge digital infrastructures. Legal victories have also sometimes stimulated political victories, forcing political authorities to implement protection.

5. Reputational risks: Both political and corporate actors are vulnerable to negative publicity or scandal that can arise from the violence and harm embedded in digital coercive infrastructure. Corporations such as Google or Accenture that are focused on consumers or on business clients that provide some key support services or infrastructural nodes are particularly vulnerable to reputational risks as bad publicity concerning their security-focused contracts can threaten other significant areas of their business.

6. Financial dependencies: Systems may rely on specific funding sources or investment patterns that can be other points of leverage. In New York, for example, there have been successful campaigns to divest pension funds from Securus, one of the two major prison tech companies, which contributed to the company almost declaring bankruptcy in 2025.

Resistance strategies – starting from collective organising

The interconnected nature of digital coercive infrastructure means that it is critical to confront this in a systematic way rather than focusing solely on specific tools or instances. The convergence of coercive systems means we need a convergence of movements. This work requires bringing together communities unused to working together, operating within different rationales or disciplines, cultures and geographies. This approach also provides opportunities, however, because such a system can only be confronted if it is challenged on all sides and by a sustained form of political counter power that can lead to lasting change.

Practically, developing a convergence of movements requires:

- Shared analysis, languages and frameworks for understanding digital coercion
- Strategic alignment: Identifying issues and campaigns where different movements can work together.
- Resource sharing: Sharing resources, expertise, and infrastructure across movements, particularly in challenging areas like technical expertise
- Mutual support and struggle: Providing support and solidarity across different movements and contexts and ensuring those most vulnerable to violence and surveillance are not put at further risk with our work
- Valuing not just the narrative-tellers but also those who do the care work that sustain movements
- Long-term relationship building: Investing in building relationships and trust across movements, a process which takes time.

The growing violence and inequalities arising from these systems also mean there will be more opportunities for groups to coalesce in a common struggle and to build solidarity networks. For example, communities resisting a data centre in the US state of Georgia that is expropriating land, water, electricity, and resources can now be connected to anti-ICE movements across the US, peace campaigners against AI warfare, digital rights campaigners, content moderators in Kenya, and Palestinian solidarity movements opposed to the Gaza genocide. Campaigns that may start from a Not in My Backyard (NIMBY) sentiment, angry at the loss of local land or water, can be politicised to take on a more systemic and internationalist critique when they realise the data centre is part of a larger imperial corporate and violent infrastructure.

There is, therefore, an opportunity to link previously distinct and siloed movements with Indigenous struggles, environmental campaigns, democratic movements and so on. The digital or the tech tools may not be the starting points for these campaigns, but rather examples of a broader unjust political economy that needs transformation. These movements will need to be international in the same way as the digital coercive system is global. The international linkages and supply chains also provide points of leverage. There are, for example, campaigns for countries producing raw materials to place conditions on their exports of critical minerals so that they are used only for green transition and prohibited from military production or related purposes.

It is important to be aware in this process of coalition building that there are dangers of skirting around important conversations about the underlying politics of analysis and what is needed to resist. This risks leading much more reformist approaches and watered-down politics, such as engaging corporations involved in coercive infrastructure that ends up reinforcing their power and only minor reforms that fail to challenge the underlying system of violence.

BOX 3: Learning from the European trade justice campaigns

The European Trade Justice movement is committed to changing trade rules to protect people and the environment. Despite its focus on very complex and technical issues of trade regulations, they succeeded in stopping reversing several damaging trade agreements such as the EU-US TTIP and the Energy Charter Treaty as well as preventing the EU from advancing new rounds of negotiations at the World Trade Organization (WTO). Its success has lessons for the movement against digital coercion – it shows the need for:

1. Technical expertise to understand and challenge the systems being opposed.
2. Coalition building across different sectors and movements.
3. The power of narrative that links technical issues to broader values like privacy, dignity and justice and which includes powerful symbolism that capture the injustice and resonate with the public (e.g. TTIP being associated with 'Chlorinated Chicken' or the so-called villains 'Big Pharma', 'Big Tech').
4. Good timing, and taking advantage of political opportunities, which can have a dramatic impact on effectiveness, depending on broader political contexts.
5. Multiple strategies – technical, legal, political, and public pressure – as no single strategy will work.

Despite these successes, the trade justice movement faces big challenges in the context of the Trump era and which highlight another lesson – this time from its failure to develop positive political demands of what trade justice would look like. This failure allowed a figure like Trump to claim to have embraced the increasingly popular anti-free-trade critique, while developing a trade policy that was far from what the trade justice movement had envisaged. The vacuum of alternatives to free trade allowed Trump to present his own alternative – one based on bullying and naked mercantilism rather than labour rights and environmental protection.

Data minimisation

Minimising the collection and sharing of data is a fundamental goal to reduce the levels of harm. Every action that minimises data collection by state coercive agencies helps limit their power.

Corporate accountability

The architecture of digital security is underpinned by corporate actors developing and profiting from digital coercion, so targeting them must be a central strategy for pressure. Companies can be vulnerable to reputational risk as the harms they cause become public in growing areas of daily life. There is a need for detailed corporate research to examine the supply chains as well as financial systems and state strategies that sustain these corporations. This research needs to look across the whole sector from the specific technologies (e.g. fingerprinting scanners) to the IT companies that provide the servers and software such as Amazon, Google, Microsoft and Palantir, and to the financial investors that facilitate their growth and expansion.

Activists campaigning to isolate Israel and stop its genocide and apartheid policies, for example, have identified that 33% of the world's cyber 'unicorns' (US \$5 billion companies), come from the country;¹⁹ and in 2021, 40% of the private global investment in cybersecurity and the cyber sector was in Israel.

The Israeli tech sector is highly dependent on private investment (91%), with foreign funding accounting for 80% of venture capital investment.²⁰

In some cases, it might also be possible to stoke division between corporate actors vying for control and profits in this space – as a ‘divide and resist’ strategy.

It is important, however, to not focus solely on single companies and ignore the underlying architecture. Companies will sometimes fall, change or be taken over. Therefore any efforts to achieve corporate accountability need to be accompanied by confronting the wider political economy that enables their profits, whether the military institutions that develop or deploy them, academic institutions that produce the underlying research and the patents required for these technologies, and/or of course, the political actors that normalise and protect their use. The latter will include intervening in decision-making circles, where corporate actors exercise huge influence, as was seen in the debates that led to EU’s AI Act (2024) where Big Tech succeeded in watering down limitations on AI deployment.²¹

Legal Resistance Strategies

Human rights frameworks remain important for challenging digital coercion but have limitations, particularly when international law is being systematically undermined globally. Certain strategic litigation cases have achieved specific victories, set broader precedents and raised awareness. Leveraging data-protection regulations can help limit surveillance by constraining how data is collected and used.

However, there are also challenges, particularly at a time of blurred military-civilian tech, where international law related to war and conflict is distinct from civil human rights frameworks – which leaves a gap as they apply to different actors. The way corporate and state actors are blending into each other, as well as the way military and policing and immigration enforcement is blurring in roles, means that there is an accountability gap.

Use geopolitical divisions to our advantage but resist tech nationalism

The rise of a belligerent strand of US imperialism has created some geopolitical divisions that work against the attempts to build a cohesive digital coercive infrastructure. This presents new possibilities for resistance and obstruction. For example, the US is currently threatening to expel partner countries from its Visa Waiver programme unless they sign an agreement to share more data.²² Campaigning to leave the programme would create an important choke-point in cross-border data-sharing and undermine the EU’s own attempts to impose this on neighbouring countries. The anti-US public feeling and comparisons between the EU and US immigration policy could provide some important hooks for public campaigning and policy.

It is important, however, to be extremely careful of using ‘sovereign’ arguments (digital sovereignty, digital nationalism) to prevent US Big Tech, as this can backfire and end up defending and justifying other extractive and exploitative new corporate actors and initiatives. Rather than a framework of sovereignty (which is exclusive and tied strongly to rhetoric and militarised practices of national security), we need a new language and narrative rooted in justice, community and cooperation. Movements for digital sovereignty may serve a purpose to dilute the power of US-based Big Tech, but that doesn’t necessarily translate into a rejection of coercive control.

Counter-surveillance

Counter surveillance has been critical to undermining digital coercion. In the US, for example, citizens have been developing sophisticated forms of monitoring ICE activity, evidence gathering and analysis to challenge the agency's increased use of violence. Smartphone apps such as Red Dot and ICEBlock allowed people to report ICE sightings; however in 2025 these apps were removed from the App and Google Play Store after Apple and Google were pressured (although not legally compelled) to do so by the US Department of Justice. New tools continue to be deployed by activists, increasingly under the radar.

It has also been critical for activists to use technology to protect themselves from surveillance and control, for example through secure messaging systems such as Signal and through limiting reliance on Big Tech infrastructure.

Cultural resistance and long-term change

Art and culture are critical both for understanding digital systems in new ways but also imagining alternatives. Cultural work is also about changing the bedrock on which values and systems are built. This is long-term work, which is true of many struggles, such as the fight against Israeli apartheid. It requires slow thinking, a realisation that we are in this for the long haul, an acknowledgement that there are no simple solutions, and that as human beings we all have limitations as workers and as citizens. This requires a level of compassion and empathy as we build movements together.

BOX 4: Bug Reports

Bug reporting is a practice where users document errors, flaws, and failures they encounter in software and that developers then can try to fix. It is common within free software communities and necessarily requires other types of expertise than writing code. On several occasions, TITiPI has organised collective bug-reporting sessions on technologies with significant social impact such as the COVID app. Together with people who would probably be affected by its implementation, we understood it as a racist technology which would also tie governments to Big Tech players. The publication of the bug report sparked a conversation with developers of the app, but also with a wider group that had similar concerns. While the bug report targeted a specific technology, it shifted the scope from reporting on whether the app was working as it was designed, to asking if it should be actively undesigned and not exist at all.²³

Building alternatives

Creating and promoting technologies that prioritise privacy, security, and community control over surveillance and exploitation could both provide alternatives but also model them. In Germany, for example, activists campaigning against the Bezahlkarte, have created a system whereby people issued with the card use it to buy vouchers from the assigned supermarkets that are then exchanged for cash with members of the public. This allows migrants to buy anything they need where they like and without being tracked.

The key in Germany and elsewhere has been to involve affected communities in the design of alternative technologies and to use digital tools with the goals of supporting mutual aid and community resilience.

Building alternative digital services can also help undermine corporate profit incentives. If you can make the technology for free that that is currently on a paid subscription you can directly hurt those companies that seek to profit from coercive activities. This has happened, for example, in New York, which has made all prison phone calls free, ending a market for an exploitative private phone company.

BOX 5: Confronting the arguments that stop us before we start

1. The technical complexity argument: Systems are too technically complex for ordinary people to understand or challenge. > This requires slowing down adoption rather than the opposite, so that the systems we adopt are understandable and carefully considered. Complexity also sometimes provides opportunities for resistance.
2. The inevitability argument: Digital coercion is inevitable and resistance is futile. > Nothing about these systems is inevitable – they reflect choices about values and priorities, and those choices can be changed.
3. The convenience argument: People will adopt these technologies regardless of what they do because they are convenient. > There's an arc for big tech platforms in terms of convenience and service where the service starts with everything but then is whittled away to an ad-invasive utilitarian husk ('enshittification' as Cory Doctorow calls this).
4. The resource argument: Resistance requires resources that many movements lack. > While resources are important, creativity and strategic thinking can often compensate for limited resources.
5. The fragmentation argument: Resistance efforts are too fragmented to be effective. > Fragmentation is a challenge, but it also reflects the diverse nature of these systems. Because many systems are interconnected, success in one area can also have effects elsewhere.
6. The speed argument: Technological change is happening too fast for resistance efforts to keep up. > Rapid change can make existing systems vulnerable and create space for alternatives.

Next Steps: Research Priorities

Workshop participants identified several key areas where research is critically needed:

1. **Technology:** Better understanding of the technical architecture, vulnerabilities, and potential points of intervention in digital coercive infrastructure.
2. **Corporate:** Mapping the corporate ecosystem, including the public-private procurement and contract processes, the full supply chains (e.g. critical minerals, financial actors) and understanding the business models driving digital coercion.
3. **Impacts:** Documenting the effects of digital coercion on different communities and populations as well as learning from the resistance in all regions of the world, for example the anti-data centre struggles in Malaysia, Indonesia, Thailand and Vietnam.
4. **Policies:** Analysing the policy frameworks and regulatory environments that enable digital coercion.
5. **Alternatives:** Developing research on alternative models and approaches to digital infrastructure.
6. **Historical:** Understanding historical patterns of technological control and resistance that can provide important insights into current developments.
7. **Big picture:** Understanding how digitalisation is changing capitalism and neoliberalism, and war and imperialism

Conclusion: A call to dismantle the Digital Fortress

The workshop took place during a period of intense global upheaval and violence, in the aftermath of the US kidnapping of Maduro in Venezuela, at the start of an Israeli–US war on Iran, and in the context of Israel's continuing genocide in Gaza and the West Bank. There is a public mood of disorientation, confusion and disaffection. Yet what is clear is that Big Tech and new forms of coercion and surveillance are at the heart of both the revived US imperial project and among the other countries jostling for power. In the process digital coercive infrastructure is ever more pervasive, powerful and entrenched.

TNI and TITIPI made a commitment to deepen the research and analysis of the workshop as part of the Digital Fortresses Project – which will include learning exchanges through a webinar series in September, commissioning of further analysis in a series of essays, and an 'operations room' to critically examine the Bezhalkarte in Berlin by those who most feel its impact.

Despite its complexity, there is increasing public awareness of the existing and growing dangers of digital infrastructures. Resistance is escalating. For digital justice movements, this involves responding to the public opposition, while deepening understanding and sharpening strategies as the field keeps shifting and changing.

The workshop pointed to the strategies this resistance movement will need to embrace to confront these digital infrastructures of control. These include deepening analysis and research, educational efforts to build popular understanding, coordinating across and building cross-sectional movements, and developing and building alternatives.

Fortunately there is already a unity and common vision that it is possible to create digital systems that serve human needs, advance social justice, and support democratic values. But working out the best points of leverage and intervention will require many strategies and experimentation. Most of all it will call for a diversity of tactics to accompany the strategies above: between research and advocacy, immediate and long-term actions, political campaigns and cultural change, from targeting certain corporations and technologies to challenging the broader political systems, resistance and building alternatives.

The digital fortress is vulnerable: it's time to bring it down.

Disclaimer: This summary was produced by TNI and TITIPI based on the workshop discussions and the contributions of many individual experts and organisations that shared their work on a particular issue or domain. This does not mean that everyone who attended agrees with everything written here.

Annex: Further resources

- Authoritarian stack website: <https://www.authoritarian-stack.info>
Maps the 'Authoritarian Stack'—a network of firms, funds, and political actors turning core state functions into private platforms.
- Chander, S., Gürses, S. (2024), From Infrastructural Power to Redistribution: How the EU's Digital Agenda Cements Securitization and Computational Infrastructures (and How We Build Otherwise), AI Now. <https://ainowinstitute.org/publications/from-infrastructural-power-to-redistribution-how-the-eus-digital-agenda-cements-securitization-and-computational-infrastructures-and-how-we-build-otherwise>
- [How Big Tech companies captured our public health system](#) – Arun Kundnani in conversation with Seda Gürses, Transnational Institute, YouTube.

Borders

- 'The EU must stop the digitalisation of the deportation regime and withdraw the new Return Regulation'. <https://www.accessnow.org/press-release/the-eu-must-stop-the-digitalisation-of-the-deportation-regime/>
- 'How a new Europol reform threatens digital war on migrants'. <https://www.accessnow.org/new-europol-reform-threatens-digital-war-on-migrants/>
- 'The EU Migration Pact: a dangerous regime of migrant surveillance'. <https://www.accessnow.org/press-release/joint-statement-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance/>
- 'The U.S. government requires all participants in its Visa Waiver Program (VWP) to enter into an "Enhanced Border Security Partnership" (EBSP)'. The demand is for direct access to fingerprints and facial images in police databases. See <https://digit.site36.net/2026/01/14/access-to-biometric-police-data-eu-commission-wants-to-negotiate-secretly-with-the-u-s>
- Owen, K., Eiger, Y., Radkha, B. et al. (2025)'Understanding experiences with compulsory immigration surveillance in the U.S'. ACM Digital Library. <https://dl.acm.org/doi/10.1145/3715275.3732057>

Policing

- Statewatch (2022) [Building the biometric state: Police powers and discrimination](#)

Prisons/Detention

- 2021: "'You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People'. <https://dl.acm.org/doi/10.1145/3411764.3445055>
- 2022: 'Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives'. <https://www.usenix.org/conference/usenixsecurity22/presentation/owens>
- 2025: 'How transdermal microchips could revolutionize prison security'. <https://www.corrections1.com/jail-management/how-transdermal-microchips-could-revolutionize-prison-security>

Militarisation

- Smith, A. (2026) [We spent Two Days at Milipol: France's 'Security Showcase'](#)
- Chowdhury, A. (2026) [Onodrim Industries: 40M euros secured for European defence tech platform](#)
- What is militarisation of tech? <https://www.privacyinternational.org/long-read/5668/what-militarisation-tech>
- The Tech Arms Race is Reshaping Our Lives — and Threatening Democracy: <https://www.techpolicy.press/the-tech-arms-race-is-reshaping-our-lives-and-threatening-democracy/>
- Blurring of the lines between military and civic spaces: <https://www.privacyinternational.org/long-read/5669/blurring-line-how-militarisation-tech-reshaping-our-town-squares>
- How data drives the militarisation of tech: <https://www.privacyinternational.org/long-read/5667/how-data-drives-militarisation-tech>
- Key concerns around governance: <https://www.privacyinternational.org/long-read/5671/key-concerns-regarding-governance-era-militarisation-tech>
- <https://www.privacyinternational.org/campaigns/militarisation-of-tech>

Digital ID

- Kalema, N.L. (2025) [The 'digital transformation for development' anti-politics machine: A case study on global digital development governance and public-sector digital transformation in Uganda](#), Policy & Internet
- UNHCR (2020) [Digital payments to refugees – a pathway towards financial inclusion](#)
Human Rights for Digital ID (HR4ID) Coalition – Common Position on Mandatory Digital ID <https://hr4id.org/common-position/>
- Human Rights for Digital ID (HR4ID) Coalition – Digital ID Map <https://hr4id.org/national-mapping/>
- World Bank ID4D – Building Statelessness-Sensitive ID Systems <https://openknowledge.worldbank.org/entities/publication/5d920f70-3080-448b-acf8-a82c9dc33056>
- Institute of Development Studies (2025) 'Biometric Digital ID in Africa Progress and Challenges: Ten Country Case Studies'. <https://www.ids.ac.uk/publications/biometric-digital-id-in-africa/>

Endnotes

- 1 Ru Paré Community. <https://rupare.nl/>
- 2 Aizeki, M., Bingham, L., and Narvaez, S. (2024) 'The everywhere border'. Amsterdam: Transnational Institute. <https://www.tni.org/en/article/the-everywhere-border>
- 3 Wired Staff (2023) 'Ring Doorbell cameras raise privacy concerns', Wired. <https://www.wired.com/story/ring-doorbell-camera-amazon-privacy/>
- 4 Balayn, A., Gürses, S. (2026) 'Misguided AI regulation needs a shift'. Policy Review, 1796. Available at: <https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796>
- 5 International Womens* Space 'No to Bezahlkarte': <https://iwspace.de/event/nein-zur-bezahlkarte/>
- 6 González, R.J. (2025) 'Militarising big tech'. Amsterdam: Transnational Institute. <https://www.tni.org/en/article/militarising-big-tech>
- 7 O'Donnell, J. and Guo, E. (2026) 'Border towers surveillance investigation'. MIT Technology Review, 21 September. <https://www.technologyreview.com/2026/09/21/1144166/border-towers-surveillance-investigation/>
- 8 Statewatch (2026a) 'Frontex and interoperable databases: knowledge as power'. <https://statewatch.org/frontex-and-interoperable-databases-knowledge-as-power/>
- 9 Statewatch (2026b) 'EU agencies and interoperable databases'. <https://statewatch.org/publications/reports-and-books/eu-agencies-and-interoperable-databases/>; Digit Site36 (2026) 'Roadmap for interoperability: EU expands its border police databases with facial recognition'. <https://digit.site36.net/2026/03/07/roadmap-for-interoperability-eu-expands-its-border-police-databases-with-facial-recognition/>
- 10 Citizen Digital (2026) 'US–Kenya health deal: the data privacy concerns, America's soft power and Kenya's stake'. <https://citizen.digital/article/us-kenya-health-deal-the-data-privacy-concerns-americas-soft-power-and-kenyasstake-n374443>
- 11 Chauke, T. and Yusif, M. M. (2026) 'Mandatory Digital ID: A Common position by the Human Rights for Digital ID (HRDID)'. Paper P7-S5. <https://id4africa.com/2026/files/P7-S5-HR4ID-FINAL.pdf>
- 12 Human Rights Watch (2021) UN Shared Rohingya Data Without Informed Consent'. New York. HRW. <https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent>
- 13 Owens, K., Eiger, Y., Radka, B., Kohno, T. and Roesner, F. (2025) 'Understanding experiences with compulsory immigration surveillance in the US', in Proceedings of the 2025 ACM conference on Fairness, Accountability and Transparency. <https://dl.acm.org/doi/10.1145/3715275.3732057>
- 14 Prison Policy Initiative (2026) Money Report. <https://www.prisonpolicy.org/reports/money2026.html>
- 15 Akkerman, M. (2019) The Business of Building Walls. Amsterdam: Transnational Institute. <https://www.tni.org/en/publication/the-business-of-building-walls>
- 16 Border Violence Monitoring Network (2026) 'Controlled and confined: unveiling the impact of technology in the Samos Closed Controlled Access Centre'. <https://www.borderviolence.eu/reports/controlled-and-confined-unveiling-the-impact-of-technology-in-the-samos-closed-controlled-access-centre>
- 17 Georgia Tech News (2026) 'Why Iran targeted Amazon data centers, and what does and doesn't change about warfare'. <https://www.gatech.edu/news/2026/04/01/why-iran-targeted-amazon-data-centers-and-what-does-and-doesnt-change-about-warfare>
- 18 Africancio (2026) 'Kenya mandates fair pay and mental healthcare for AI data workers'. <https://africancio.com/en/blog/kenya-mandates-fair-pay-and-mental-healthcare-for-ai-data-wo/>
- 19 Government of Israel (2020) National Strategy on Artificial Intelligence. <https://www.gov.il/en/pages/2020ind>
- 20 Innovation Israel (n.d.) 'A global comparison'. <https://innovationisrael.org.il/en/report/a-global-comparison/>
- 21 Amnesty International (2026) 'EU Simplification Laws'. <https://www.amnesty.org/en/latest/campaigns/2026/04/eu-simplification-laws/>
- 22 EDRI (2026) 'The EU is about to sell our most sensitive data to the US for visa-free travel'. <https://edri.org/our-work/the-eu-is-about-to-sell-our-most-sensitive-data-to-the-us-for-visa-free-travel/>
- 23 For more on TITPI's bug reports and other methodologies see: <https://titipi.org/methods>

AUTHORS: Nick Buxton with Josephine Solanki and TITiPI collective

DESIGN: Evan Clayburg

ILLUSTRATION: Michelle Tylicki

Published by the Transnational Institute

Amsterdam, October 2026

Contents of the report may be quoted or reproduced for non-commercial purposes, provided that the source of information is properly cited. TNI would appreciate receiving a copy or link of the text in which this document is used or cited. Please note that for some images the copyright may lie elsewhere and copyright conditions of those images should be based on the copyright terms of the original source.

<http://www.tni.org/copyright>